Fog Computing Pushing Intelligence to the Edge

Monika Gupta
Department of Electronics & Communication Engineering
New Horizon College of Engineering Bengaluru, India

Abstract

Cloud computing is a delivery platform which promises a new way of accessing and storing personal as well as business information. It provides resources to its users through the Internet. But it also has a risk that is the involvement of a third party which makes it difficult to trust that user data is secure enough and will not be misused. To provide security, new technology called Fog computing is used. Fog computing, also termed edge computing, can address those problems by providing elastic resources and services to end users at the edge of network, while cloud computing are more about providing resources distributed in the core network. Fog computing extends cloud computing by providing virtualized resources and engaged location-based services to the edge of the mobile networks so as to better serve mobile traffics. Therefore, Fog computing is a lubricant of the combination of cloud computing and mobile applications.

Keywords: Fog Computing, Cloud Computing, NFV, SDN

I. INTRODUCTION

As the Internet of Things evolves into the Internet of Everything and expands its reach into virtually every domain, high-speed data processing, analytics and shorter response times are becoming more necessary than ever. Meeting these requirements is somewhat problematic through the current centralized, cloud-based model powering IoT systems, but can be made possible through fog computing, a decentralized architectural pattern that brings computing resources and application services closer to the edge, the most logical and efficient spot in the continuum between the data source and the cloud. The term fog computing, coined by Cisco, refers to the need for bringing the advantages and power of cloud computing closer to where the data is being generated and acted upon. Fog computing reduces the amount of data that is transferred to the cloud for processing and analysis, while also improving security, a major concern in the IoT industry. In a fog computing environment, much of the processing takes place in a data hub on a smart mobile device or on the edge of the network in a smart router or other gateway device. This distributed approach is growing in popularity because of the Internet of Things (IoT) and the immense amount of data that sensors generate. It is simply inefficient to transmit all the data a bundle of sensors creates to the cloud for processing and analysis; doing so requires a great deal of bandwidth and all the back-and-forth communication between the sensors and the cloud can negatively impact performance. Although latency may simply be annoying when the sensors are part of a gaming application, delays in data transmission can be life-threatening if the sensors are part of a vehicle-to-vehicle communication system or large-scale distributed control system for rail travel.

Fig. 1: Fog between Edge and Cloud
Fog computing can be perceived both in large cloud systems and big data structures, making reference to the growing difficulties in accessing information objectively. This results in a lack of quality of the obtained content. The effects of fog computing on cloud computing [1, 2] and big data systems may vary; yet, a common aspect that can be extracted is a limitation in accurate content distribution, an issue that has been tackled with the creation of metrics that attempt to improve accuracy. CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things (IoT), to run directly at the network edge. Customers can develop, manage and run software applications on Cisco IOx framework of networked devices, including hardened routers, switches and IP video cameras. Cisco IOx brings the open source Linux and Cisco IOS network operating system together in a single networked device (initially in routers). The open application environment encourages more developers to bring their own applications [3] and connectivity interfaces at the edge of the network. Regardless of Cisco’s practices, we first answer the questions of what the Fog computing is and what are the differences between Fog and Cloud. In Fog computing [4], services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the “ground”, creates automated response that drives the value. Both Cloud and Fog provide data, computation, storage and application services to end-users. However, Fog can be distinguished from Cloud by its proximity to end-users, the dense geographical distribution and its support for mobility. We adopt a simple three level hierarchy as in Figure 1.

II. PROBLEM WITH THE CLOUD COMPUTING

As the Internet of Things proliferates, businesses face a growing need to analyze data from sources at the edge of a network, whether mobile phones, gateways, or IoT sensors. Cloud computing has a disadvantage: It can’t process data quickly enough for modern business applications. The IoT owes its explosive growth to the connection of physical things and operation technologies (OT) to analytics and machine learning applications, which can help glean insights from device-generated data and enable devices to make “smart” decisions without human intervention. Currently, such resources are mostly being provided by cloud service providers, where the computation and storage capacity exists.

However, despite its power, the cloud model is not applicable to environments where operations are time-critical or internet connectivity is poor. This is especially true in scenarios such as telemedicine and patient care, where milliseconds can have fatal consequences. The same can be said about vehicle to vehicle communications, where the prevention of collisions and accidents can’t afford the latency caused by the roundtrip to the cloud server. “The cloud paradigm is like having your brain command your limbs from miles away — it won’t help you where you need quick reflexes.”

Moreover, having every device connected to the cloud and sending raw data over the internet can have privacy, security and legal implications, especially when dealing with sensitive data that is subject to separate regulations in different countries. IoT nodes are closer to the action, but for the moment, they do not have the computing and storage resources to perform analytics and machine learning tasks. Cloud servers, on the other hand, have the horsepower, but are too far away to process data and respond in time.

