**Fog Computing: A Survey**

Saloni Mohan

Sammeta Sudheer

Department of Computer Engineering

San Jose State University

Lalini Wudali

Sahitya Mullapudi

Department of Computer Engineering

San Jose State University

***Abstract****:* As the future looks towards IoTs (Internet of Things), there is a possibility of exponential increase in data being generated by various devices in the network. This humongous amount of data along with the geographical distribution of IoTs is sure to have a cascading effect on network latency. To address this issue, a new paradigm called ‘Fog Computing’ has been introduced. Fog Computing moves compute, storage, communication, control and decision making closer to the network edge where data is being generated. In this document, we shall discuss the advantages, challenges, architecture and applications of Fog computing as well as compare and contrast Fog computing with other existing computing paradigms.

1. **Introduction**

The past few years, there has been an explosion in the number of mobile devices, computers, tablets, wearable devices and more connecting to the internet. The advent of Internet of Things (IoT) devices/sensors has added another dimension to this exponential growth in internet traffic. The surge in demand for high quality mobile on-demand services has led to the Fog Computing paradigm. Fog computing is a concept introduced by Cisco in 2012 [1], [2] to address these challenges. Fog computing places light-weight Fog Cloud servers or nodes in proximity to IoT devices and mobile users which can then serve as direct localized sites to provide customized location-aware services.

***A. Understanding Fog Computing***

Fog computing is an extended Cloud computing distributed paradigm for managing distributed and virtualized environments that extend the Cloud based services like compute, storage and network closer to the devices themselves by introducing an intermediate layer between the Cloud datacenters and the mobile/IoT devices. The geographically centralized nature of Cloud computing has led to its inability to cope up with the increasing processing and storage demands in a timely manner. This has led to high network traffic and increased latency which cannot be handled efficiently by existing communication and computing infrastructure causing clients to experience poor Quality of Service (QoS). By decentralizing the computations away from the cloud systems towards the edge of the network and closer to the user, there is reduced load on the Cloud servers. Fog computing uses the intermediate logical layer to perform computing and processing, thereby allowing for more efficient data processing and faster turnaround in the same timeframe.

**B. Definition of Fog Computing**

Fog computing is a model to complement the cloud for decentralizing the concentration of computing resources (for example, servers, storage, applications and services) in data centers towards users for improving the quality of service and their experience [2].

Fog computing model uses the computing resources available on intermediate devices like routers or switches [2]. In this model, additional resources can also be made part of the network devices which are closer to the clients/users. These additional devices increase computing strength midway between the Cloud and the end user devices facilitate performance and improve latency for applications with requirements of low latency with a wide geographical spread.

This helps in the optimization of certain types of applications like gaming, video streaming etc. that communicate large amounts of data and are user driven. A typical example is that of a Cloud application such as an online game that many users can be playing at the same time by connecting to the Cloud server via various end user devices which could range from tablets, cellphones to laptops. If the users playing this game are moving from their location constantly, their coordinates will need to be updated accordingly [2]. This is an example of an application that sends and receives large amounts of data where high latency can affect performance. Such applications can benefit from the game server’s proximity to the player as per the Fog computing paradigm.

**C. Motivation for Fog Computing**

Integrating mobile device applications into the Cloud has proven to be more challenging than was expected, which led to the introduction of the concept of Fog computing. Some of these challenges include:

***Limited Adaptability of current cloud services:***

Mobile applications are quite diverse; while they need to explicitly be location aware, another prominent aspect of these applications is that they additionally need to be environmentally aware. The billions of requests coming from geographically dispersed mobile users cannot be managed efficiently by the cloud servers as per the current centralized design. In addition, current mobile devices and tablets have limited storage as well as computing resources placing the burden of the entire job on to the cloud. Cloud services are not able to adapt to the quick and agile real-time response expected by these mobile applications. This dependency on the Cloud server for sensing and data processing needs has now extended to various other devices including wearable devices like Apple watch, Fit Bit, Google glasses and the like [6].

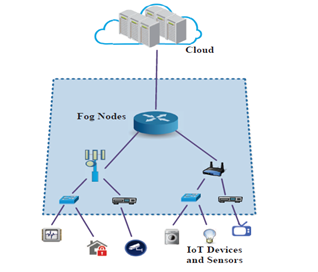
***Mobile Bandwidth:***

Mobile and real time applications need high computing resources and need large amounts of data to be passed to and from the cloud at high speeds. High cost of bandwidth is preventing mobile users to run applications that are resource intensive with satisfying results. Applications like real-time games e.g. Poke Mon send and receive large amounts of data and this also changes based on the location of the end user [2]. This model of sending and receiving data from the centralized cloud does not work efficiently at such high cost of broadband service.

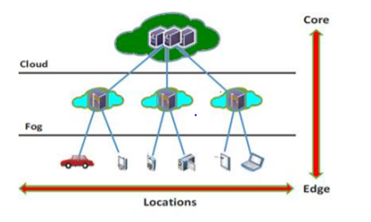
***Low latency requirements:***

New real time applications especially in the fields of health monitoring and response and emergency systems that are highly sensitive to the speed at which services are provided to consumers, are getting hit with large network delays caused by several billions of data being transmitted and received in the same pathways to the cloud data centers causing network congestion. This is causing serious performance implications that are calling for new innovative solutions to the inherently low latency requirements of such time sensitive applications.

**Fog computing infrastructure**

Fog computing infrastructure comprises of devices like routers, switches and other infrastructure like cellular base stations that are used to route network traffic between the edge devices and the cloud and these are much usually placed closer to the end user devices than the Cloud servers as indicated by Figure1.These intermediate devices are also equipped with not only computing capabilities, but also with other Cloud provided services like networking and storage and can be used to support the execution of applications. Fog computing can use these intermediate network devices to deliver large geographical Cloud-based service distribution model.

**Figure1: Fog Computing Environment [1]**



**Figure2: Cloud and Fog Comparison**

**D. Main characteristics of Fog Computing**

As Fog computing is not a completely different paradigm from Cloud computing, but an extension of Cloud Computing concept, it shares many of the characteristics of Cloud computing viz. on-demand services, rapid elasticity, scalability, metering and monitoring etc. However, Fog computing will have to have additional characteristics that are specific only to Fog computing.

***Widespread geographical distribution:***

Unlike Cloud servers that are located in specific central locations and serve the entire user base, Fog computing is characterized by multiple Fog servers or nodes that are dense (multiple nodes with high density) and geographically closer to the user base that they serve.

***Mobility access and location awareness:***

Support for location awareness and mobility access is one of the distinguishing characteristics of Fog computing. In a typical Cloud computing environment, the servers are stationed in a centralized place and it serves as a repository for all of the information flowing from the end users. Although there may be some form of decentralization by assigning servers in the closest geographical area, this is still far from the location awareness and support needed by mobile applications. By having the server nodes reside closer to the user devices being served and thereby providing local customized services for these applications, Fog computing provides location awareness and greater mobility support.

