**UNIT II**

**Sensors Interfacing:** Temperature and Humidity Sensor (DHT11), Motion Sensor (PIR), Obstacle detection using Ultrasonic sensor, etc, Communicating using RPi- GSM interfacing, Accessing on-board Wi-Fi, Connecting

**IoT Design using Raspberry Pi:** IoT Applications based on Pi, Node-RED, MQTT Protocol

**Interfacing with IoT Platforms:** Basic hardware components like LED, Button, Camera, 8X8 LED Grid, Motor etc and interfacing them for input/output with IoT devices using PWM, GPIO, SPI

**Using Sensor & Actuators**: Overview of Sensors working, Interfacing of Actuators, Servo Motor

**Introduction to IoT**

Internet of Things (IoT) is a massive network of physical devices embedded with sensors, software, electronics, and network which allows the devices to exchange or collect data and perform certain actions.

Simply put, IoT is made up of two words: Internet & Things.

**Things – physical devices, appliances, gadgets, etc.**

**Internet – through which these devices are connected**

IoT aims at extending internet connectivity beyond computers and smartphones to other devices people use at home or for business. The technology allows devices to get controlled across network infrastructure remotely. As a result, it cuts down the human effort and paves the way for accessing the connected devices easily. With autonomous control, the devices are operable without involving human interaction. IoT makes things virtually smart through AI algorithms, data collection, and networks enhancing our lives.

**Characteristics of IoT**

**Dynamic & Self Adapting:** IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user‘s context or sensed environment. Eg: the surveillance system is adapting itself based on context and changing conditions.

**Self Configuring:** allowing a large number of devices to work together to provide certain functionality.

**Inter Operable Communication Protocols**: support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.

**Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address).

Integrated into Information Network: that allow them to communicate and exchange data with other devices and systems.

##### IoT Categories:

1. **Consumer IoT (CIoT)** refers to the use of IoT for consumer applications and devices. Common CIoT products include smartphones, wearables, smart assistants, home appliances, etc. Typically, CIoT solutions leverage Wi-Fi, Bluetooth, and ZigBee to facilitate connectivity. These technologies offer short-range communication suitable for deployments in smaller venues, such as homes and offices.

While CIoT tends to focus on augmenting personal and home environments, Commercial IoT goes a bit further, delivering the benefits of IoT to larger venues. Think: commercial office buildings, supermarkets, stores, hotels, healthcare facilities, and entertainment venues.There are numerous use cases for commercial IoT, including monitoring environmental conditions, managing access to corporate facilities, and economizing utilities and consumption in hotels and other large venues. Many Commercial IoT solutions are geared towards improving customer experiences and business conditions.

1. **Industrial IoT (IIoT),** is perhaps the most dynamic wing of the IoT industry. Its focus is on augmenting existing industrial systems, making them both more productive and more efficient. IIoT deployments are typically found in large-scale factories and manufacturing plants and are often associated with industries like healthcare, agriculture, automotive, and logistics. The Industrial Internet is perhaps the most well-known example of IIoT.
2. **Infrastructure IoT** is concerned with the development of smart infrastructures that incorporate IoT technologies to boost efficiency, cost savings, maintenance, etc. This includes the ability to monitor and control operations of urban and rural infrastructures, such as bridges, railway tracks, and on- and offshore windfarms. Technically speaking, infrastructure IoT is a subset of IIoT. However, due to its significance, it’s often treated as its own separate thing.
3. The last type of **IoT is the Internet of Military Things (IoMT),** often referred to as Battlefield IoT, the Internet of Battlefield Things, or simply IoBT. IoMT is precisely what it sounds like — the use of IoT in military settings and battlefield situations. It is chiefly aimed at increasing situational awareness, bolstering risk assessment, and improving response times. Common IoMT applications include connecting ships, planes, tanks, soldiers, drones, and even Forward Operating Bases via an interconnected system. In addition, IoMT produces data that can be leveraged to improve military practices, systems, equipment, and strategy.

**Sensors**

Sensors are used for sensing things and devices etc. A sensor is 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.

