Name: Shivam Tiwari Roll No: 5117060

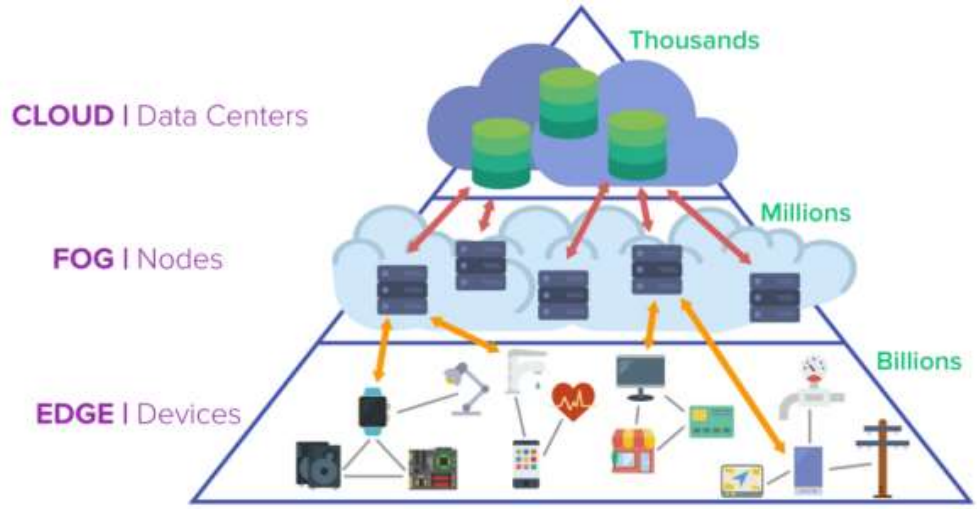
Experiment 6

AIM: Case Study on Fog Computing

THEORY:

1. What is fog computing?

Fog Computing enables a new breed of applications and services, and that there is a fruitful interplay between the Cloud and the Fog, particularly when it comes to data management and analytics. Fog Computing extends the Cloud Computing paradigm to the edge of the network. While Fog and Cloud use the same resources (networking, compute, and storage), and share many of the same mechanisms and attributes (virtualization, multi-tenancy) the extension is a non-trivial one in that there exist some fundamental differences that stem from the Fog raison d'être. The Fog vision was conceived to address applications and services that do not fit well the paradigm of the Cloud.



They include:

- Applications that require very low and predictable latency—the Cloud frees the user from many implementation details, including the precise knowledge of where the computation or storage takes place. This freedom from choice, welcome in many circumstances becomes a liability when latency is at premium (gaming, video conferencing).
- Geo-distributed applications (pipeline monitoring, sensor networks to monitor the environment).
- Fast mobile applications (smart connected vehicle, connected rail).
- Large-scale distributed control systems (smart grid, connected rail, smart traffic light systems).

2. Implementation of fog computing.

A fog computing framework can have a variety of components and functions depending on its application. It could include computing gateways that accept data from data sources or diverse collection endpoints such as routers and switches connecting assets within a network.

The process of transferring data through fog computing architecture in an IoT environment includes the following steps:

- Signals from IoT devices are read by an automation controller.
- The controller executes the system program needed to automate the IoT devices.
- The control system program sends data through to a standard OPC Foundation server or through other gateway protocols. (OPC is the interoperability standard for data exchange in IoT.)
- This data is converted into a protocol understood by internet-based service providers such as MQTT or HTTP(S).
- Once converted, the data is sent to a fog node or IoT gateway. These endpoints collect the data for further analysis or transfer the data sets to the cloud for broader use.

3. Applications of fog computing.

- Connected cars:

Self-driven or self-autonomous cars are now available in the market and they produce a large amount of data. The data needs to be analysed and processed quickly based on the information provided like traffic, driving conditions, climate etc., All this data is processed quickly with the help of fog computing. Other data like vehicle maintenance, tracking is sent directly to the manufacturer. Both edge and endpoint communication is made possible with the help of connected cars.

- Smart grids and smart cities:

For effectively running systems, utility systems are using real-time data. It is essential to process the remote data close to the place where it is created. It is also possible the data is generated from many sensors. Fog computing is designed in such a way that it can sort both the issues.

- Real-time analytics:

Data can be transferred from the place it is created to different places using fog computing deployments. Fog computing is used for real-time analytics which transfers the data from manufacturing systems to financial institutions which use real-time data.

The smart electric grid is the best example of grid computing. Electrical grids are smart and dynamic these days. It will be responsive while needing less production and electrical consumption. Fog computing is ideal in a situation where the data is generated from a remote location, it can be processed there itself rather than to carry it to data centres. Some of the data may be generated from single sensors or a group of sensors and it can be processed there to avoid overloading of the cloud. Electric meters is one best example of this.

4. Security and privacy issues in fog computing.

- TRUST

IoT networks are expected to provide reliable and secure services to the EUs. This requires all devices that are part of the fog network to have a certain level of trust on one another. Authentication plays a major role in establishing the initial set of relations between IoT devices and fog nodes in the network. But this is not sufficient as devices can always malfunction or are also susceptible to malicious attacks. In such a scenario, trust plays a major role in fostering relations based on previous interactions. Trust should play a two way role in a fog network. That is, the fog nodes that offer services to IoT devices should be able to validate whether the devices requesting services are genuine.

- AUTHENTICATION

Authentication of networked devices subscribed to fog services is one of the foremost requirements in fog network. To access the services of a fog network, a device has to first become part of the network by authenticating itself to the fog network. This is essential to prevent the entry of unauthorized nodes. It becomes a formidable challenge as the devices involved in the network are constrained in various ways including power, processing and storage.

