Role of Fog Computing in IoT based applications

Manasi Kulkarni, Damini Mahale, Mayur Panchariya,
Ritesh Kulkarni and Bhushan Nandwalkar

October 20, 2020

ROLE OF FOG COMPUTING IN IOT BASED APPLICATIONS

Manasi Kulkarni
Computer Engineering
Shri Vile Parle Kelvani Mandal's Institute of Technology
Dhule, India
manu221143@gmail.com

Damini Mahale
Computer Engineering
Shri Vile Parle Kelvani Mandal's Institute of Technology
Dhule, India
daminimahale234@gmail.com

Mayur Panchariya
Computer Engineering
Shri Vile Parle Kelvani Mandal's Institute of Technology
Dhule, India
mayurpanchariya95@gmail.com

Ritesh Kulkarni
Computer Engineering
Shri Vile Parle Kelvani Mandal's Institute of Technology
Dhule, India
riteshkulkarni2311@gmail.com

Bhushan Nandwalkar
Assistant Professor
Shri Vile Parle Kelvani Mandal's Institute of Technology
Dhule, India

***Abstract*— Internet of things (IoT) services have been accepted and accredited globally for the past couple of years and have had increasing interest from researchers. Internet of Things (IoT), requires mobility support and geo-distribution in addition to location awareness and low latency. We argue that a new platform is needed to meet these requirements; a platform we call Fog Computing.**
Fog Computing extends the Cloud Computing paradigm to the edge of the network, thus enabling a new breed of applications and services. The patent concept of fog computing is currently attracting many researchers as it brings cloud services closer to the end-user. The aim of this paper is to highlight the role of fog computing in IOT based applications.

Keywords: Fog computing, Cloud computing, Edge computing, IoT applications

INTRODUCTION

The potent concept of fog computing is currently attracting many researchers as it brings cloud services closer to the end-user.
In recent years, Internet of Things (IoT) has gathered considerable attention, as it provides various IoT services in almost all fields of life. IoT is an interconnected network of large numbers of IoT devices, each having the capability of sensing and communication, through which they report their sensed data to the main server. This enables the control center, based on received data, to take decisions intelligently Like small wireless devices used in S-band sensing technique, IoT uses small sensor devices. The increase in usage of IoT devices has led to requirement of resource and computing paradigms which may work efficiently in collaboration with IoT environment. The major paradigms are Cloud computing, Fog computing and Edge computing.This paper will primarily focus on Fog computing in IoT Environment

Before focusing on Fog computing let us know the technologies used before it, that are Cloud Computing and Edge Computing.

1.IOT:

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Thanks to the arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything,from something as small as a pill to something as big as an aeroplane into a part of the IoT.
Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The Internet of Things is making the fabric of the world around us more smarter and more responsive, merging the digital and physical universes.

2.Cloud Computing:

Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet).
Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.
The term is generally used to describe data centersavailable to many users over the internet.
Various requirements of IoT such as scalability, privacy, enormous bandwidth requirements, energy consumption, efficiency in network computations and delay-sensitive communication, were not managed efficiently by Cloud.

3.EDGE Computing:

Edge computing is the computational processing of sensor data away from the centralized nodes and close to the logical edge of the network, toward individual sources of data.The technology involved network nodes storing static cached media information at locations closer to end-users. Only partial sets of information processed and analyzed by edge computing. Only delete the rest of the records. Due to its proximity to the users, latency in edge computing is typically lower than in cloud computing. Edge Computing cannot Support the Multiple IOT Devices.

4.Fog computing:

Fog computing is a new technology paradigm to reduce the complexity, scale and size of the data actually going up to the cloud. Pre-processing of raw data coming out of the sensors and IOT devices is essential and it is an efficient way to reduce the load of the big data on the cloud.

Fog computing bridges the gap between the cloud and end devices (e.g., IoT nodes) by enabling computing, storage, networking, and data management on network nodes within the close vicinity of IoT devices.