**Characteristics of a Sensor**

1. **Sensitivity** is a measure of the change in output of the sensor relative to a unit change in the input (the measured quantity.) Example: The speakers you purchase for your home entertainment may have a rated sensitivity of 89 dB Signal Pressure Level per Watt per meter.
2. **Resolution** is the smallest amount of change in the input that can be detected and accurately indicated by the sensor. Example: What is the resolution of an ordinary ruler? of a Vernier Calipers?
3. **Linearity** is determined by the calibration curve. The static calibration curve plots the output amplitude versus the input amplitude under static conditions. Its degree of resemblance to a straight line describes the linearity.
4. **Drift** is the deviation from a specific reading of the sensor when the sensor is kept at that value for a prolonged period of time. The zero drift refers to the change in sensor output if the input is kept steady at a level that (initially) yields a zero reading. Similarly, the full -scale drift is the drift if the input is maintained at a value which originally yields a full scale deflection. Reasons for drift may be extraneous, such as changes in ambient pressure, humidity, temperature etc., or due to changes in the constituents of the sensor itself, such as aging, wear etc.
5. **The range** of a sensor is determined by the allowed lower and upper limits of its input or output. Usually the range is determined by the accuracy required. Example: a pocket ruler.
6. **Repeatability**is defined as the deviation between measurements in a sequence when the object under test is the same and approaches its value from the same direction each time. The measurements have to be made under a short enough time duration so as not to allow significant long term drift. Repeatability is usually specified as a percentage of the sensor range.
7. **Reproducibility** is the same as repeatability, except it also incorporates long time lapses between subsequent measurements. The sensor has to be operation between measurements, but must be calibrated. Reproducibility is specified as a percentage of the sensor range per unit of time.

**Classification of Sensors**

**The common IoT sensors include:**

**Temperature sensors, Pressure sensors, Motion sensors, Level sensors, Image sensors, Proximity sensors, Water quality sensors, Chemical sensors, Gas sensors, Smoke sensors, Infrared (IR) sensors, Humidity sensors, etc.**

**Temperature sensors**

[Temperature sensors](https://www.thomasnet.com/products/temperature-sensors-73754103-1.html) detect the temperature of the air or a physical object and concert that temperature level into an electrical signal that can be calibrated accurately reflect the measured temperature. These sensors could monitor the temperature of the soil to help with agricultural output or the temperature of a bearing operating in a critical piece of equipment to sense when it might be overheating or nearing the point of failure.

**Pressure sensors**

[Pressure sensors](https://www.thomasnet.com/products/pressure-sensors-73751604-1.html) measure the pressure or force per unit area applied to the sensor and can detect things such as atmospheric pressure, the pressure of a stored gas or liquid in a sealed system such as tank or pressure vessel, or the weight of an object.

**Motion sensors**

[Motion sensors](https://www.thomasnet.com/products/motion-sensors-73748352-1.html) or detectors can sense the movement of a physical object by using any one of several technologies, including passive infrared (PIR), microwave detection, or ultrasonic, which uses sound to detect objects. These sensors can be used in security and intrusion detection systems, but can also be used to automate the control of doors, sinks, air conditioning and heating, or other systems.

**Level sensors**

[Level sensors](https://www.thomasnet.com/products/liquid-level-sensors-73747107-1.html) translate the level of a liquid relative to a benchmark normal value into a signal. Fuel gauges display the level of fuel in a vehicle’s tank, as an example, which provides a continuous level reading. There are also point level sensors, which are a go-no/go or digital representation of the level of the liquid. Some automobiles have a light that illuminates when the fuel level tank is very close to empty, acting as an alarm that warns the driver that fuel is about to run out completely.

**Image sensors**

[Image sensors](https://www.thomasnet.com/products/image-sensors-73745986-1.html) function to capture images to be digitally stored for processing. License plate readers are an example, as well as facial recognition systems. Automated production lines can use image sensors to detect issues with quality such as how well a surface is painted after leaving the spray booth.

**Proximity sensors**

[Proximity sensors](https://www.thomasnet.com/products/proximity-sensors-73751851-1.html) can detect the presence or absence of objects that approach the sensor through a variety of different technology designs.