***Vertical Scaling****:*

In traditional Cloud data centers, rapid elasticity is achieved by scaling resources horizontally. Horizontal scaling is the Cloud service provider’s ability to add multiple Virtual Machines (VMs) or multiple software processes on-demand based on the increasing requests made by the Cloud clients during heavy load. However, in Fog Computing, resources need to be scaled vertically [2]. This means that additional layers of devices at different levels of hierarchy need to be added which will result in the reduction of amount of traffic that passes from the end user devices to the Cloud, thereby helping to reduce the communication latency. Although vertical scaling is seen as a standard characteristic of Fog computing, it is not as easy to implement as horizontal scaling. Vertical scaling is seen as comparatively more challenging due to the fact that its resources are not usually as tightly paired as opposed to cloud servers in various data centers. Additionally, issues can arise regarding ownership of vertical resources.

***Heterogeneity of devices:***

While homogeneity is often a more common aspect of cloud computing resources, heterogeneity plays a fairly prominent role in fog computing. Virtual Machines (VM) often correspond to the same set of physical servers, thereby providing a uniform environment to the clients requesting the cloud services. However, the intermediate resources that are part of a Fog computing system like sensors, routers, switches and base stations are a diverse mix of machines dotted across the Fog clouding landscape. These resources could be equipped with varying degrees of computing and performance improvement capabilities and serve as the intermediate server points for data going from the end users to the cloud data center. This methodology of using both vertical and horizontal scaling with multiple heterogeneous resources is one of the main characteristics of Fog computing [1], [2], [5].

***Volume and diversity of devices:***

Due to the increasing number of devices and end users connecting to the Cloud data center, there will be a need to increase the nodes in the Fog computing nodes to meet the service demands. Fog computing needs to not only scale vertically, but also continue to scale horizontally as the traditional Cloud services thereby increasing the network of devices and resources available and visible in the network [2]. Due to the heterogeneity and this multi-dimensional scaling, volumes of devices are going to be in the order of magnitude of billions, creating very complex structures that will be challenging to control and regulate.

***Transparency and Visibility:***

The Cloud computing model includes many resources such as storage, computing power and applications or tools that are visible to end users via a user interface over the internet. These offerings often have a wide range and new services are offered in the market every day to increase competitive advantage in the evolving marketplace. This particular feature of Cloud computing is particularly hard to implement in Fog computing since there is a heterogeneous mix of resource types which form the backbone of the network of nodes in a Fog cloud environment. Ensuring these nodes are visible to users and accessible is a daunting task, not to speak of security risks involved with such an endeavor. In addition to the resources being varied, there is also the issue of the ownership of these resources, which are distributed across several entities. Challenges like security and privacy of data need to be addressed first if fog computing devices are to become a reality in servicing consumers and end users. In additional to addressing these challenges or even mitigating the risks associated with these challenges, entities or companies need to work together to develop benchmarks and standards that can be widely adopted to minimize risks associated with usage of the various devices in the Fog computing network.

**E. Advantages of Fog Computing**

In this section, we will explicitly list the advantages associated with Fog computing.

***Reduction of network traffic****:*

As per recent estimates, the number of devices connected to the internet could go close to 50 billion in less than five years [5]. All of these devices including tablets, mobile devices and wearable devices are not only generating large amounts of data, but are also sending and receiving vast amounts of data which clearly demonstrates the need to reduce this huge network traffic across the networks to central cloud servers. Some of the traffic sensors or other sensors in the Internet of things (IoT) devices send data by the second. The biggest benefit of fog computing is the presence of intermediate resources or devices which are situated way closer to the devices generating this data which causes a steep reduction in the amount of network traffic being sent between the end user device and the cloud via the internet [3], [5] .

***Ideal for IoT devices****:*

In Internet of things (IoT) applications, most of the data pertains to the device itself and needs to be processed quickly and in the context of the device and its surroundings and the need to send the data to the centralized cloud servers for analysis is minimal or non-existent. Citing the example of a smart connected bus which needs to be aware of events happening a few thousand feet around it, there is no requirement to process this data outside of that geographical location and it is also way faster to process it closer to where the data is being gathered [5]. A second example is that of a mobile emergency response vehicle that needs to gather data of any critical accidents around its vicinity and this data processing is ideally done close to the device itself, e.g. in a router or local Fog server as opposed to a Cloud server located several thousands of miles away in that particular state or country.

***Dense geographical distribution****:*

Fog computing creates edge networks which sits at various points to extend the direct cloud service. Fog clouds can have dense, geographically isolated infrastructure that can help handle and interpret big data faster. Fog server administrators can help support location-based mobility demands of various devices by allowing access to the needed Fog servers, but limiting access to the rest of the network.

***Great support for mobility****:*

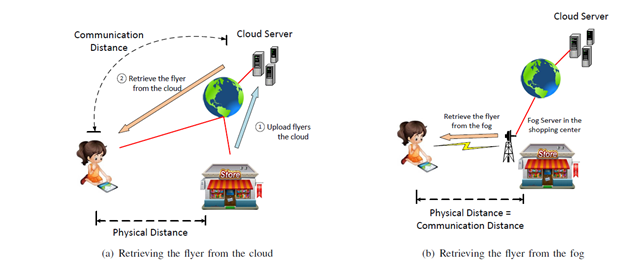
There is a tremendous increase in the amount of data and devices especially due to the explosion in devices connecting wirelessly. A fog system is equipped to handle this large data and information and provides a better and faster way to access and analyze the data.

***Low latency****:*

Real-time applications need processing of data to be performed almost instantly. Some of the examples of such applications are mobile games, drone applications, cloud robotics etc. Such applications depend on the data collected by the sensors on the location of the device and their geographical location, the obstacles in the path and depend a lot on the feedback of the control system. If such a system were to reside in the cloud, the transfer of such location specific data will be quite slow and not meet the specifications required by the application. By moving the processing requirements for such a control system very close to the drone itself as per the Fog computing principles, there can be a quick turnaround time for data processing thereby making the real-time response satisfactory and meeting the application requirements [5], [6].

***Scalability:***

Although the Cloud computing systems claim infinite elasticity and scalability, bottlenecks are bound to arise if the data generated by the 50 million mobile devices are all passed to the centralized cloud server. By de-centralizing data processing closer to the data source and having multiple such intermediate devices, the scalability issues can be addressed or mitigated to a large extent [5].



**Figure 3: Example of Fog Cloud [3]**

**F. Understanding of Fog Cloud Computing**

The fog computing ecosystem comprises of the user

device layer at the edge of the network, the intermediate Fog server layer and the cloud server which is the final tier in the multi-tier hierarchy. The different Fog nodes which

could be devices such as gateways, routers and base stations that are equipped with additional storage and computing powers. Fog cloud is the term referring to these devices in the intermediate layer. Fog cloud is composed of geographically distributed server nodes that could be deployed very close to the user devices, e.g parks, shopping malls, bus terminals etc. A Fog server achieves truly geographically distributed cloud computing since a huge number of nodes are operating at the edge of the network and are being used for their computing and storage capabilities that would normally not be used for this purpose. Fog servers can be adapted from existing network components by upgrading the computing and storage resources. A Fog server can exist at a static location such as inside a restaurant or shopping mall [3]. The role of the Fog cloud is to act as a bridge between mobile and the cloud. Fog servers can independently provide services to mobile users in its wireless coverage, and also independently communicate to the cloud over internet as needed.

