

Review on Fog Computing

Rajat Sethi

M. Tech. Student

Department of Computer Science & Engineering
Shri Mata Vaishno Devi University, J & K, 182320, India

Abstract— Fog Computing is a paradigm that extends the Cloud Computing services to the edge of the network. It provides a new category of assistance for users and applications. Major characteristics of Fog Computing are: a) Mobility, b) Geographical dispensation, c) Low latency, d) Large number of nodes, e) Prominent role of wireless access, f) Presence of real time & Streaming applications, g) Diversity, h) Local location awareness. This article elaborates the motivation and advantages of Fog computing, Fog computing as a platform for Internet of Things (IoT) & how it can minimize the attacks and provides security in cloud computing environment.

Key words: Cloud Computing, Fog Computing, Internet of Things, Mobility

I. INTRODUCTION

Fog computing, sometimes which is also termed as fogging, is a Platform in which some application services are controlled at the network edge devices (Which might contain mobile devices or other fog devices) in a data center and some application services are handled in a remote smart device in the cloud. The main aim of fog computing is to enhance effectiveness and reduce the amount of data that needs to be moved to the cloud for various purposes such as: storage, processing & manipulation [1]. In a fog computing environment, most of the processing takes place on a smart device (such as Smartphones etc.) or on the network on devices such as smart routers or gateway devices.

Fog Computing, a term coined by Professor Salvatore J. Stolfo, can be used with both large data structures and enormous cloud systems, making reference to the rising problems in gaining access to information accurately. This dispersed approach is growing in reputation because of the Internet of Things (IoT) and the enormous amount of data created by it. It is simply uneconomical to transfer all the data to the cloud for its processing it would simply waste a large amount of bandwidth; because doing so requires a large amount of bandwidth and it can reduce the performance of the overall network due to its both way communication. Latency is sometimes annoying if it is a part of a gaming application, delays in transmission of data can be life-threatening in some situations, which involve real time processing.

Term fog computing is also sometimes related with Cisco. "Cisco Fog Computing" is a name which is disclosed whereas "fog computing" is open to all the community. The word "fog" is used to express the idea that the immense advantages of cloud computing should be fetched closer to the data source. (In simple terms fog is a cloud that is closer to the users.)

II. EVOLUTION OF FOG COMPUTING

Cloud computing expanded its position and gained attention of both users and service providers as the most capable

computing paradigm in the recent times, which no other computing paradigms of the past has enjoyed [2]. Cloud computing makes computing resources such as memory, high performance processors and other computer hardware, application development platform and computer applications which are available to the users as services over the Internet. Diverse services which made available to customers in this manner are known as Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Figure 1 shows the various layers of cloud computing business architecture as how they are arranged on each other. The bottom two layers namely the virtualized hardware layer and the physical hardware layer provides the essential platform along with the required security and segregation for multiple systems to run simultaneously.

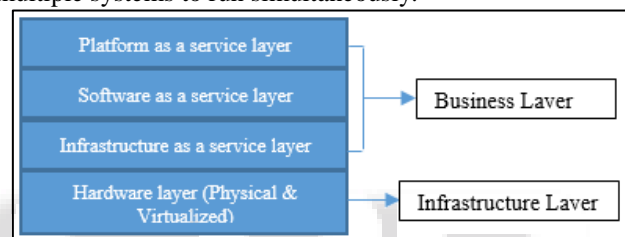


Fig. 1: Layers of Cloud Computing

Cloud computing provides many advantages to users compared to traditional purchase, own and run your own computing systems model. The key advantages of cloud computing over the traditional computing paradigm are the economic advantages and the elimination of computer systems administrative tasks and associated costs. Users can access the cloud services and pay for only the services accessed on a utility costing basis. Utilities such as electricity, water, gas and telephony are used by customers irrespective of the nature and place of service generation and pay only for the amount of services which are being received or being consumed. Similar to cloud computing services these are also priced on a time basis irrespective of how much of resources were used. As all the computing hardware and software is hosted in a remote data centre owned and operated by a service provider, the clients can only concentrate on their core business functions. Even the customers who are involved in computing related businesses such as software development, don't worry about purchasing their own software and hardware such as project management tools or development platform or managing them in house.