**Water quality sensors**

The importance of water to human beings on earth not only for drinking but as a key ingredient needed in many production processes dictates the need to be able to sense and measure parameters around [water quality.](https://www.thomasnet.com/products/water-quality-sensors-73756157-1.html) Some examples of what is sensed and monitored include:

Chemical presence (such as chlorine levels or fluoride levels),[Oxygen levels](https://www.thomasnet.com/products/dissolved-oxygen-sensors-95975082-1.html) (which may impact the growth of algae and bacteria),[Electrical conductivity](https://www.thomasnet.com/products/conductivity-sensors-73741944-1.html) (which can indicate the level of ions present in water), [pH level](https://www.thomasnet.com/products/ph-sensors-73750101-1.html) (a reflection of the relative acidity or alkalinity of the water),Turbidity levels (a measurement of the amount of suspended solids in water)

**Chemical sensors**

[Chemical sensors](https://www.thomasnet.com/products/electrochemical-sensors-96152129-1.html) are designed to detect the presence of specific chemical substances which may have inadvertently leaked from their containers into spaces that are occupied by personnel and are useful in controlling industrial process conditions.

[**Gas sensors**](https://www.thomasnet.com/products/gas-sensors-73744856-1.html)

[Gas sensors](https://www.thomasnet.com/products/gas-sensors-73744856-1.html) are tuned to detect the presence of combustible, toxic, or flammable gas in the vicinity of the sensor. Examples of specific gases that can be detected include:

Bromine (Br2), Carbon Monoxide (CO), Chlorine (Cl2), Chlorine Dioxide (ClO2),Hydrogen Cyanide (HCN),Hydrogen Peroxide (H2O2), Hydrogen Sulfide (H2S), Nitric Oxide (NO), Nitrogen Dioxide (NO2), Ozone (O3), etc.

**Smoke sensors**

[Smoke sensors or detectors](https://www.thomasnet.com/products/smoke-detectors-22181606-1.html) pick up the presence of smoke conditions which could be an indication of a fire typically using optical sensors (photoelectric detection) or ionization detection.

**Infrared sensor**

[Infrared sensor technologies](https://www.thomasnet.com/products/infrared-imaging-sensors-96182977-1.html) detect infrared radiation that is emitted by objects. Non-contact thermometers make use of these types of sensors as a way of measuring the temperature of an object without having to directly place a probe or sensor on that object. They find use in analyzing the heat signature of electronics and detecting blood flow or blood pressure in patients.

**Acceleration sensors**

While motion sensors detect movement of an object, [acceleration sensors](https://www.thomasnet.com/products/acceleration-sensors-73740771-1.html), or accelerometers as they are also known, detect the rate of change of velocity of an object. This change may be due to a free-fall condition, a sudden vibration that is causing movement with speed changes, or rotational motion (a directional change).

**Actuators**

An actuator is a machine component or system that moves or controls the mechanism or the system. Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform. Actuators convert an electrical signal into a corresponding physical quantity such as movement, force, sound etc.

**Servo motars**

Servo is a small device that incorporates a two wire DC motor, a gear train, a potentiometer, an integrated circuit, and a shaft (output spin).

**Stepper motars**

Stepper motors are DC motors that move in discrete steps. They have multiple coils that are organized in groups called “phases”. By energizing each phase in sequence, the motor will rotate, one step at a time. With a computer controlled stepping, you can achieve very precise positioning and/or speed control.

**DC motars**

Direct Current (DC) motor is the most common actuator used in projects. They are simple, cheap, and easy to use. DC motors convert electrical into mechanical energy. Also, they come in different sizes.

**Linear actuator**

A linear actuator is an actuator that creates motion in a straight line, in contrast to the circular motion of a conventional electric motor. Linear actuators are used in machine tools and industrial machinery, in computer peripherals such as disk drives and printers, in valves and dampers, and in many other places where linear motion is required

**Relay**

A relay is an electrically operated switch. Many relays use an electromagnet to mechanically operate a switch. The advantage of relays is that it takes a relatively small amount of power to operate the relay coil, but the relay itself can be used to control motors, heaters, lamps or AC circuits which themselves can draw a lot more electrical power

**Solenoid**

A solenoid is simply a specially designed electromagnet. Solenoids are inexpensive, and their use is primarily limited to on-off applications such as latching, locking, and triggering. They are frequently used in home appliances (e.g. washing machine valves), office equipment (e.g. copy machines), automobiles (e.g. door latches and the starter solenoid), pinball machines (e.g., plungers and bumpers), and factory automation.