Fog Computing and IoT

Internet of Things (IoT) needs to operate on a fast network topologies that provides end-to-end connection and real-time responses. For instance the frequent disconnections and reconnections by the devices, or notifications of a disaster or an imminent collapse of the system. In many cases, decisions must be taken in a short time and it is necessary to be able to rely on a reliable connection between the customer and the corresponding servant who performs complex tasks. In many situations, especially dictated by the overload of communications in multi-hop WAN networks, these qualities are not guaranteed by the Cloud

Because cloud computing is not viable for many Internet-of-Things applications, fog computing is often used. Its distributed approach addresses the needs of IoT and industrial IoT, as well as the immense amount of data smart sensors and IoT devices generate, which would be costly and time-consuming to send to the cloud for processing and analysis. Fog computing reduces the bandwidth needed and reduces the back-and-forth communication between sensors and the cloud, which can negatively affect IoT performance.

Although latency may be annoying when sensors are part of a gaming application, delays in data transmission in many real-world IoT scenarios can be life-threatening -- for example, in vehicle-to-vehicle communications systems, smart grid deployments or telemedicine and patient care environments, where milliseconds matter. Fog computing and IoT use cases also include smart rail, manufacturing and utilities.

Hardware manufacturers, such as Cisco, Dell and Intel, are working with IoT analytics and machine-learning vendors to create IoT gateways and routers that support fogging. The OpenFog Consortium was founded in November 2015 by members from Cisco, Dell, Intel, Microsoft, ARM and Princeton University; its mission is to develop an open reference architecture and convey the business value of fog computing.

LITERATURE SURVEY

Our Literature survey is based on previous technologies i.e. Cloud computing and Edge computing with reference to some technical parameters.

1.Geographically distributed: As per the author the cloud computing system is not geographically distributed whereas as per survey of authors the edge computing and fog computing are distributed systems. We can say that the edge computing and fog computing are interface between server and the IoT application. [1][2]

We can say that edge computing is partially geographically distributed system because it repeatedly needs a reference of cloud server to response to smart devices whereas fog computing is completely distributed system because to distribute data to move it closer to the end user which eliminate or decrease the latency.[3]

2. Real time application: The author cloud computing does not support real time application due to some reasons like it is not geographically distributed system.[1]

Also author says that the edge computing supports small real time applications as follows the repetitive query system.[2]

Whereas the fog computing fully supports the real time applications as it is geographically distributed system, its latency is low .[3]

3. Large scale Application support: As per the author the cloud computing does not support large scale application because it’s bandwidth cost is high as compared to edge computing and fog computing [2][3]

Edge computing is suitable/supports large scale application but drawback of this system it is a partially distributed system and it follows repeated query system due to which response time is increased.[2] Whereas author claims that fog computing is perfect or complete solution for real time as well as large scale application because it is a distributed system as it distributes the data in many small modules nearer to the end user due to which its bandwidth cost is low and response time is high. [3]

4. Server and Storage: As per the author in case of server cloud computing is centralized server system whereas edge computing is partially centralized server system and fog computing has decentralized server because it is a completely distributed system i.e. it has multiple remote locations same as its application like smart city or smart watch has. In case of storage cloud computing has a big storage as compared to edge and fog because edge computing act as a interface between server and end user. So we can say that it is a small bridged storage whereas fog computing has a multi storage or multiple storage due to its distributed format . [1][2][3]

5. Security: After studying the data security problems in Fog-IoT network, authors considered different security protocols that could be used in Fog-IoT network for data security.The key focus of this model is data security during data travelling from client to Fog nodes.

They selected Shibboleth security protocol after its critical analysis in Cloud-IoT environment. Shibboleth provides system with integrity, authentication and privacy.

In Shibboleth, access control mechanism compares attributes, issued by identity provider. Moreover, metadata is the trust basis between Shibboleth providers.

Considering the substantial of this protocol, authors added new layers of Shibboleth protocol between client and Fog node.

The purpose is to secure data access, authentication, authorization and user's privacy from Service Providers (SP). Later, they used High-Level Petri Net (HLPN) for system modelling and Z3 constraints solver for automated SMT solution and formal verification. In addition, it also provided the correctness of system.

So we can say that if we compare all three systems then cloud and edge computing are less secured than fog computing because:

a. As cloud is centralized and edge is partially centralized system so it can get easily affected by any malware attacks like DOS attack , MITM attack ,etc.

Application Based Explanation:

Smart City:

Smart city with Fog Computing:

Large cities face challenges from traffic congestion, public safety, high energy use, sanitation and in providing municipal services. These challenges can be addressed within a single IoT network by installing a network of fog nodes.