Cloud computing has many advantages, but it also suffers from certain shortcomings. These limitations are their necessity of high capacity (bandwidth) security and high latency, client access link. These limitations have heavy impacts on certain kinds of computing needs such as sensor networks and especially the emerging Internet of Things paradigm that envisages to have every device which exist over Internet. To overcome these restrictions of cloud computing and to meet the demands of emerging computing models and paradigms, new kind of cloud computing models

are currently being proposed by researchers. In this new model, the devices that respond to and process the client request are hosted either at the edge of the local network or very close to it rather than far away in an location which might be unknown somewhere in middle of the Internet cloud. This type of cloud computing model is given the name "Fog Computing". We present a journey to see how this new proposed model of cloud computing can eliminate or reduce the limitations of the current cloud computing model and respond to the changing demand of the users and emerging computing paradigms.

III. CLOUD VS. FOG

Point of Difference	Cloud Computing	Fog Computing
Location Awareness	No	Yes
Distribution(Geographical)	Centralized	Distributed
Latency	High	Low
Delay Jitter	High	Very Low
Connectivity	Leased Line	Wireless
Mobility Support	Limited	Supported
Real Time Applications	Supported	Supported
Number of server nodes	Few	Large
Security	Undefined	Can be defined
Distance Between Client & Server	Multiple hops	One hop
Attack on Data Enroute	High probability	Very Low probability
Place of processing	Done at cloud	Done at devices

Table 1: Cloud Computing Vs. Fog Computing

IV. RELATED WORK

The expression "Fog Computing" was first presented by the Cisco Systems as another model to encourage remote information exchange to dispersed gadgets in the Internet of Things (IoT) worldview. Cisco has characterized Fog Computing as a model that stretches out Cloud computing administrations to the edge of the system i.e. to the clients itself. Alike Cloud, Fog gives information, register, application, and capacity administrations to end-clients [6]. The recognizing Fog attributes are its closeness to end-clients, its thick geographic dispersion, and portability bolster. Administrations can be facilitated at even end gadgets, for example, set-top-boxes or get to focuses or organize edge. By doing so, Fog improves QoS, resulting in pompous user-experience. Fog Computing supports Internet of Everything (IoE) applications which might demand real-time latency (networks of sensors and actuators, industrial automation). Due to its wide spread geographic reach the Fog paradigm is well placed for real time analytics and real time big data. Fog supports data collection points which might be densely distributed, hence adding a new axis to the Big Data dimensions (variety, volume, and velocity).

The Internet of Things (IoT) speeds up awareness and response to events. Its transforming whole industries, including manufacturing, oil and gas, utilities, transportation, public safety, and local government. But the IoT requires a new kind of infrastructure. The cloud can't connect and analyse data from millions of different kinds of things spread

out over huge areas by itself. Capturing the power of the IoT requires a solution that can:

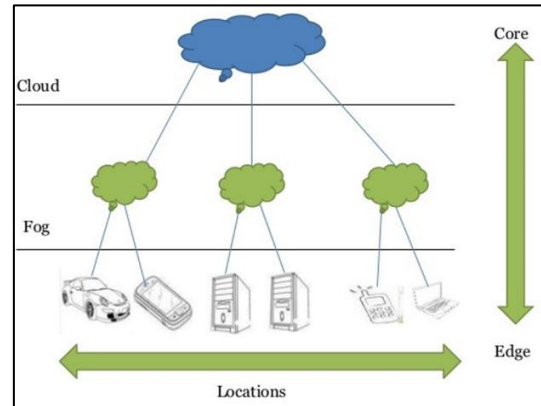


Fig. 2: Fog Architecture

- Connect new sorts of things to your system. Some of them may be in cruel situations. Others may impart utilizing modern conventions, not IP.
- Secure the things that produce data.
- Handle unprecedented variety, volume and velocity of data. Billions of devices which were previously disconnected are generating huge amount of data each day of the order of exabytes. Sending all of it to the cloud for analysis and storage is not practical. Plus, in the time it takes to send data to the cloud for analysis, the opportunity to act on it might be gone.

Cisco Fog computing solutions meet these requirements. They're part of the Cisco IoT System, a comprehensive set of products for deploying, accelerating value, and innovating with the Internet of Things. Cisco Fog computing solutions include everything you need to:

- Connect any kind of IoT device.
- Secure your IoT devices and protect the data they produce as it travels between the network edge and the cloud.
- Quickly develop and deploy fog applications.
- Guide information to the best place for examination: fog hubs or your data centre cloud stage. The choice of how time-sensitive the decision is and data-privacy requirements.
- Automating provision and simplified management of huge numbers of nodes spread out over large amount of areas.