Fog cloud could consist of the following types of nodes [2]:

**Traffic routing nodes:** These are switches or routers that route the data being sent from the end user devices, which normally do not process or store the data or perform computational operations.

**II. Fog Cloud Classification**

***A. Classification based on nodal collaboration***

In this chapter, we try to classify Fog Clouds based on nodal collaboration [1].

1. Cluster
2. Peer to Peer
3. Master – Slave

**Cluster**

Fog nodes (servers, switches, routers, base stations etc.) at the edge of the network can collaborate with each other to maintain an execution environment by forming into groups among themselves. Fog clusters can be formed based on homogeneity of nodes and location or functional specifications of the nodes.

In Fog clusters, the combined capacity of the nodes can be used towards a single processing or computational task if necessary. Clusters can be either static or dynamic. Static clusters cannot provide scalability whereas forming clusters dynamically might heavily depend on availability. Vehicular Fog Computing (VFC) uses cluster model [25].

**Peer to Peer**

Peer to peer network mechanism is commonly used in Fog cloud computing. Peer nodes are user devices or nodes that have spare computational services and are made available in network [2]. In peer to peer collaboration, one node’s output becomes another node’s input. Due to this process, freeing of nodes will not be an issue.

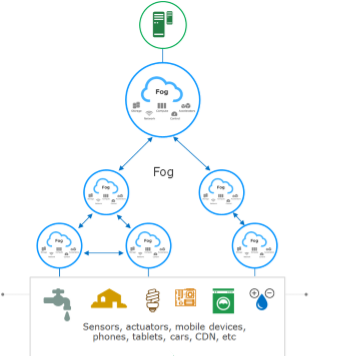
**Master – Slave**

In Master – Slave based collaboration, master node controls load processing, resource management, functionalities of the underlying slave nodes [1]. Slave nodes are relatively simple compared to master nodes [26]. Master nodes usually keep track of available capacity in the slave nodes. The drawback of this type of nodal collaboration is due to the decomposition of functions among the slave nodes, there will be high communication between master and slave nodes which requires high bandwidth [1].

***B. Classification of Fog based on deployment models***

To address different domain scenarios various combinations of fog and cloud models are deployed [24]. Fog elements in the model may consist of cluster of fog nodes or a mesh of peer fog nodes. Fog based on deployment models may be classified into four types.

a) A deployment model where Fog is independent of cloud. In this model, all the data collection and processing is done at fog elements. This model may be applicable where cloud infrastructure is not available or where utmost security is required. Figure4 illustrates the cloud independent Fog deployment model [24].

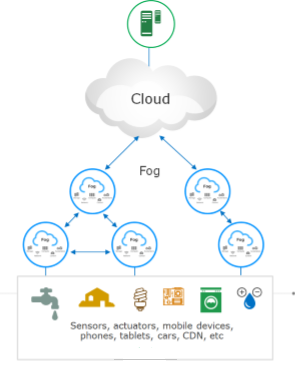
**b)** Figure5 illustrates the deployment model where fog and cloud share the tasks. Information related to decision making is processed at cloud. All the operation centric data processing and

**Figure4: Fog deployment model**

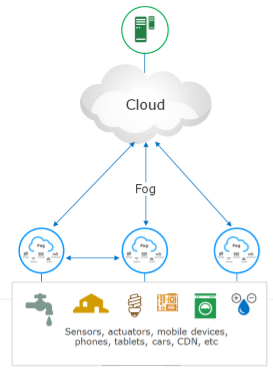
computing is done at the fog elements nearer to the edge network. Examples include commercial building monitoring and solar panel monitoring [24].

**c)** This model also is a combination of both fog and cloud infrastructure. But here, fog is used only for time sensitive data or information processing and computing. The operational and business related processing is done at cloud as illustrated in Figure6. Examples include mobile network acceleration [24].

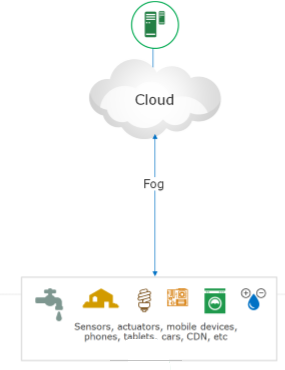
**d)** In this model fog nodes play a very minor role at the device layer. Monitoring and safety related control functions are executed in the Fog layer. All the information is processed at the cloud. This model might be deployed where building a fog infrastructure might not be feasible. Figure7 illustrates this model. Examples include remote weather stations [24].



**Figure5: Fog deployment model**



**Figure6: Fog deployment model**



**Figure7: Fog deployment model**

***C. Classification of Fog based on service models***

Cisco is the one who coined the term ‘Fog’ and is also a pioneer in Fog cloud technologies. In this section, we include Cisco development model of Fog. Cisco classified fog cloud service models similar to that of traditional cloud [23]. Fog service model has

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

**IaaS**: Host applications on fog nodes. Fog applications should be able to communicate with IoT devices that use any protocol. Fog applications can also send data to cloud.

**PaaS**: This system facilitates development and deployment of applications. Fog applications need to communicate with heterogeneous devices. Developing different applications for different types of IoTs is not possible. So, device abstraction must be followed. Fog nodes can also support different programming languages.

**SaaS:** This offers MaaS (Machine as a Service) [23]. The services can be managed from the fog.

**III. Fog Cloud Services**

In this chapter, we discuss various services provided by Fog cloud.

1. Network Services
2. Storage
3. Improved Performance
4. Security

***Network services***

The days of network services as connectivity between devices are gone. These days network services include storage, computation and connectivity which is key to fog architecture. Providing intelligence to network nodes increases the hardware infrastructure that is available which is so far left untapped. Any hardware like switches, routers, surveillance cameras can be used as fog node.

The fog cloud along with performing the traditional connectivity services can also provide storage and computation services depending on the nodes involved in the network. As there are heterogeneous devices in a fog network, fog cloud can be used by heterogeneous devices. Fog is also a geographically distributed architecture rather than centralized at some remote location [7].

***Security***

Providing security for data remains major problem for the cloud providers. The data encryption and user access control standards followed failed from time to time for reasons including insider attacks and faulty implementations [22]. In fog scenario, data is kept in the network rather than sending the data to centralized servers. But the main issue in fog might be that the authentication required at several levels of the fog network. To solve this issue, encryption algorithms can be used.

A proposal of providing decoy technology to solve the data theft and data attack issues is particularly interesting [10], [11]. Combining user profiling and decoy technology can provide significant improvement in the security at the fog nodes. If user access is abnormal, the cloud could ask a series of questions. If the user answers are correct to some extent, the cloud sends the actual document or else the cloud sends a decoy document which resembles the actual document but does not contain legitimate data.