A lack of broadband bandwidth and connectivity is a major issue in establishing smart cities. While most modern cities have one or more cellular networks providing adequate coverage, these networks often have capacity and peak bandwidth limits that barely meet the needs of existing subscribers. This leaves little bandwidth for the advanced municipal services envisioned in a smart city. Deploying a fog computing architecture allows for fog nodes to provide local processing and storage. This optimizes network usage.

Smart cities also struggle with safety and security, where time-critical performance requires advanced, real-time analytics. Municipal networks may carry sensitive traffic and citizen data, as well as operate life-critical systems such as emergency response. Fog computing addresses security, data encryption and distributed analytics requirements.

Smart cities can see the following benefits through fog computing:

- A minimal amount of data sent to the cloud

- The central goal of fog computing is to make big data smaller and more manageable. It is estimated that the volume of data captured by connected devices will exceed 79 zettabytes by 2025 according to IDC's 2019 forecast. Fog computing is capable of reducing this vast amount of data through the application of intelligent sensing and filtering, which allow the transmission of only useful information based on the knowledge available locally at a given fog device.

- Low data latency

Fog nodes are able to process and onboard data without sending it to remote cloud servers and delivering the results back. This makes it easier to save time considerably when the data is traveling and to receive responses in real time. Immediate data processing will only become more essential for smart city systems, especially when decisions or actions need to be made quickly: for example, lives could be saved by being able to suddenly change traffic lights to green when emergency vehicles are moving through the city.

- Reduced bandwidth

Transmitting and processing data requires a massive amount of bandwidth, which can be limited in the case of cloud computing. However, this is not an issue when it comes to fog computing seeing as all of the data is distributed between local devices and is not sent wirelessly. This allows for a significant decrease in the network bandwidth consumption.

- Enhanced data security

Data security is another critical driver behind smart cities turning their resources over to fog computing. It keeps the more sensitive and confidential data out of reach from the vulnerable public networks, thereby preventing any cybercriminals from easily gaining access to it. Fog computing allows for malware and infected files to be found at an early stage in their cycles at the device level long before they even have the opportunity to infect the whole network.

Smart city with cloud Computing:

Vendor lock-in is a problem, together with the lack of control on the location where applications run and data are stored. This is an important barrier to cloud- based smart city solutions, in particular when applica-tions manage personal data and the provider has legal obligation for securing data privacy. cloud computing suffers from processing time inefficiency due to the large overhead of smart city device data.

Smart city with edge Computing:

Edge computing is less scalable compared to fog computing. Also, edge computing supports little interoperability, which might make IoT devices incompatible with certain cloud services and operating systems. Also, multiple tasks and operations performed by IoT devices and cloud cannot be extended .

Smart city requires multiple iot devices but edge computing cannot support multiple iot devices.

Conclusion:

Fog Computing aims to reduce processing burden of cloud computing. Fog computing is bringing data processing, networking, storage and analytics closer to devices and applications that are working at the network's edge. that's why Fog Computing today's trending technology mostly for IoT Devices.

We have outlined the vision and defined key characteristics of Fog Computing, a platform to deliver a rich portfolio of new services and applications at the edge of the network.The motivating examples peppered throughout the discussion range from conceptual visions to existing point solution prototypes. We envision the Fog to be a unifying platform,rich enough to deliver this new breed of emerging services and enable the development of new application.

References

[1] Rajaputhri Maharaja1 • Prashant Iyer1 • Zilong Ye1. A hybrid fog-cloud approach for securing the Internet of Things. Cluster Computing (2020) 23:451–459

[2] D. S. Park. Future computing with IoT and cloud computing The Journal of Super computing (2018) 74:6401–6407

[3] Ping Zhang1·Mimoza Durresi2·Arjan Durresi1 Multi-access edge computing aided mobility for privacy protection in Internet of Things . Computing(2019)101:729–742 .

[4] Rida Zojaj Naeem1 · Saman Bashir1 · Muhammad Faisal Amjad1 · Haider Abbas1.Hammad Afzal1. Fog computing in internet of things: Practical applications and future directions. Peer-to-Peer Networking and Applications (2019) 12:1236–1262

[5] SalvatoreVenticinque1 · Alba Amato1 . A methodology for deployment of IoT application in fog. Journal of Ambient Intelligence and Humanized Computing (2019) 10:1955–1976