V. ANALYSIS ON RELATED WORK

A. Platform for Internet of Things and Analytics

This section demonstrates the role Fog plays in three scenarios of interest: Connected Vehicle and Actuator Networks and Wireless Sensor.

1) Connected Vehicle (CV)

Connected Vehicle deployment creates a situation of availability and connections: vehicle to vehicle, vehicle to access points (Wi-Fi, 3G, LTE, roadside units [RSUs], Smart Traffic lights), and access points to access points. The Fog has various properties that make it the perfect stage to convey a rich menu of SCV benefits in infotainment, security, movement bolster, and investigation: geo-dissemination (all through urban communities and along streets), portability and area mindfulness, heterogeneity, low idleness, and support for constant between activities. The savvy movement light

hub (Smart traffic light) can stay in contact with various sensors, which may recognize the nearness of various substances on street like people on foot and bikers, and measures the separation and speed of moving toward vehicles. It can likewise associates with neighboring lights to facilitate the green movement wave if required. On the premise of this, smart light can sends cautioning signal data to the vehicles drawing nearer, and can alters its own particular cycle if required to counteract mishaps.

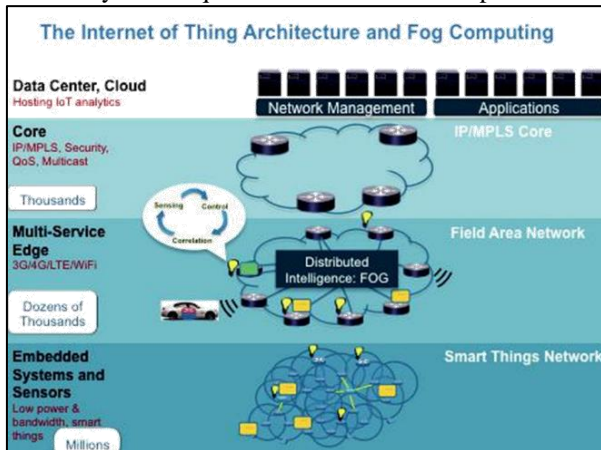


Fig. 3: Internet of Things and Fog Computing

Re-coordinating with Smart traffic lights through the orchestration layer. The data collected by the STLs is processed in order to perform real-time analysis. The data from these clusters of smart traffic lights is sent to the Cloud for global and long-term analysis.

B. Wireless Sensors Networks

The Wireless Sensor Nodes, nicknamed motes, were intended to work at low power with a specific end goal to stretch out battery life or to make energy collection attainable. A greater part of these Wireless Sensor Networks include a low data transfer capacity, little processing power, low energy, little memory motes, working as sources of a sink (collector), unidirectionally. Sensing the environment conditions, processing, and afterwards sending information to the static sink are the obligations of these sensor systems, for which the open source TinyOS2 is the standard working framework utilized in these situation. Motes have proved helpful in an assortment of situations to gather ecological information (moistness, temperature, measure of precipitation and so forth.).

Energy poor Wireless Sensor Networks progressed in a several directions: different sinks, mobile sinks, and portable sensors were proposed in progressive indication to meet necessities of new applications yet, they miss the mark if there should be an occurrence of detecting and tracking, but may require actuators keeping in mind the end goal to apply physical activities (open, close, move, center, target, even convey sensors). Actuators, which can control either a framework or the estimation process itself, convey new measurements to sensor systems.

The data flow is not unidirectional (from the sensors to the sink), but rather bi-directional (sensors to sink, and controller hub to actuators). In a subtler, yet huge way, it turns into a closed loop framework, in which the issues of stability and potential oscillatory conduct can't be disregarded. Latency and jitter are a critical worry in frameworks that require fast reaction.

The qualities of the Fog (closeness and location mindfulness, geographic appropriation, association) make it the reasonable stage to help both energy compelled Wireless Sensor Networks and WSANs.

C. Smart Grid

As we know Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization. Many applications require both Fog localization, and Cloud globalization, particularly for analytics and Big Data. It can be seen in the case of a smart grid. Fog collectors at the edge ingest the data generated by grid sensors and devices. Some of this data relates to protection and control loops that require real-time processing (from milliseconds to sub seconds). This tier of the Fog, designed for machine-to-machine (M2M) interaction, collects, process the data, and issues control commands to the actuators.