The fog layer is the perfect junction where there are enough compute, storage and networking resources to mimic cloud capabilities at the edge and support the local ingestion of data and the quick turnaround of results.

The variety of IoT systems and the need for flexible solutions that respond to real-time events quickly make Fog Computing a compelling option.

III. ARCHITECTURE OF FOG COMPUTING

![Fig. 2: Fog Architecture as proposed by CISCO](image-url)
The Fog computing extends cloud computing by introducing an intermediate Fog layer between mobile devices and cloud. This accordingly leads to a three-layer Mobile-Fog-Cloud hierarchy. The intermediate Fog layer is composed of geodistributed Fog servers which are deployed at the local premises of mobile users, e.g., parks, bus terminals, shopping centers, etc.. A Fog server is a virtualized device with build-in data storage, computing and communication facility; the purpose of Fog computing is therefore to place a handful of compute, storage and communication resources in the close proximity of mobile users, and accordingly provide fast-rate services to mobile users via the local short-distance [8] high-rate wireless connections. A Fog server can be adapted from existing network components, e.g., a cellular base station, WiFi access point or router by upgrading the computing and storage resources and reusing the wireless interface. A Fog server can be static at a fixed location, e.g., inside a shop installed similar as a WiFi access point, or mobile placed on a moving vehicle as the Greyhound “BLUE” system. The role of Fog servers is to bridge the mobile users and cloud [9]. On one hand, Fog servers directly communicate with mobile users through single-hop wireless connections using the off-the-shelf wireless interfaces, such as WiFi, cellular or Bluetooth1. With cloud-like resources, a Fog server is able to independently provide predefined application services to mobile users in its wireless coverage without the assistances of other Fog servers or remote cloud. On the other hand, the Fog servers can be connected to the cloud over Internet so as to leverage the rich computing and content resources of cloud.

IV. BENEFITS OF FOG COMPUTING

Fog computing provides: Low latency and location awareness, it has Wide-spread geographical distribution, supports Mobility, is compromised due to the huge number of nodes. The main task of fog is to deliver data and place it closer to the user who is positioned at a location which at the edge of the network. Here the term edge refers to different nodes to which the end user is connected and it is also called edge computing. If we look according to architecture fog is situated below the cloud at the ground level. The term fog computing is given by CISCO as a new technology in which mobile devices interact with one another and support the data communication within the Internet of Things.

- Frees up network capacity – Fog computing uses much less bandwidth, which means it doesn’t cause bottlenecks and other similar occupancies. Less data movement on the network frees up network capacity, which then can be used for other things.
- It is truly real-time – Fog computing has much higher expedience than any other cloud computing architecture we know today. Since all data analysis are being done at the spot it represents a true real time concept, which means it is a perfect match for the needs of Internet of Things concept.
- Boosts data security – Collected data is more secure when it doesn’t travel. Also makes data storing much simpler, because it stays in its country of origin. Sending data abroad might violate certain laws.

V. DISADVANTAGES

Security is the biggest concern when it comes to fog computing. By leveraging a remote cloud based infrastructure, a company essentially gives away private data and information, things that might be sensitive and confidential. It is then up to the fog service provider to manage, protect and retain them, thus the provider’s reliability is very critical. A company’s existence might be put in jeopardy, so all possible alternatives should be explored before a decision. On the same note, even end users might feel uncomfortable surrendering their data to a third party.

- Analytics is done locally- Fog computing concept enables developers to access most important IoT data from other locations, but it still keeps piles of less important information in local storages.
- Some companies don’t like their data being out of their premises- with Fog Computing lots of data is stored on the devices themselves (which are often located outside of company offices), this is perceived as a risk by part of developers’ community.
- Whole system sounds a little bit confusing- Concept that includes huge number of devices that store, analyze and send their own data, located all around the world sounds utterly confusing.

VI. FUTURE OF FOG COMPUTING

The current trend shows that fog computing will continue to grow in usage and importance as the Internet of Things expands and conquers new grounds. With inexpensive, low-power processing and storage becoming more available, we can expect computation to move even closer to the edge and become ingrained in the same devices that are generating the data, creating even greater possibilities for inter-device intelligence and interactions. Sensors that only log data might one day become a thing of the past. It seems obvious that while cloud is a perfect match for the Internet of Things, we have other scenarios and IoT solutions that demand low-latency ingestion and immediate processing of data where Fog Computing is the answer.

