Case Study – Expt. 12

Aim : Case Study on Fog Computing

Theory :

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

Fog computing is the concept of a network fabric that stretches from the outer edges of where data is created to where it will eventually be stored, whether that's in the cloud or in a customer's data center.

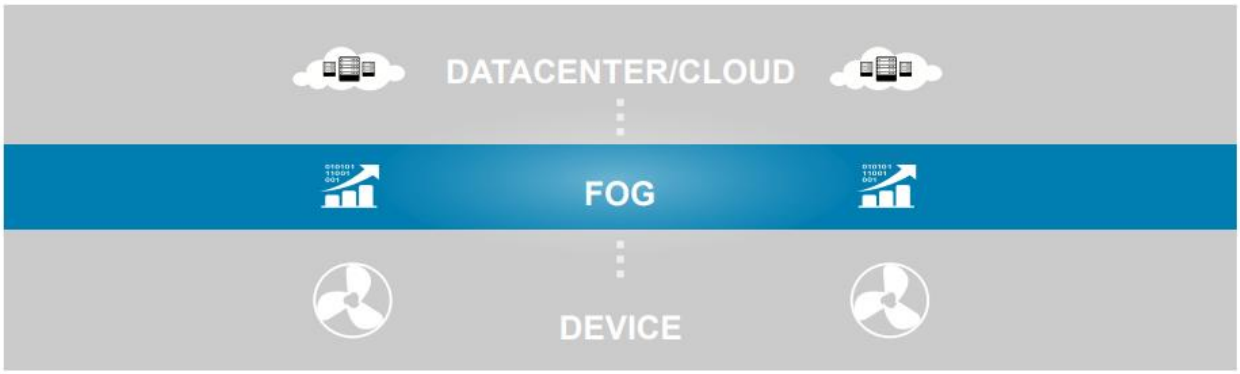
Fog is another layer of a distributed network environment and is closely associated with cloud computing and the internet of things (IoT). Public infrastructure as a service (IaaS) cloud vendors can be thought of as a high-level, global endpoint for data; the edge of the network is where data from IoT devices is created.

Fog computing is the idea of a distributed network that connects these two environments. "Fog provides the missing link for what data needs to be pushed to the cloud, and what can be analyzed locally, at the edge," explains Mung Chiang, dean of Purdue University's College of Engineering and one of the nation's top researchers on fog and edge computing.

What Is It?

The fog extends the cloud to be closer to the things that produce and act on IoT data. These devices, called fog nodes, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oil rig. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and video surveillance cameras. IDC estimates that the amount of data analyzed on devices that are physically close to the Internet of Things is approaching 40 percent.1 There is good reason: analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network, and it keeps sensitive data inside the network. Analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network. And it keeps sensitive data

inside the network.



Examples of Fog Applications :

Fog applications are as diverse as the Internet of Things itself. What they have in common is monitoring or analyzing real-time data from network-connected things and then initiating an action. The action can involve machine-to-machine (M2M) communications or human-machine interaction (HMI). Examples include locking a door, changing equipment settings, applying the brakes on a train, zooming a video camera, opening a valve in response to a pressure reading, creating a bar chart, or sending an alert to a technician to make a preventive repair. The possibilities are unlimited.

Benefits of Fog Computing

● Greater business agility: With the right tools, developers can quickly develop fog applications and deploy them where needed. Machine manufacturers can offer MaaS to their customers. Fog applications program the machine to operate in the way each customer needs.

● Better security: Protect your fog nodes using the same policy, controls, and procedures you use in other parts of your IT environment. Use the same physical security and cybersecurity solutions.

● Deeper insights, with privacy control: Analyze sensitive data locally instead of sending it to the cloud for analysis. Your IT team can monitor and control the devices that collect, analyze, and store data.

● Lower operating expense: Conserve network bandwidth by processing selected data locally instead of sending it to the cloud for analysis.

CONCLUSION : We learned the concept of Fog Computing applications.