Fog, Edge and Cloud in IoT

Fog Computing

The solution to the challenges in IoT is to distribute data management throughout the IoT system, as close to the edge of the IP network as possible. The best-known embodiment of edge services in IoT is fog computing. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.

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

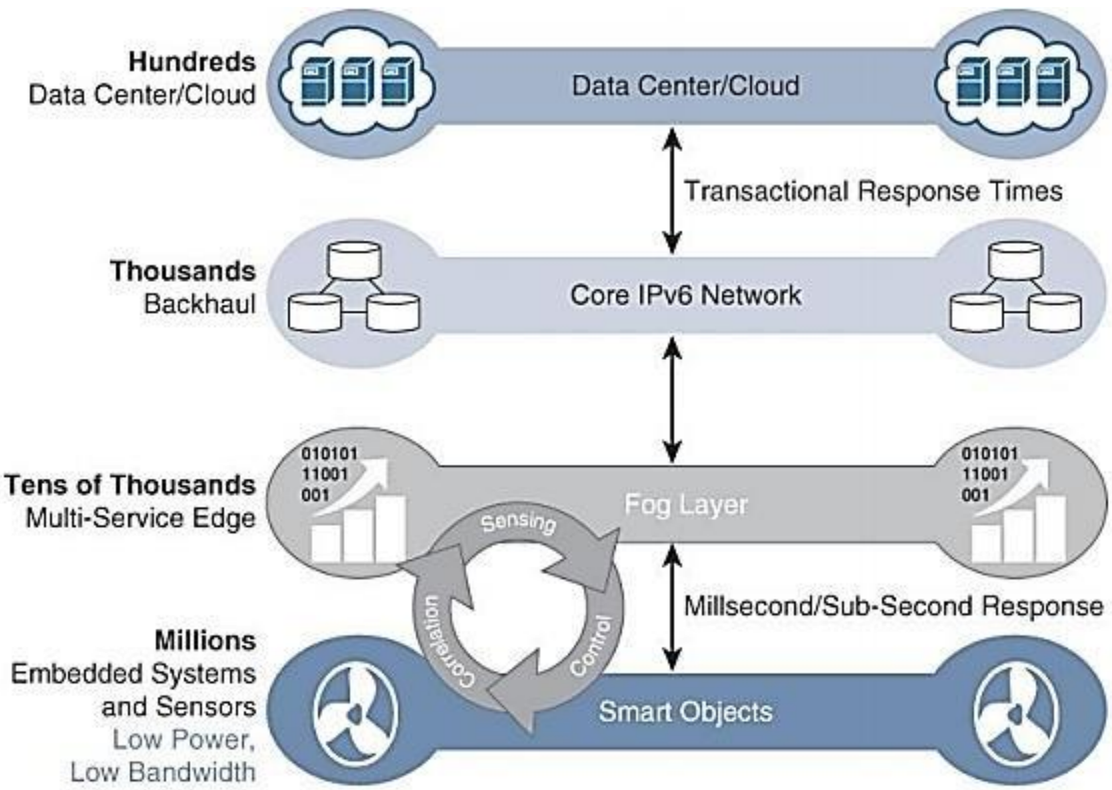

Fig.1.3 Fog computing

The defining characteristic of fog computing are as follows:

Contextual location awareness and low latency: The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.

Geographic distribution: In sharp contrast to the more centralized cloud, the services and applications targeted by the fog nodes demand widely distributed deployments.

Deployment near IoT endpoints: Fog nodes are typically deployed in the presence of a large number of IoT endpoints. For example, typical metering deployments often see 3000 to 4000 nodes per gateway router, which also functions as the fog computing node.

Wireless communication between the fog and the IoT endpoint: Although it is possible to connect wired nodes, the advantages of fog are greatest when dealing with a large number of endpoints, and wireless access is the easiest way to achieve such scale.

Use for real-time interactions: Important fog applications involve real-time interactions rather than batch processing. Pre-processing of data in the fog nodes allows upper-layer applications to perform batch processing on a subset of the data.

Advantages of fog computing in IoT

The fogging approach has many benefits for the Internet of Things, Big Data, and real-time analytics. The main advantages of fog computing over cloud computing are as follows:

- **Low latency** - Fog tends to be closer to users and can provide a quicker response.
- **There is no problem with bandwidth** - pieces of information are aggregated at separate points rather than sent through a channel to a single hub.
- Due to the many interconnected channel**s - loss of connection is impossible**.
- **High Security** - because the data is processed by multiple nodes in a complex distributed system.
- **Improved User Experience** - Quick responses and no downtime make users satisfied.
- **Power-efficiency** - Edge nodes run power-efficient protocols such as Bluetooth, Zigbee, or Z-Wave.

Disadvantages of fog computing in IoT

The technology has no obvious disadvantages, but some shortcomings can be named:

- **Fog is an additional layer in a more complex system** - a data processing and storage system.
- **Additional expenses** - companies must buy edge devices: **routers, hubs, gateways**.
- **Limited scalability** - Fog is not scalable like a cloud.

Edge Computing

Fog computing solutions are being adopted by many industries, and efforts to develop distributed applications and analytics tools are being introduced at an accelerating pace. The natural place for a fog node is in the network device that sits closest to the IoT endpoints, and these nodes are typically spread throughout an IoT network. However, in recent years, the concept of IoT computing has been pushed even further to the edge, and in some cases it now resides directly in the sensors and IoT devices.