By combining the encryption technologies, strong user access control and decoy technology with user profiling, fog offers improved security than traditional cloud technologies. Though all the above-mentioned features can be taken care of at traditional cloud technologies, the number of requests and data transfers required to achieve the security goal increases latency. While in fog cloud, as the data resides at the network edge, latency would not be an issue. For physical security, as traditional network is mostly accessible, surveillance solutions can be used [23].

***Improved performance***

The addition of computing and storage capabilities to the network devices in the fog architecture helps improve performance of real time applications. In a traditional cloud computing environment, with the increase in mobile devices and IoTs, data transfers and data requests give raise to number of TCP Connections testing the bandwidth of the network. This problem is set to accelerate in the future.

In fog architecture, the gateways or routers can act as web cache with their local context awareness. By analyzing the traffic in the local area, the routers can cache data for which most TCP requests are being generated. This helps to reduce the stress on bandwidth from fog to cloud data centers and also helps reduce latency. With the decrease in number of data requests, the data centers can allocate the processing time to more resources.

For smart applications like sensor based applications, rather than sending data from all the virtual sensors to cloud data centers for processing, with the computing capability at the fog level, the fog nodes could compute the data at local network level and then send the composite data to cloud data centers for further analysis. This decrease the amount of data connections to the cloud data centers exponentially [9].

***Storage***

Fog provides storage services with the help of network devices that have storage capacity [8]. Using Containers which operate as virtualization, storage is provided by fog cloud. Fog is ideal for applications which require just temporary storage. Real time applications like gaming which computes scores of player at every level, need not store the player’s score data once the user moves to next level. For these applications, fog can temporarily store data and after that the data can be erased. For time sensitive applications, data is collected and processed and more meaningful data is generated. Once the data is moved to cloud, the data at Fog nodes is deleted [7].

**COMPARISON OF CLOUD AND FOG COMPUTING**:

Although the concept of Fog computing is very much similar to cloud computing, we can show the difference between these two close concepts by evaluating a few key parameters. Table 1 summarizes the advantages of Fog Computing over Conventional Cloud Computing [3].

|  |  |  |
| --- | --- | --- |
| PARAMETERS | FOG COMPUTING | CLOUD COMPUTING |
| Target users | Mobile users, IoT end devices | General internet users |
| Hardware | Limited storage and compute capabilities (limited by the router, switches etc.) | Unlimited storage and compute resources (scalable) |
| Distance from user | Physically located much closer to end user devices requesting the service/data | Can be located very far away from the service requester |
| Server nodes location | At the edge of the network | Within the Internet |
| Latency | Low | High |
| Delay | Low | High |
| Geographical distribution | Dense and Distributed | Centralized |
| Number of server nodes | Large | Few |
| Mobility | Supported | Limited support |
| Location awareness | Yes | No |
| Security | More secure, Can be defined | Less secure, Undefined |
| Attacks on data en route | Very low probability | High probability |
| Environment | Fog servers could be anywhere in the closest network hub from the end user devices e.g. malls, streets, malls etc. | Cloud data centers are typically centralized in huge warehouse like structures |
| Service Providers | Hubs could be centralized or distributed by local Telecom provider or business owners | Centralized and maintained by companies like Amazon, Microsoft etc. |
| Storage | Less to none storage provided | Large storage considered infinite |

**Table1: Comparison between Fog Computing and cloud Computing**

|  |  |
| --- | --- |
| **Fog Computing** | **Edge Computing** |
| Large computing resources but less than cloud | Limited Computational resources |
| Fog can provide PaaS and SaaS | Edge does not provide PaaS and SaaS |
| Fog has a hierarchal and flat architecture with several layers forming a network | Edge computing relies on separate nodes that do not form a network |
| Fog is inclusive of cloud | Edge excludes the cloud |
| Fog provides less to none storage | Edge does not provide storage |
| Fog computing pushes intelligence/ processing capabilities to local area network that is processing data at fog node | Edge computing pushes processing capabilities to the devices |

**Table2: Comparison between Fog Computing and Edge Computing**

**IV. Fog Cloud Infrastructure**

One of the key attribute of fog computing is to distribute services closer to end devices or edge of the network, and anywhere along the continuum between cloud and things. In order to achieve this, we need to make the existing network elements more intelligent and more powerful. In addition to this, if data is going to be computed and stored at various points between two network end points. The fog infrastructure comprises the following network elements.

**Fog Servers:** These servers are similar to Cloud servers and possess computing, storage and networking capabilities but in micro size when

compared to cloud servers. In contrast to cloud, these are distributed across different geographical locations.

**Networking Devices:** These devices are the same that are present in normal network. They include gateways, switches, routers and do the same job as they do in regular computer network. In a fog network, these are equipped with additional processors and memory storage capabilities.

**Cloudlets:** These exist in midway between edge devices and cloud servers. These are virtualized and handle multiple end devices simultaneously.

Base Stations: These are regular base stations which are seen in wireless networks. In fog environment, they are provided with computing and storage capacities.

**Vehicles:** These are edge devices which might be mobile or immobile but have computational capabilities and can communicate with other vehicles directly. As they can be mobile, they provide a distributed environment.

**A. Fog Computing Platform**

***1) Characterization of Fog Computing [5]:***

Figure 8 shows the components of fog computing platform. Fog Computing can be viewed as an extension of the Cloud Computing with the key differentiation being the place where computing and storage happens. The network infrastructure of Fog computing has the following characteristics.

**Latency**: One of the primary motivating factor for the Fog Computing is the requirement of low latency by many time critical applications.

**Generality**: Fog Nodes are deployed in different forms in different environments. They should be able to support and work seamlessly while establishing a communication between disparate networks. Moreover, we need to provide abstraction to other layers. This can be achieved by using APIs in accordance with existing protocols.

**Efficiency**: The resources and energy at the disposal of fog nodes should be used efficiently. This is because most of the fog nodes are very limited in terms of computing power and storage capabilities and also most of the edge devices are battery powered where the rate of consumption of energy becomes very critical [27].

***2) Challenges***

It is difficult to design a fog computing platform having the characteristics mentioned above. Below are the list one might encounter while designing a fog computing platform.

**1.Choice of Virtualization Technology**: We need isolated environments for fog computing at the nodes. This is achieved by virtualization. So, a decision must be made - whether to go by hypervisor or container. Hypervisor offers more flexibility when compared to container virtualization.

**2. Fight with Latency**: Fog computing is aimed at time-sensitive applications. So, there cannot be much delay as this would have an adverse impact on user experience. The following measures can be taken to bring in the latency in fog computing.

a. Data aggregation: If data aggregation is not finished before data processing, there can be a delay due to the geo distributed nature of fog computing.