**Machine-to-Machine or M2M** is a technology that allows connectivity between network devices. It allows tapping of sensor data and transmitting it over a public network.

IoT technology, on the other hand, expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. It allows users to create high performance, fast and flexible networks that can connect a variety of devices.

|  |  |
| --- | --- |
| **M2M – Machine 2 Machine** | **IoT – Internet of Things** |
| Point to point connection establishment | Devices are connected through the network and also supports connecting to global cloud networks. |
| Limited amount of intelligence | Decision making is enabled |
| Makes use of internet protocols like- HTTP, FTP, etc. | Makes use of traditional communication protocols |
| Generally may not rely on internet connection | Generally Rely on internet connection |
| Less scalable | Highly scalable |

**Components of IoT Implementation**

IoT systems can be implemented by **four** components.

**Sensors**

Sensors are devices that are capable of collecting data from the environment. There are various types of sensors available –temperature sensors, pressure sensors, RFID tags, light intensity detectors, electromagnetic sensors, etc.

**Network**

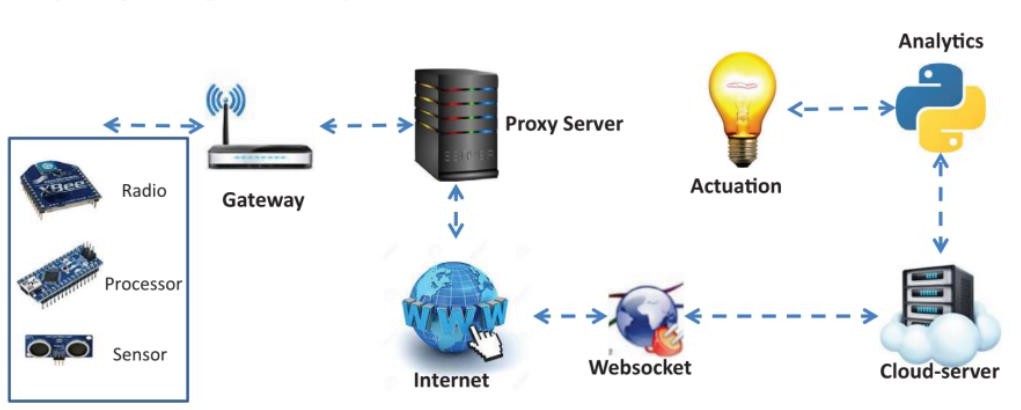
Data collected from sensors are passed over the network for computations to the cloud or processing nodes. Depending upon the scale, they may be connected over LAN, MAN or WAN. They can also be connected through wireless networks like- Bluetooth, ZigBee, Wi-Fi, etc.

**Analytics**

The process of generating useful insights from the data collected by sensors is called analytics. Analytics when performed in real time, can have numerous applications and can make the IoT system efficient.

**Action**

Information obtained after analytics must be either passed to the user using some user interface, messages, alerts, etc; or may also trigger some actions with the help of actuators. Actuators are the devices that perform some action depending on the command given to them over the network.



**Gateways**

Gateways are networking devices that connect IoT devices like sensors or controllers to Cloud. In other ways we can say that data generated by IoT devices are transferred to Cloud servers through IoT gateways.

Gateways connect IoT LANs and WANs together. It is responsible for forwarding packets between them on the IP layer. Since a large number of devices are connected, address space needs to be conserved. Each connected device needs a unique address. IP addresses allocated to devices within a gateway's jurisdiction are valid only in its domain. Same addresses may be allocated in another gateway’s domain. Hence to maintain uniqueness, each gateway is assigned a unique network prefix. It is used for global identification of gateways. This unique identifier removes the need of allocating a unique IP address to each and every device connected to the network, hence saves a lot of address space.

**IoT Identification And Data Protocols**

IoT devices are diverse in their architecture and its use cases can scale from single device deployment to massive cross-platform deployment. There are various types of communication protocols that allow communication between these devices. Some of the protocols are given below.