Some new classes of IoT endpoints have enough compute capabilities to perform at least low-level analytics and filtering to make basic decisions. For example, consider a water sensor on a fire hydrant. While a fog node sitting on an electrical pole in the distribution network may have an excellent view of all the fire hydrants in a local neighborhood, a node on each hydrant would have clear view of a water pressure drop on its own line and would be able to quickly generate an alert of a localized problem.

Another example is in the use of smart meters. Edge compute–capable meters are able to communicate with each other to share information on small subsets of the electrical distribution grid to monitor localized power quality and consumption, and they can inform fog node of events that may pertain to only tiny sections of the grid. Models such as these help ensure the highest quality of power delivery to customers.

Cloud computing

The delivery of on-demand computing services is known as cloud computing. We may use applications to store and process power over the Internet. Without owning any computing infrastructure or data center, anyone can rent access to anything from applications to storage from a cloud service provider.It is a pay-as-you-go service.By using cloud computing services and paying for what we use, we can avoid the complexity of owning and maintaining infrastructure. Cloud computing service providers can benefit from significant economies of scale by providing similar services to customers.

Cloud computing technology provides a variety of services that are classified into three groups:

- **IaaS (Infrastructure as a Service)** - A remote data center with data storage capacity, processing power, and networking resources.
- **PaaS (Platform as a Service)** - A development platform with tools and components to build, test, and launch applications.
- **SaaS (Software as a Service)** - Software tailored to suit various business needs.

By connecting your company to the Cloud, you can access the services mentioned above from any location and through various devices.

Therefore, availability is the biggest advantage. Plus, there's no need to maintain local servers and worry about downtimes - the vendor supports everything for you, saving you money.

Integrating the Internet of Things with the Cloud is an affordable way to do business. Off-premises services provide the scalability and flexibility needed to manage and analyze data collected by connected devices. At the same time, specialized platforms (**e.g., Azure IoT Suite, IBM Watson, AWS, and Google Cloud IoT**) give developers the power to build IoT apps without major investments in hardware and software.

Advantages of Cloud for IoT

Since connected devices have limited storage capacity and processing power, integration with cloud computing comes to the aid of:

- **Improved performance** - faster communication between IoT sensors and data processing systems.
- **Storage** Capacity - Highly scalable and unlimited storage space can integrate, aggregate, and share huge data.
- **Processing Capabilities** - Remote data centers provide unlimited virtual processing capabilities on demand.
- Low Cost - The license fee is less than the cost of on-premises equipment and its ongoing maintenance.

Disadvantages of Cloud for IoT

Unfortunately, nothing is spotless, and cloud technology has some drawbacks, especially for Internet of Things services.

- **High latency** - More and more IoT apps require very low latency, but the Cloud cannot guarantee this due to the distance between client devices and data processing centers.
- **Downtimes** - Technical issues and network interruptions can occur in any Internet-based system and cause customers to suffer from outages; Many companies use multiple connection channels with automatic failover to avoid problems.
- **Security and Privacy** - your data is transferred via globally connected channels along with thousands of gigabytes of other users' information; No wonder the system is vulnerable to cyber-attacks or data loss; the problem can be partially solved with the help of hybrid or private clouds.

Difference between Fog Computing and Cloud Computing:

- In fog computing, data is received from IoT devices using any protocol.
- Cloud computing receives and summarizes data from different fog nodes.

Structure:

- Fog has a decentralized architecture where information is located on different nodes at the source closest to the user.
- There are many centralized data centers in the Cloud, making it difficult for users to access information on the networking area at their nearest source.

Protection:

- Fog is a more secure system with different protocols and standards, which minimizes the chances of it collapsing during networking.
- As the Cloud operates on the Internet, it is more likely to collapse in case of unknown network connections.

Component:

- Fog has some additional features in addition to the features provided by the components of the Cloud that enhance its storage and performance at the end gateway.
- Cloud has different parts such as frontend platform (e.g., mobile device), backend platform (storage and servers), cloud delivery, and network (Internet, intranet, intercloud).

Accountability:

- Here, the system's response time is relatively higher compared to the Cloud as fogging separates the data and then sends it to the Cloud.
- Cloud service does not provide any isolation in the data while transmitting the data at the gate, increasing the load and thus making the system less responsive.

Application:

- Edge computing can be used for smart city traffic management, automating smart buildings, visual Security, self-maintenance trains, wireless sensor networks, etc.
- Cloud computing can be applied to e-commerce software, word processing, online file storage, web applications, creating image albums, various applications, etc.

Reduces latency:

- Fog computing cascades system failure by reducing latency in operation. It analyzes the data close to the device and helps in averting any disaster.

Flexibility in Network Bandwidth:

- Large amounts of data are transferred from hundreds or thousands of edge devices to the Cloud, requiring fog-scale processing and storage.
- For example, commercial jets generate 10 TB for every 30 minutes of flight. Fog computing sends selected data to the cloud for historical analysis and long-term storage.

Wide geographic reach:

- Fog computing provides better quality of services by processing data from devices that are also deployed in areas with high network density.

- On the other hand, Cloud servers communicate only with IP and not with the endless other protocols used by IoT devices.

Real-time analysis:

- Fog computing analyzes the most time-sensitive data and operates on the data in less than a second, whereas cloud computing does not provide round-the-clock technical support.

Operating Expenses:

- The license fee and on-premises maintenance for cloud computing are lower than fog computing. Companies have to buy edge device routers.

Fog Computing vs. Cloud Computing for IoT

According to Statista, by 2020, there will be 30 billion IoT devices worldwide, and by 2025 this number will exceed 75 billion connected things.

These tools will produce huge amounts of data that will have to be processed quickly and permanently. Fog computing works similarly to cloud computing to meet the growing demand for IoT solutions.