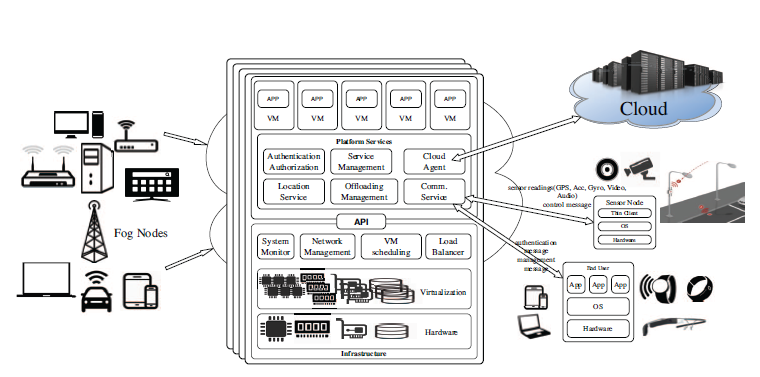
This can be reduced by applying data partitioning/filtering and distributing the computation to reduce load on higher layers.

b. Resource Provisioning: As the fog nodes possess very limited resources, there might be scenarios where resources cannot be provided to some tasks. For this, we need to schedule the processing of tasks based on priority and mobility model.

c. Node Mobility, churn and failure: System monitor and location service provides the information needed to develop the risk mitigation strategies and make the computing resilient.

**3.Network Management**: The network management will be difficult for fog computing unless we make efficient use of SDN and NFV techniques. We need to redesign not only the south bound and north bound but also east-west bound API as well which should be done carefully to meet the goals of latency and efficiency.

**4.Security and Privacy**: As we have computation and storage all over the network, security is of paramount importance at every fog node. To provide this, we need to have access control and intrusion detection systems all through the network.

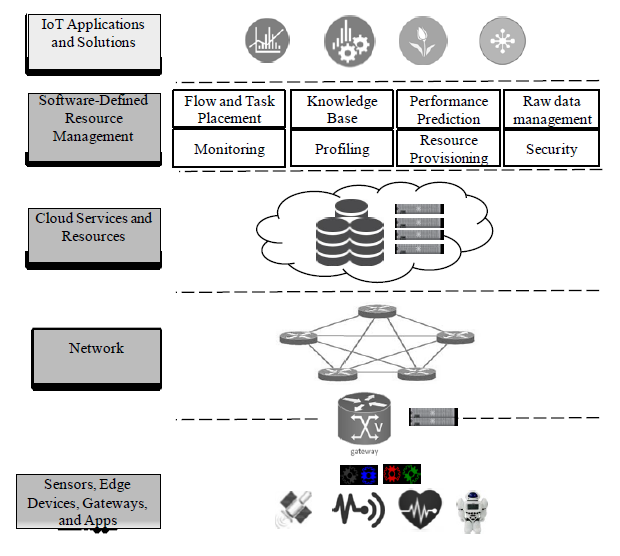


**Figure8: Components of Fog Computing Platform.**

**B. Fog Cloud Architecture**

Figure 9 shows a reference architecture for fog computing. On one end, we have end devices such as sensors, actuators, edge devices. This can include applications on end device which helps for the efficient functioning of fog computing. All these devices and apps use the services of network layer to communicate among themselves and to the higher layers. Cloud services and resources layer helps the management of resources and computing the tasks, whose outcome is passed onto the cloud or to the end devices. Software Defined Resource Management layer helps the management of infrastructure by allocating resources, monitoring the network and providing security. The topmost layer has the IoT applications and solutions which take the leverage of fog computing to provide services to end users.

Going into the details of Software Defined Resource Management layer, the main purpose of this layer to use the cloud and fog resources in a optimizing fashion which helps the IoT applications on the



**Figure 9: Fog Reference Architecture**

top layer to benefit from this. The optimization is achieved by reducing the use of cloud for processing tasks and improving the performance of applications by decreasing the latency. This reduction in latency is achieved by computing and processing at distributed fog nodes instead of centralized cloud. All these are achieved by making multiple services, described below, working in cohesion with one another.

**Flow and Task Placement:** This maintains the available list of resources available and their state so that it can identify the resources which can be assigned with the incoming requests and their execution flow. This data is then communicated to Resource Provisioning service which in turn decides how the identified resources can be allocated with tasks.

**Knowledge Base:** This creates a knowledge repository by storing historical information about usage of network resources by the applications or any other behavior that can be used by other services so that they can optimize the performance and helps efficient delivery of services.

**Performance Prediction:** This service predicts the performance of network resources by using the historical data provided by Knowledge Base service. The predictions made by this service are used by the other services to achieve the optimized performance.

Raw Data Management: This is a critical component to leverage the use of fog computing. The incoming raw data from end devices need to be processed and may be modelled into a different view and sent to the cloud or to other services.

**Monitoring**: This service keeps track of every component in the network. For example, application's usage of resources, their performance, network health and several other parameters are monitored by this service. This data is utilized by other services as and when required.

**Profiling:** This service helps to determine the application or network resource profiles which help in decision making and analytics in future.

**Resource Provisioning:** This service acts as the administrator of network by allocating resources to applications as per demand by taking inputs from other services like Knowledge Base, Monitoring, and Performance prediction. This also decides at which level a task need to be executed depending on the tolerable latency time for that task.

**Security**: This address the security concerns related to the applications and the nodes in the network.

**V. Fog Cloud Applications and Services**

The concept of Fog computing was introduced for the applications and services which could not be efficiently supported by cloud computing. Fog computing is an emerging technology and a lot of research and work is being conducted to utilize it in real life scenarios. There are many applications of Fog computing. In this section, we will discuss some of them.

***Internet of Things***

IOT is a concept, wherein, the physical devices connect over the internet and exchange data and information with each other. The “things” here means the non-communicating object, such as a table or a chair, as well as, communicating devices, typically, smart objects, which perform some tasks and is digital in nature. IOT is an attempt to connect everything to the internet. Some properties of the IOT applications are 1. Low Latency Applications 2. Geographically distributed 3. Mobile in nature. Considering the properties of IOT applications, it would not be wrong to conclude that the integration of cloud and IOT, referred to as Cloud of Things(COT) is not totally feasible. The cloud provides the centralized structure, and cannot cater to the needs of IOT applications.

The total number of devices connected to the network are already 9 billion and are expected to grow till 24 billion by 2020. All these devices would generate data and with the increase in so many devices, the amount of data and the processing of data would eventually increase multiple folds. This will increase a lot of load over network and cloud resources and there is possibility, that the cloud infrastructure might not be able to handle the burden of so much of data and processing. The Fog computing paradigm can handle the situation by preprocessing the data and sending only the filtrated information to the cloud. The Fog cloud can handle much of the processing on its own before sending the data to the cloud. For instance, in case of departmental store, it is not necessary to store the information of each transaction, but the data required to perform some analytics and business decisions can be preferably stored over cloud.

**Use case: Wind Farm [17]**

Wind Farm is one of the most suitable use case for Fog computing and equally shares the characteristics of Internet of Things (IOT). The following are the attributes of wind farm –

* Real Time and Batch processing.
* Widely geographically distributed system
* There must be enough interaction between devices, such as, controllers, sensors and actuators.

The speed of the wind turbine must be coordinated with the speed of wind. There are criteria to decide the speed of the turbine with respect to the speed of the wind –

* If the wind speed is low, then the turbines should not run, otherwise the wind energy would not be sufficiently converted to Electrical power and the system would run into losses.
* There is a normal scenario, where, the wind speed is such that the maximum efficiency is obtained.
* There is a certain threshold, above which if, the wind speed increases, the power must be limited, to, avoid going above the safe threshold limit.
* If the wind speed becomes further high, then the turbines needs to be powered down.