**IPv4**

Internet Protocol is a network layer protocol version 4 used to provide addresses to hosts in a network. It is a widely used communication protocol for different kinds of networks. It is a connectionless protocol that makes use of packet switching technology. It is used to give a 32 bit address to a host. It is divided into five classes – A, B, C, D, and E. It can provide upto 4.3 billion addresses only which is not sufficient for an IoT device. It allows data to be encrypted but does not limit access to data hosted on the network.

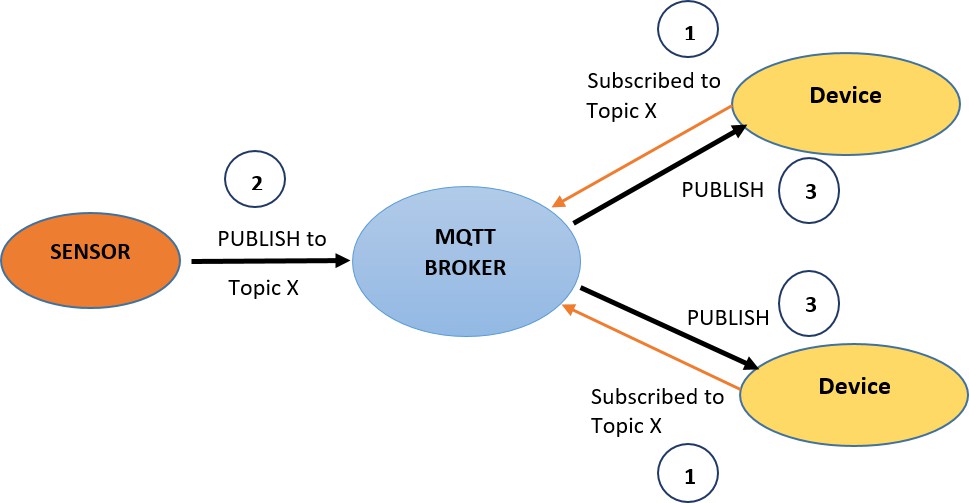
**IPV6**

As the total number of addresses provided by IPv4 are not sufficient specially for IoT devices, Internet protocol version 6 or IPv6 is introduced. It is an upgraded version of IPv4. It uses 128 bits to address a host hence anticipates future growth and provides relief from shortage of network addresses. It gives better performance than IPv4. It also ensures privacy and data integrity. It is automatically configured and has built-in support for authentication. Some of the differences between IPv4 and IPv6 are shown in table.

|  |  |
| --- | --- |
| IPv4 | IPv6 |
| Its length is 32 bits | Its length is 128 bits |
| Possible number of addresses are 232 | Possible number of addresses are 2128 |
| It is represented in dotted decimal notation | It is represented in hexadecimal notation |
| IPsec is optional | IPsec is compulsory |
| It supports manual or DHCP configuration | It supports auto-configuration |
| It supports broadcasting | It supports multicasting |

**MQTT**

Message queuing telemetry transport (MQTT) is a widely used light-weight messaging protocol based on subscription. It is used in conjunction with TCP/IP protocol. It is designed for battery powered devices. Its model is based on Subscriber, Publisher and Broker. Publishers are light weight sensors and subscribers are applications which will receive data from publishers. Subscribers need to subscribe to a topic. Messages updated in a topic are distributed by brokers. Publisher collects the data and sends it to the subscriber through a broker. Broker after receiving messages, filtering and making decisions, sends messages to the subscribers. Brokers also ensure security by authorizing subscribers and publishers. Fig 5 shows the working of MQTT



**CoAP**

Constrained Application Protocol (CoAP) is a web transfer protocol used to translate the HTTP model so as to be used with restrictive devices and network environments.It is used for low powered devices. It allows low power sensors to interact with RESTful services. It makes use of UDP for establishing communication between endpoints. It allows data to be transmitted to multiple hosts using low bandwidth.