VII. DOES THE FOG ELIMINATE THE CLOUD

Fog computing improves efficiency and reduces the amount of data that needs to be sent to the cloud for processing. But it’s here to complement the cloud, not replace it [2]. The cloud will continue to have a pertinent role in the IoT cycle. In fact, with fog computing shouldering the burden of short-term analytics at the edge, cloud resources will be freed to take on the heavier tasks,
especially where the analysis of historical data and large datasets is concerned. Insights obtained by the cloud can help update and tweak policies and functionality at the fog layer. And there are still many cases where the centralized, highly efficient computing infrastructure of the cloud will outperform decentralized systems in performance, scalability and costs. This includes environments where data needs to be analyzed from largely dispersed sources. “It is the combination of fog and cloud computing that will accelerate the adoption of IoT, especially for the enterprise.” In essence, Fog Computing allows for big data to be processed locally, or at least in closer proximity to the systems that rely on it. Newer machines could incorporate more powerful microprocessors, and interact more fluidly with other machines on the edge of the network. While fog isn’t a replacement for cloud architecture, it is a necessary step forward that will facilitate the advancement of IoT, as more industries and businesses adopt emerging technologies.

VIII. MODELING AND SIMULATION

To enable real-time analytics in fog computing, we must investigate various resource-management and scheduling techniques including the placement, migration, and consolidation of stream-processing operators, application modules, and tasks. This significantly impacts processing latency and decision-making times. However, constructing a real IoT environment as a test bed for evaluating such techniques is costly and doesn’t provide a controllable environment for conducting repeatable experiments. To overcome this limitation, an open source simulator called iFogSim [5] is available. iFogSim enables the modeling and simulation of fog-computing environments for the evaluation of resource-management and scheduling policies across edge and cloud resources under multiple scenarios, based on their impact on latency, energy consumption, network congestion, and operational costs. It measures performance metrics and simulates edge devices, cloud datacenters, sensors, network links, data streams, and stream-processing applications.

IX. CHALLENGES IN FOG COMPUTING DEPLOYMENT

Realizing fog computing’s full potential presents several challenges including balancing load distribution between edge and cloud resources, API and service management and sharing, and SDN communications [6]. There are several other important examples.

A. Enabling Real-Time Analytics

In fog environments, resource management systems should be able to dynamically determine which analytics tasks are being pushed to which cloud or edge-based resource to minimize latency and maximize throughput. These systems also must consider other criteria such as various countries’ data privacy laws involving, for example, medical and financial information.

B. Programming Models and Architectures

Most stream- and data-processing frameworks, including Apache Storm and S4[3], don’t provide enough scalability and flexibility for fog and IoT environments because their architecture is based on static configurations. Fog environments require the ability to add and remove resources dynamically because processing nodes are generally mobile devices that frequently join and leave networks.

C. Security, Reliability and Fault Tolerance

Enforcing security in fog environments—which have multiple service providers and users, as well as distributed resources—is a key challenge. Designing and implementing authentication and authorization techniques that can work with multiple fog nodes that have different computing capacities is difficult. Public-key infrastructures and trusted execution environments are potential solutions. Users of fog deployments also must plan for the failure of individual sensors, networks, service platforms, and applications. To help with this, they could apply standards, such as the Stream Control Transmission Protocol, that deal with packet and event reliability in wireless sensor networks.

D. Power Consumption

Fog environments consist of many nodes. Thus, the computation is distributed and can be less energy efficient than in centralized cloud systems. Using efficient communications protocols such as CoAP, effective filtering and sampling techniques, and joint computing and network resource optimization can minimize energy consumption in fog environments.

X. USE OF FOG COMPUTING IN EMERGING TECHNOLOGIES

A. 5G Technologies

Fog computing focuses on serving customized location-based applications to mobile users. The Fog layers can be adapted by using the existing accessing networks, e.g., WiFi, or emerging 5G wireless technologies with a virtualized architecture.
B. Network Function Virtualization (NFV)

In contrast NFV which targets to enabled virtualized network functions inside network nodes, e.g., switches and routers, Fog computing aims at enabling virtualized location-based applications at the edge device and providing desirable services to localized mobile users.

C. Software-defined Networking (SDN)

The Fog computing, as the local surrogate of cloud, needs to synchronize frequently with cloud for data update and support. With a global network view, the cloud can manage the entire network using a SDN approach.

XI. CONCLUSION

Fog computing as a new paradigm or as made-up marketing hype, you’ll probably encounter the term over the next few years as the IoT gains traction. Fog computing takes some of the heavy lifting off regular cloud services by utilizing local resources for quicker and smoother processes, and whatever you want to call it, you can expect it to increase in importance as more objects become smart and connected. Fog computing will evolve with the rapid development in underlying IoT, edge devices, radio access techniques, SDN, NFV, VM and Mobile cloud. We think fog computing is promising but currently need joint efforts from underlying techniques to converged at “fog computing”.

REFERENCES