Currently, it is handled by the controllers at each turbine, but a global controller is highly recommended for coordination between each subsystem (turbine), to reap out the maximum potential benefit from the wind farm.

The requirements for the system can be outlined as follows –

* Networking infrastructure – For communication between each subsystem and between system and cloud
* Global controller – The global controller will process the information received from each subsystem and define policy which will be global, but will act as unique for each turbine (subsystem), per the wind conditions, location and the condition of the turbine. The global controller will need to make real time decisions and would need to process the information very fast. This is where Fog can play a very important role as the cloud will not be able to provide very low latency.
* Mediator – Middleware between system and cloud
* Data Analytics – The data can also be collected for analysis and can be stored on the cloud.

The wind farm acts as an appropriate example of interplay between fog and cloud.

***Mitigating Insider data theft attacks in the cloud***

In the world of cloud computing, trust is the biggest concern as the customers would not be aware of the location of their data and would also be unaware of data from which other sources is stored with their data. The cloud customer will not have the data locally stored on their machines, which is why, they cannot apply any strategy by themselves to secure their data and would have to totally depend on the cloud provider for its security. One of the major security threats for the cloud applications is malicious attack by an insider. The administrator will have an access to the server on which the virtual machines for the customers will run. The administrator himself can gain access to the virtual machine hosted on the server and can access customer data. In PaaS, the developer might have access to all the user’s data and user might not be aware of it. The administrator responsible for performing backup of data, can also have access to sensitive customer information. The access of customer data by unauthorized user and its misuse can have a huge negative impact on the company reputation and will lead to loss of customer trust.

Current solutions which the cloud company proposes to mitigate insider data theft attacks is listed below –

* Not allowing physical access to the server, but it will be of no use as the server would be accessible remotely.
* There are two mechanisms which will help to curb insider attacks, but they would be useful only after the attack has taken place –

1. Firing an employee after his identity is released
2. Generating audit logs which can provide information about which virtual machine was accessed with which User ID.

.

Cloud providers can improve their hiring practices, but we certainly cannot rely fully on this.

Cryptography is widely used in cloud while sharing passwords with the users, but even the strong encryption algorithms, such as, FHE (Fully Hormonic Encryption) and ABE (Attribute Based Encryption) has certain limitations and the safety of secret and confidential data cannot be guaranteed through Encryption mechanisms. Moreover, Key Management is a very big task for such humongous number of clients.

There is a need of a robust and concrete solution for the data security in cloud. A solution is being proposed for the data security in cloud and mitigate the impact of insider data theft and masquerader attack in cloud.

It is mainly composed of two features [10] –

**User behavior Profiling** – It is expected that the actual user would be aware of the file and directory structure of his/her own system, but the attacker who uses the system for the first time would not be aware of the locations of the file and data. Hence, his search behavior would be very different from the normal user. This technique is aimed to identify the deviation in the normal behavior of the user regarding user commands, database / file accesses and search behavior. Volume and frequency of user activities will vary from normal user to masquerader. According to a user study experiment mentioned in prior paper [29], eighteen computer science students installed windows host sensor on their Personal Computers, to collect data, such as, Windows GUI and file accesses, all registry based activities, process creation and destruction, etc.

They were made to use their PC for a span of four days and Windows Host sensor collected the data and saved it on to the server. After this, sixty computer science students were divided into the group of three, namely –

Malicious – The intent of Malicious group is to steal information

Benign -The Benign group used the system, but their intent was not to steal the information.

Neutral – The neutral group had a choice if they wanted to use the system or not.

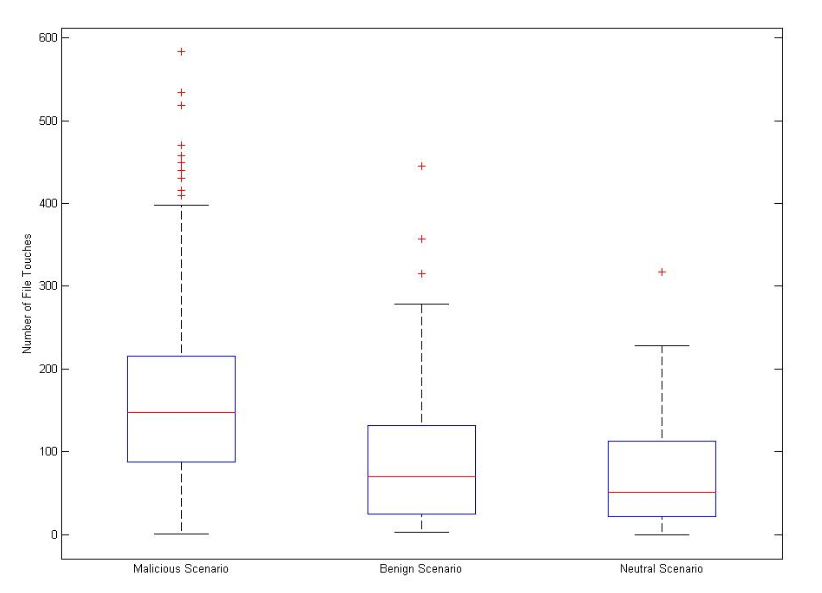
Each of the group was given 15 minutes to access freely the Personal Computers of the eighteen Computer science students. The basis of the experiment is that the user search behavior is impacted by user’s intent. Based on search activities and files accesses, it will be detected who is a genuine user and who is a masquerader. Over the span of 15 minutes for each group, several statistics were collected of which two proved to be highly significant for detecting the masquerader behavior. These statistics were –

* Number of file touches
* Percentage of user actions related to file system navigation.

Box whisker plots were generated for both the criteria.

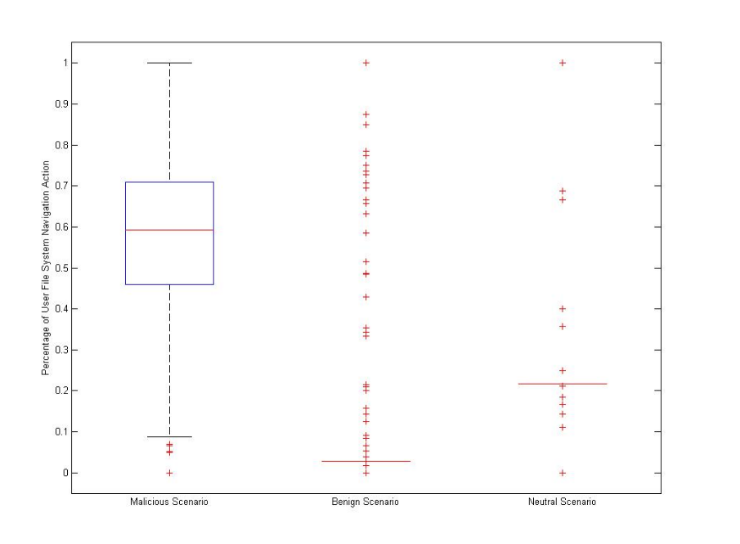
The horizontal line in the middle of the box shows the median value. Fifty percent of the value lies inside the box and the top and bottom quartile (25 %), lies above and below the horizontal line outside the box.