**XAMPP**

Extensible messaging and presence protocol (XMPP) enables real time exchange of extensible data between network entities. It is a communication protocol based on XML i.e. extensible markup language. It is an open standard hence anyone can implement these services. It also supports M2M communication across a variety of networks. It can be used for instant messaging, multi-party chat, video calls, etc.

**AMQP**

Advanced message queuing protocol i.e AMQP is an application layer message oriented protocol. It is open standard, efficient, multi-channel, portable and secure. This is fast and also guarantees delivery along with acknowledgement of received messages. It can be used for both point-to-point and publish-subscribe messaging. It is used for messaging in client-server environments. It also supports a multi-client environment and helps servers to handle requests faster.

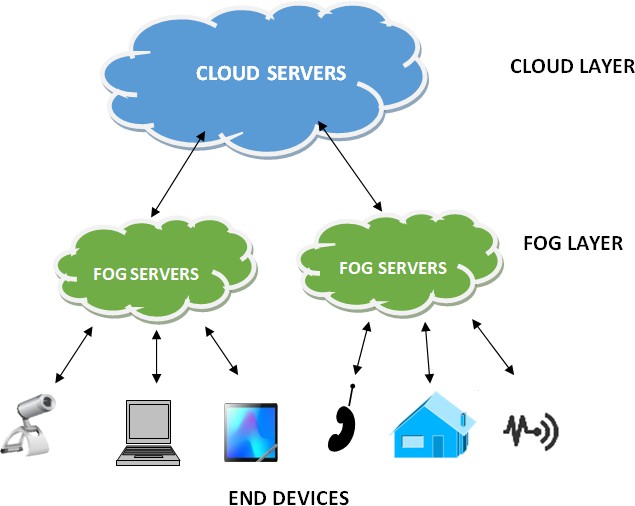
**CLOUD COMPUTING Vs FOG COMPUTING**

Cloud computing technology offers computation service over the internet on a pay-per-use basis. Resources offered by this technology like – storage, compute or network can be dynamically provisioned according to user’s demand. This technology offers several advantages like – low cost, rapid provisioning, high computation power, flexible, automatic updates, no management or monitoring needed from user’s side, etc. Enormous amounts of data generated by IoT devices and users can be stored and processed on cloud servers. But in addition to these benefits, there are several shortcomings associated with this technology – like increased response time due to distant location of servers and centralized architecture, security as resources are remotely stored and provided over insecure internet, demand of higher network bandwidth, increasing load on network due to further increasing users.

Fog computing is a technology in which resources like - compute, data, storage and applications are located in-between the end user layer (where data is generated) and the cloud. Devices like gateways, routers, base stations can be configured as fog devices. It can bring all the advantages offered by cloud computing closer to the location where data is generated; hence leading to reduced response time, reduced bandwidth requirements, enhanced security and other benefits.

Cloud computing is defined as a model that allows ubiquitous access to shared resources on demand over the internet on a pay-per-use basis. Large pools of resources are maintained at data centers by the cloud service providers. Virtual resources from these pools are dynamically provisioned and allocated to users on demand. High performance can be achieved by using cloud resources but it may not be used for real time applications that demand higher response time due to the distant location of cloud servers.

Fog computing is introduced to fill up the gap between the cloud servers and end devices. Fog servers like cloud servers can offer various resources – compute, storage, or network. Due to its proximity to end users, it allows computations to be done faster or near real time. Hence it is better suited for latency sensitive applications. Since fog computing makes use of devices like- switches, routers, gateways; it is generally limited by resources and hence offers less computation power as compared to cloud.



|  |  |
| --- | --- |
| **CLOUD COMPUTING** | **FOG COMPUTING** |
| Architecture in centralized | Architecture is distributed |
| Distant location from the end users | In the proximity of end users |
| Huge amount of resources | Limited amount of resources |
| Higher computation capabilities | Lower computation capabilities |
| More response time | Less response time |
| Can be accessed over internet | Can be accessed by various protocols and standards |
| Less security | More security |