- SECURE COMMUNICATIONS IN FOG COMPUTING

The way processing and storage requirements can be offloaded to fog nodes, security requirements cannot be offloaded. Even IoT devices need to implement the minimum security requirements. Communications between IoT devices VOLUME 5, 2017 19295 M. Mukherjee et al.: Security and Privacy in Fog Computing: Challenges are considered to be taken care of the security practices in place for IoT communications. IoT devices interact with fog nodes only when they need to offload a processing or storage request. Any other interactions would not be considered as part of the fog environment as such communications would happen as part of the network. These fog nodes interact with each other when they need to effectively manage network resources or to manage network itself

- END USER'S PRIVACY

Fog computing lies on the computational power of distributed nodes for reducing the total pressure of the data center. In fog computing, privacy preservation is more challenging since fog nodes that are in vicinity with EUs may collect sensitive data concerning the identity, usage of utilities, e.g. smart grid or location of end users compared to the remote cloud server that lies in the core network. Moreover, since fog nodes are scattered in large areas, centralized control is becoming difficult. The compromise of a poorly secured edge node can be the entry point for an intruder to the network. The intruder once inside the network can mine and steal users' privacy data that is exchanged among entities.

- MALICIOUS ATTACKS

Fog computing environments can be subjected to several malicious attacks and without proper security measures in place may severely undermine the capabilities of the network. One such malicious attack that can be launched is a Denial-ofService (DoS) attack. Since the majority of the devices connected to the networks are not mutually authenticated, launching a DoS attack becomes straight forward. The

attack may be launched when devices that are connected to IoT network request for infinite processing/storage services.

5. Advantage and limitation of computing.

Advantages:

- Privacy

Fog computing can be used to control the extent of privacy. Any sensitive data of the user can be analyzed locally instead of sending them to a centralized cloud infrastructure. Through this way the team of IT will be able to track and control the respective device. Furthermore if any subset of data needs to be analyzed it can be sent to the cloud.

- Productivity

If customer needs to make the machine function according to the way they want, they can utilize fog applications. These fog applications can be easily made by the developers with the right set of tools. After the development has taken place it can be deployed whenever they want.

- Security

Fog computing has the capability to connect multiple devices to the same network. Because of this the operations take place at various end points in a complex distributed environment rather than a centralized location. This makes it easier to identify potential threats before it affects the whole network.

- Bandwidth

The bandwidth required for transmitting data can be expensive depending upon the resources. Due to the fact that the selected data can be processed locally instead of sending it to the cloud, there are very few bandwidth requirements. This bandwidth savings will be especially beneficial when increasing the number of IoT devices

- Latency

Another benefit of processing selected data locally is the latency savings. The data can be processed at the nearest data source geographically closer to the user. This can produce instant responses especially for the time sensitive services.

Limitations:

- Complexity

Due to its complexity, the concept of Fog computing can be difficult to understand. There are many devices located at different locations storing and analyzing their own set of data. This could add more complexity to the network. In addition to that there are more sophisticated fog nodes present in a fog infrastructure.

- Security

As mentioned earlier there are numerous devices and different fog nodes present in a fog computing architecture. There are chances for these fog nodes to be in a less secure environment. Hackers can easily impose fake IP addresses on them gaining access to the respective fog node. Or else they increase the risk of corrupted files infiltrating the main data stream infecting both the device and the company. This makes them vulnerable to Man-in-the-middle attacks.

- Authentication

Service offered by fog computing is of large scale. The fog computing is composed of end users, internet service providers and cloud providers. This can often raise trust and authentication issues in the fog.

- Maintenance

Unlike cloud architecture, where maintenance is made seamless, it is not so in fog. Since controllers and storages are distributed across various locations in the network it needs more maintenance. The fog architecture is decentralized for processing.

- Power Consumption

The number of fog nodes present in a fog environment is directly proportional to the energy consumption of them. Which means that these fog nodes require a high amount of energy for them to function? As there are more fog nodes in a fog infrastructure there is more power consumption as well. Most companies often try to lower their cost using these fog nodes.

CONCLUSION:

Detailed comparison of cloud computing and fog computing:

Feature	Cloud Computing	Fog Computing
Latency	Cloud computing has high latency compared to fog computing	Fog computing has low latency
Capacity	Cloud Computing does not provide any reduction in data while sending or transforming data	Fog Computing reduces the amount of data sent to cloud computing.
Responsiveness	Response time of the system is low.	Response time of the system is high.
Security	Cloud computing has less security compared to Fog	Fog computing has high Security.
Speed	Access speed is high depending on the VM connectivity.	High even more compared to Cloud Computing.
Data Integration	Multiple data sources can be integrated.	Multiple Data sources and devices can be integrated.
Mobility	In cloud computing mobility is Limited.	Mobility is supported in fog computing.
Location Awareness	Partially Supported in Cloud computing.	Supported in fog computing.
Number of Server Nodes	Cloud computing has Few number of server nodes.	Fog computing has Large number of server nodes.
Geographical Distribution	It is centralized.	It is decentralized and distributed.
Location of service	Services provided within the internet.	Services provided at the edge of the local network.
Working environment	Specific data center building with air conditioning systems	Outdoor (streets,base stations, etc.) or indoor (houses, cafes, etc.)
Communication mode	IP network	Wireless communication: WLAN, WiFi, 3G, 4G, ZigBee, etc. or wired communication (part of the IP networks)