Below are the graphs which represents the same –



**Figure 10: Distribution of file touches across three groups**

The vertical line shows the number of file touches and it is clear from the graph that the number of file touches for the malicious group is much more than the other two groups.



**Figure 11: Distribution of the Percentage of File**

**System Navigation User Actions across the three**

**User Study Groups**

The vertical line shows the percentage of user actions which are search related and it is clearly more for Malicious group, which is the first group in the graph.

The experimental results for detecting theft using user search behavior modelling has been achieve 98.9 % accuracy result with 1.1 % false rate, where legitimate user is considered as masquerader.

**Decoy** – Decoys are the documents which contains false information and can be used to confuse the attacker. The information would be presented in such a manner that it looks correct to the attacker, but it would indeed be a false information. It is kind of trap or bait to the attacker. It has been experimented that both the techniques combinedly can give better results than both individually.

The approach to using both the techniques together can be achieved through two sensors –

USB (User search behavior) Sensor – It will detect any abnormal user search related activity.

DDA (Decoy Document Access) Sensor – This sensor will monitor any access to the decoy documents.

If any abnormal user search behavior is detected, the sensor will sense it and the information will be sent to the Fog cloud and the cloud in turn can send decoy documents to the client’s machine. Any normal user will be aware of the location of decoy document and would know where they are stored, hence, a normal user will not tend to open them, but, on the contrast, the attacker will not know of the same and can fall into the trap of opening them.

This will give the confidence that some malicious activity is taking place and RUU (Are You You) sensor will perform any of the three activities –

1. Sending an alert message to the remote server.
2. Displaying a set of challenge questions that the owner must correctly respond to during installation
3. If the webcam is available, stealthily recording audio and taking a picture

Per an experimental evaluation in the prior paper [30], the false positive rate of combined approach is 0.77 % and that of search profiling alone is 1.1 %, which clearly shows that integrated approach gives better results.

The data used and generated is real time and the technique requires quick response. It is necessary to generate decoy documents as quick as possible, once the suspicious user search behavior is detected, hence, Fog paradigm highly suits this new solution being proposed to enhance cloud security. The technique does not involve any long-time data analytics and hence, it is not necessary to store data on cloud.

***Healthcare***

Fog computing can play a very efficient role in the improvement of healthcare services by enhancing telehealth. Telehealth is the means of delivering healthcare and health-related education through telecommunications technologies with the help of smart devices, such as, sensors. These sensors are composed of transducers and can detect electrical, thermal, optical, chemical, genetic and other signals with physiological origin. Signal processing algorithms can help to calculate, forecast and measure different features of human health based on input of these sensors [31]. The examples of some basic sensors are thermometer, blood glucose monitors, ECG, etc.

A report issued by World Health Organization (WHO)

state that there is most patients who do not adhere with their medical prescriptions as they are supposed to which results in decay or failure in the treatment of diseases. In such scenarios, smart healthcare items can support the monitoring of patient adherence and allow for better treatment by providing solutions to such problems which come up with features like opening at correct time and recording of pill intake time. If the details of patient’s disease and treatment is stored in the cloud, they would adhere their medical prescriptions as they are supposed to. Smart healthcare items like physiological parameter monitors can automatically record the health parameters and update it to the cloud, which will be easy for decision making and would help in deciding the future course of action to be taken in timely and speedy manner [31].

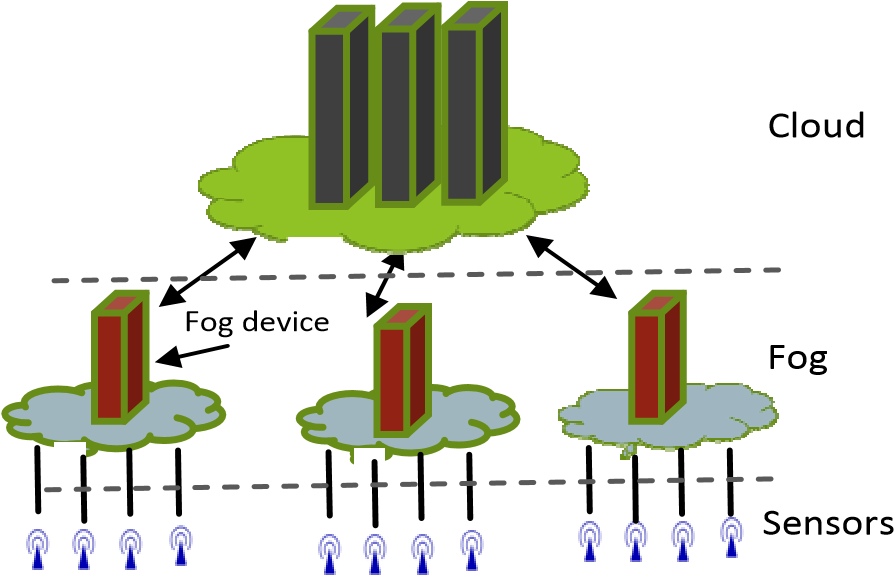
The sensors generate a huge amount of data, which is, heterogenous in nature, and it is very challenging to store and transmit such data, and to perform computations on it. Managing and processing such data is challenging for healthcare units. The optimal solution is to outsource the collection, storing and processing of data to cloud based companies. It will release the healthcare industries from the burden of infrastructure management and will cut down the labor cost associated with it. It would really help the healthcare industry to concentrate on their major goal of providing the best treatment to their patients.

The use of traditional and centralized cloud architecture is not very promising for implementation of telehealth. A heretical structure and service localization can bring about a significant performance improvement as compared to the centralized architecture. Hence, Fog computing is a suitable cloud paradigm in this scenario.

Below are many advantages of using Fog computing-

* **low latency –** With the use of fog computing, the real-time data analytics and quick response can be achieved.
* **Reliability –** The fog devices provide backup, in case the link to the cloud is faulty.
* **Storage and transmission –** Fog enables data analytics at the preliminary stage, which will reduce the amount of data to be stored and transmitted onto the cloud. Wearable sensor data along with the useful data, also carry data corruption issues and unwanted signals. Hence, data cleansing and filtration is required before sending the data to the cloud, to avoid space consumption by unwanted data. This can be well handled by Fog.

Below is the figure which shows an integration of sensors, Fog and cloud computing –

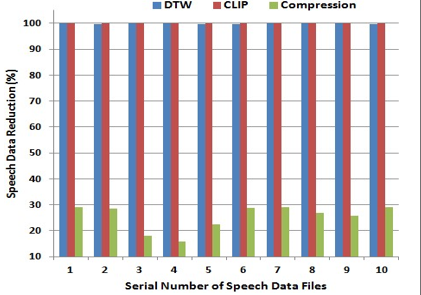


**Figure 12: Fog Computing**

The sensors upload the data onto the Fog server, post which, the data is then sent onto the cloud.