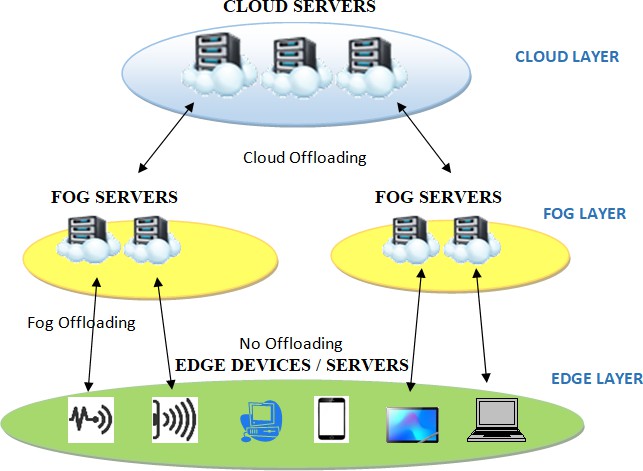
**General architecture of fog computing**

General architecture of fog computing is composed of **three** layers.

1. **End Devices Layer** - Layer 1 is composed of end devices which can be mobile devices, IoT devices, computer systems, camera, etc. Data either captured or generated from these end devices is forwarded to a nearby fog server at Layer 2 for processing.
2. **Fog Layer** - Layer 2 is composed of multiple fog devices or servers. They are placed at the edge of a network, between layer 1 and cloud servers. They can be implemented in devices like – switches, routers, base stations, access points or can be specially configured fog servers.
3. **Cloud Layer** - Layer 3 is composed of Cloud data centers. They consist of huge infrastructure - high performance servers, massive storage devices, etc. They provide all cloud benefits like- high performance, automatic backup, agility.

**Edge computing**

Edge computing is a technology which offers data processing on the same layer where data is generated by making use of edge devices having computation capabilities. This allows data to be processed even faster than processing at fog devices at no or a very low cost. This also increases utilization of edge devices.



**CLOUD Vs FOG Vs EDGE COMPUTING**

Cloud, fog and edge computing all are concepts of distributed computing. All of them perform computation but at different proximity levels and with different resource capacities. Adding Edge and fog layer to the cloud reduces the amount of storage needed at cloud. It allows data to be transferred at a faster data rate because of transferring relevant data. Also the cloud would store and process only relevant data resulting in cost reduction.

Edge computing devices are located at the closest proximity to users. Fog computing devices are located at intermediate proximity. Cloud computing devices are at distant and remote locations from users. Fog computing generally makes use of a centralized system which interacts with gateways and computer systems on LAN. Edge computing makes use of embedded systems directly interfacing with sensors and controllers. But this distinction does not always exist.

|  |  |  |
| --- | --- | --- |
| Cloud Computing | Fog Computing | Edge Computing |
| Centralized approach | Distributed approach | Distributed approach |
| Large amount of resources | Intermediate amount of resources | Limited resources |
| High latency | Medium latency | Low latency |
| Low data rate | Medium data rate | High data rate |
| Globally distributed | Regionally distributed | Locally distributed |
| Non-real time response | Near real time response | Real time response |
| Can be accessed with internet | Can be accessed with internet or without internet | Can be accessed without internet |

**Node –RED**

It is a powerful and popular tool used for **wiring together hardware devices, APIs, and online services** in new and interesting ways. It’s widely used in IoT projects for rapid prototyping, automation, and system integration.

Node-RED is a **flow-based development tool** built on **Node.js**, originally developed by IBM. It provides a **browser-based editor** that makes it easy to wire together devices, sensors, cloud services, and more using a **drag-and-drop interface**.

**Node-RED Components in IoT**

* **Input Nodes**: Receive data (e.g., from sensors via MQTT or HTTP).
* **Processing Nodes**: Transform or route data (e.g., logic, filters, functions).
* **Output Nodes**: Send data to other systems (e.g., dashboards, cloud, actuators).
* **Dashboard Nodes**: Build UI to monitor and control IoT devices.

**SPI (Serial Peripheral Interface)**

It is a **high-speed, synchronous communication protocol** used in **IoT systems** to enable communication between microcontrollers and peripherals like sensors, displays, memory chips, and more.

**PWM in IoT (Pulse Width Modulation)**

It is a **technique used to simulate analog output using digital signals**. In IoT, PWM is widely used to control **devices like motors, LEDs, buzzers**, and more — all essential parts of embedded systems and smart applications.