D. Focusing on Users at the Edge

Fog computing extends the cloud Internet by introducing an intermediary layer between mobile devices and cloud, aiming at the smooth, low-latency service delivery from the cloud to mobile. This accordingly leads to a three hierarchy Mobile-Fog-Cloud architecture as depicted in Fig. 4.

The intermediate Fog layer is composed of geo-distributed Fog servers which are deployed at the edge of networks, e.g., parks, bus terminals, shopping centres, etc. Each Fog server is similar to a light-weight cloud server, and is a highly virtualized computing system, equipped with the large data storage, processing and wireless communication facility. The role of Fog servers is to create a connection (bridging) between the mobile users and cloud. At one side, Fog servers directly communicate with the mobile users through single-hop wireless connections using the off-the-shelf wireless interfaces, such as Wi-Fi, Bluetooth. With the on-board compute facility and pre-cached contents, they can independently provide service applications to mobile users without assistances from cloud or Internet. On the other hand, the Fog servers can be connected to the cloud so as to leverage the rich functions and application tools of the cloud [4]. The next section describes some typical examples of Fog computing in details.

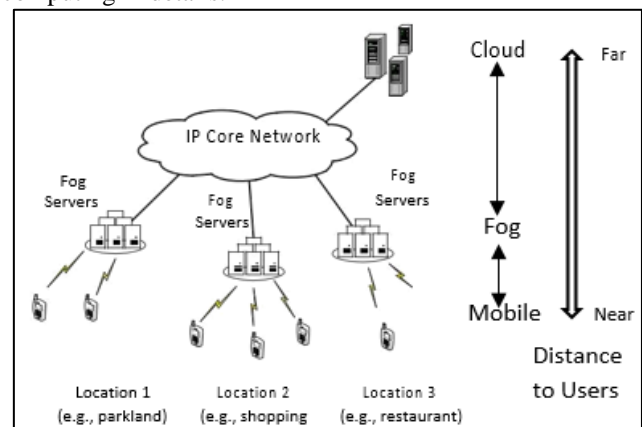


Fig. 4: Fog Computing Architecture [7]

Thus, the purpose of Fog computing is to place a handful of compute, storage and communication resources in the proximity of mobile users, and therefore to serve mobile users with the local short-distance high-rate connections. This

overcomes the drawback of cloud which is far from mobile users with elongated service delays. Therefore, the fog is interpreted as “the cloud close to the ground”.

The fog thus behaves as a surrogate of cloud or a private cloud at the user’s premises. This makes Fog servers to be more efficient and thus they can handle the localized computation requests. Therefore, Fog computing targets to deliver the localized and location-based service applications to mobile users. In what follows, some examples of Fog computing implementation from this perspective have been shown:

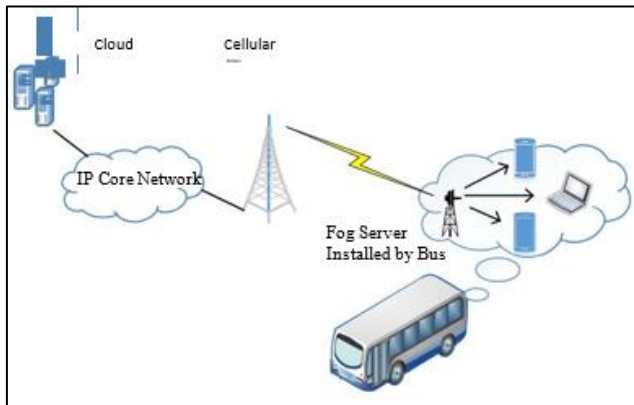


Fig. 5: On-board Fog computing system [7]

1) Shopping Centre

Assuming that a number of Fog servers are deployed inside a multi-floor shopping centre, which collectively form an integrated localized information system. The Fog servers at different locations can pre-cache location-related contents, such as the layout and ads of stores on a particular floor. The Fog servers can deliver engaged services including indoor navigation, ads distribution and feedback collections to mobile users through Wi-Fi.

2) Parkland

The Fog computing system can be deployed in the parkland to provide localized travel services. For instance, Fog servers can be deployed at the entrance and other important locations of the park. The Fog server at the entrance can cache information like park map, travel guide and local composition; other Fog servers at different locations inside the park can be incorporated with sensor networks for environment monitoring and provide navigation to travellers. By connecting the Fog servers to the park administration office and cloud, the Fog servers can be used as an information gateway to send timely alerts and notifications to travellers.

3) Inter-state Bus

Greyhound has launched “BLUE”, an on-board Fog computing system over inter-state buses for entertainment services. As outlined in Fig. 5, a Fog server can be deployed inside the bus and gives on-board video streaming, gaming and social networking services to explorers utilizing Wi-Fi. The on-board Fog server is associated with the cloud through cellular network systems to invigorate the pre-stored contents and can refresh application administrations. Utilizing its computing facility, the Fog server can likewise gather and process client’s information, for example, number of explorers and their criticisms, and reports to cloud.

4) Vehicular Fog Computing Networks

Fog computing can fill in at substantial scale arrange for confined content disseminations. Expecting that a store

introduces a Fog server at its parking area with the reason to distribute the store flyer. In step 1, the store transfers flyers to the Fog server by means of remote associations, and the Fog server circulates the flyers remotely to vehicles driving through its scope utilizing remote correspondences. With the vehicle moving to various areas, it can additionally spread the reserved flyers to different vehicles utilizing remote correspondences, as portrayed in step 2. In step 3, the flyers can likewise be recovered and stored at other Fog servers sent at various areas, e.g., transport stop, and further spread in the system.

VI. APPROACH FOR SECURING CLOUDS

The necessary idea is that we can boundary the reach of stolen information if we decrease the value of that stolen information to the attacker [5]. We can achieve this through a „preventive“ disinformation attack. We imagine that secure Cloud services can be implemented given two other security features:

A. Confusing the attacker with dummy data

We imagine that the combination of these two security features will provide unmatched levels of security for the Cloud. There are very less Cloud security method available that provides this level of security. We have useful these concepts to notice illegal data access to data stored on a local file system by masqueraders. One may see illegal access to Cloud data by an insider as the malicious act of a masquerader. Our trial results in a local file system setting show that combining both techniques can yield better recognition results, and our results advise that this approach may work in a Cloud computing environment, as it is proposed to the user as to be a local file system. In the following we analysis briefly some of the trial results achieved by using this approach to detect masquerade activity in a local file setting.

B. Module Description

- User Behavior Profiling
- Decoy documents
- Secure from dealer
- Block the nasty user
- Differentiate user

1) User profiling behavior module

In this component, admin will going to record log record of all users so that he can easily set working baseline for legal user. Admin monitor data access in the cloud and notice abnormal data access patterns User profiling will a well-known Technique that can be applied here to check how, when, and how much a client access their data in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's data is experience. This method of behavior based security will regularly use in scheme uncovering applications. Such profiles would obviously include volumetric information, how many documents are typically read and how often. We check for abnormal search behaviours that display deviations from the user baseline the connection of search actions difference identification with trap-based decoy files should provide stronger confirmation of malfeasance, and therefore recover a detector's exactness.

2) *Decoy documents module*

A different approach for securing data in the cloud using nasty decoy technology can be suggested. We can monitor all the data access in the cloud and can try to sense irregular access patterns. We can initiate a disinformation attack by persisting large amounts of decoy information to the attacker. We use this technology to begin disinformation attacks against malicious insiders, preventing them from distinguishing the valid aware customer data from bogus useless.

3) *Secure from dealer*

If legal user does not want to give access to the dealer so we can protect that access from dealer. In previous system, dealer can directly access the own or corporate data which is stored on to the cloud. There is no any situation for security of information which is stored on to the cloud. So in our planned system, all the data which is stored on the cloud is confined, it is totally depend on the user to assign access agreement to its data. In case, if dealer want to access the information which is stored on the cloud, it has to gain the private key of that particular user to decrypt the information and this method is get finished via safe key replace algorithm.

4) *Block the nasty user*

If we will found any nasty user from his user profile behavior we can directly block that user or we can ask a security questions. For e.g. User fails to login successively, animal search attack, uploads files which contains .exe files with in it etc. so, all this record of the all user will maintained in the user profiling activities, and as soon as the system detects any nasty activities, it directly block that user in case, if any allowed user try to search any other widely stored files then according to our situation our system blocks that client, but during blocking system asks security questions to that user to avoid accepted user jamming.

5) *Differentiate user*

We can differentiate user by using contact rights. We can allot human rights at the time of uploading. For example low user have only read permissions, high user has all permissions like modification. By categorizing different users on the cloud, we obtain fair and flexible control on managing resources on the cloud.

VII. VERDICT

Fog is different from cloud because of the following reasons:

- Topology in use
- Bounded Jitter & Latency
- Connectivity

Instead of traditional topologies which are used in data centers, fog computing makes use of topologies which are more rigorous as fog computing has to deal with a huge number of edge devices which are usually mobile. Thus topologies used with fog computing makes use of ad-hoc topologies. As we know that modern day computing thrives on Big Data, thus fog computing network topology has to be capable of handling large amount of data as well as it should also be reliable at the same instant. In short we can say that the topology should have following features:

- Heterogeneous interconnectivity.
- Dynamic Bandwidth.
- Latency & Reliability.
- Amorphic

Fog Computing has to deal with connecting things and by things we mean different devices like the edge devices and the devices which might be working at the backend in actual cloud, which is not an issue with a traditional cloud system as all the processing in cloud computing is done at the cloud itself but here in case of fog computing the processing might take place at different locations which can be the edge devices, the intermediate fog devices or at the back end at cloud itself thus there needs to be a proper setup of how these things(devices) could be connected with each other. In order to carry out the process we can have dedicated drivers at different interfaces within the fog network.

a) How Fog computing can help in different scenarios:

- The cloud faces critical latency requirements and fog can help in this scenario because fog has fewer network hops and lower focused loads.
- Cloud faces data mobility issue as there is a lot of data that is to be transferred between systems and actual users and in fog as we know that data is located at optimal depth thus data mobility can be reduced to a great extent. Local caches can be used at devices in order to provide data rich mobility.
- Also as we know that certain data cannot be sent to certain geographical locations (like sensitive government or military data) thus use of cloud computing becomes inappropriate, now this is where fog computing comes in picture, in such scenarios we can localize intelligence to fog servers which might lie in the geographical boundary of the data.
- As we know that Fog provides local processing of data therefore bandwidth requirement to perform a task is as compared to cloud is less and corresponding network load is less.

b) Depending upon the application, some attributes of fog can be as:

- Scalability: It can be achieved by making use of techniques like virtualization, Modularity, Orchestration etc.
- Security: Strong security is very essential for fog computing devices.
- Programmability: Fog is highly programmable at multiple levels. It has multiple application support. It has versatility in operating environment.
- Real Time Features: Fog provides real time features like deterministic timing capability. It supports different mixes of computation, networking & storage.

VIII. CONCLUSION

Fog computing gives the cloud a buddy to deal with the two Exabyte of information created day by day from the Internet of Things (IOT). Preparing information nearer to where it is delivered and required comprehends the difficulties of detonating information volume, assortment, and speed.

Fog computing quickens awareness and reaction to occasions by dispensing a round trip to the cloud for investigation. It maintains a strategic distance from the requirement for exorbitant data transmission increases by offloading gigabytes of system activity from the center system. It likewise ensures sensitive IoT information stays inside organization walls and is processed inside it. Fog Computing, hierarchical and circulated platform for service

conveyance comprising of computation, storage, and system assets. We analyzed key parts of Fog computing, and how Fog supplements and broadens Cloud computing. We took a gander to utilize cases that spurred the requirement for Fog, underlining Fog's significance to a few verticals inside IoT and Big Data space. We additionally gave an abnormal state depiction of Fog's product design, featuring the diverse innovation segments important to accomplish the Fog vision.

REFERENCES

- [1] Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the 1st edn. of the MCC workshop on Mobile cloud computing (2012)
- [2] Cloud Computing for Dummies
- [3] Archer, Jerry, et al. "Top threats to cloud computing v1.0." Cloud Security Alliance (2010).
- [4] Zhu, Jiang, et al. "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture." Service Oriented System Engineering (SOSE), 2013 IEEE.
- [5] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012
- [6] Bar-Magen Numhauser, Jonathan (2013). Fog Computing introduction to a New Cloud Evolution. *Escrituras silenciadas: paisaje como historiografía*. Spain: University of Alcala. pp. 111–126. ISBN 978-84-15595-84-7.
- [7] Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L., 2015. Fog computing: Focusing on mobile users at the edge. arXiv preprint arXiv:1502.01815.