The case study for speech monitoring of patient with Parkinson’s disease, mentioned in the prior paper [32] shows a significant amount of speech data reduction.

Below is the figure which illustrates the percentage of data reduction achieved with Dynamic Time Warping (DTW), Clinical Speech Processing Chain (CLIP) and GNU Zip-



**Figure 13: The percentage of data reduction achieved by using DTW, CLIP and GNU Zip compression on 10 speech files collected by Parkinson’s disease patient by smartwatch-based system [32]**.

The Figure shows that almost 100 percent data reduction has been achieved by DTW and CLIP and around 30 percent has been achieved by GNU Zip. This amount of data reduction at the edge of network can greatly help to combat network congestion..

**VI. Future direction of Fog Computing**

In this chapter, we try to identify some of the important gaps that exist in the current research of Fog computing in academia as well as business circles [1]. Some of these gaps are provided below, but it does not cover all of the current gaps.

**A. Context aware provisioning**

Fog computing can efficiently provision resources based on context-awareness. However, the definition of “context” can vary based on several factors including, but not limited to:

Environmental context: Time (Peak, Off peak) or location

User context: Mobility, activity

Device context: Resource availability, battery life etc.

Network context: Traffic, bandwidth etc.

These need to be fully explored and defined further before Fog computing becomes a reality.

**B. Sustainability and Reliability**

These are two areas where further research is needed to ensure that Fog computing performance is both sustainable (in terms of energy efficiency and QoS) as well as reliable in terms of performance and being fault tolerant.

**C. Interoperable Architecture of Fog Nodes**

Fog nodes can perform both networking related tasks as well as computational tasks and there is a need for an interoperable architecture that can also be customized as per the need is required. This is another area where several proposals have been made in academic circles, but more investigation is needed.

**D. Multi-tenant Support**

Further research into how a multi-tenant architecture can be supported by Fog nodes using virtualization needs to be explored further

**E. Pricing, Billing**

Fog computing resources are spread across vertically and this makes user pricing and billing challenging due to these resources being owned by multiple service providers whereas cloud computing only has horizontal scaling on demand as requested by users. This area is currently not clearly understood and needs to be looked into further.

**F. Lack of tools for Fog simulations**

Real world toolkits and simulators for measuring and evaluating performance of Fog computing environments are few and far between. This is an area that needs further work.

**G. Programming languages and standards**

Since Fog computing is an extension of existing Cloud services, there is a need to improve and extend current standards, protocols, APIs and programming languages and tools related to enabling cloud services in Fog. This is an area that needs further research and industry support.

**VII. Conclusion**

In this report, we discussed about the new computing paradigm, Fog computing. We highlighted some key concepts of Fog computing and its architecture, infrastructure and classifications. We also compared it with cloud computing and looked at how Fog computing extends cloud computing and can be utilized in real life scenarios, where, cloud computing might not be efficient. There are certain challenges in the research conducted for fog computing, which has been discussed in detail. We can conclude that Fog computing does not totally replace cloud computing, but does help in overcoming the disadvantages of using cloud computing alone, for upcoming technologies, such as, Internet of Things.

**References**

1. Mahmud, R. and Buyya, R. (2016) *Title: Fog computing: A Taxonomy, survey and future directions*. Available at: <https://arxiv.org/abs/1611.05539>
2. Varghese, B., Wang, N., Nikolopoulos, D.S. and Buyya, R. (2017) *Title: Feasibility of fog computing*. Available at: https://arxiv.org/abs/1701.05451
3. Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L. (2015b) *Title: Fog computing: Focusing on mobile users at the edge*. Available at: https://arxiv.org/abs/1502.01815v3
4. Yi, S., Li, C. and Li, Q. (2015) ‘A survey of fog computing’,pp.37–42.doi: 10.1145/2757384.2757397.
5. Dastjerdi, Vahid, A., Gupta, H., Calheiros, R.N., Ghosh, S.K. and Buyya, R. (2016) *Title: Fog computing: Principles, architectures, and applications*. Available at: https://arxiv.org/abs/1601.02752
6. Luan, Tom H., et al. "A View of Fog Computing from Networking Perspective." arXiv preprint arXiv: 1602.01509 (2016).
7. M. Aazam and E. N. Huh, "Fog Computing and Smart Gateway Based Communication for Cloud of Things," 2014 International Conference on Future Internet of Things and Cloud, Barcelona, 2014, pp. 464-470. doi: 10.1109/FiCloud.2014.83 <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6984239&isnumber=6984143>
8. L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog," ACM SIGCOMM Computer Communication Review, vol. 44, no. 5, pp. 27–32, Oct. 2014. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2677052>.
9. J. Zhu, D. S. Chan, M. S. Prabhu, P. Natarajan, H. Hu and F. Bonomi, "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture," 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, Redwood City, 2013, pp. 320-323.  
   doi: 10.1109/SOSE.2013.73 <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6525539&isnumber=6525477>
10. S. J. Stolfo, M. B. Salem and A. D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, 2012.doi: 10.1109/SPW.2012.19 <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6227695&isnumber=6227677>
11. priyankareddy, "Diksha sanghi," 2015. [Online]. Available: https://www.slideshare.net/priyankareddy14/fog-computing-provide-security-to-the-data-in-cloud.
12. K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B.Koldehofe, "Mobile fog : a programming model for large-scale applications on the internet of things," pp. 15–20, Aug. 2013. [Online]. Available: http://dl.acm.org/citation.cfm?id=2491270.
13. E.Saurez, K. Hong, D. Lillethun, U. Ramachandran, and B. Ottenwälder, "Incremental deployment and migration of geo-distributed situation awareness applications in the fog," *DEBS ’16 proceedings of the 10th ACM International Conference on Distributed and Event-based Systems*, pp. 258–269, Jun. 2016. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2933317>.
14. E. M. Tordera *et al.*, "Title: What is a fog Node A Tutorial on current concepts towards a common definition," 2016. [Online]. Available: <https://arxiv.org/abs/1611.09193>.
15. B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A hierarchical distributed fog computing architecture for big data analysis in smart cities," p. 28, Jul. 2015. [Online]. Available: http://dl.acm.org/citation.cfm?id=2818898.
16. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," *MCC ’12 Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13–16, Aug. 2012. [Online]. Available: http://dl.acm.org/citation.cfm?id=2342513.
17. Flavio Bonomi, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. “Fog Computing: A Platform for Internet of Things and Analytics” in [Big Data and Internet of Things: A Roadmap for Smart Environments](http://link.springer.com/book/10.1007/978-3-319-05029-4), Volume 546 of the series [Studies in Computational Intelligence](http://link.springer.com/bookseries/7092). Nik Bessis,CiprianDobre, Ed. Springer International Publishing, 2014, pp 169-186.
18. Ivan Stojmen, Sheng Wen. “The Fog computing paradigm: Scenarios and security issues.” In [Computer Science and Information Systems (FedCSIS), 2014 Federated Conference](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6923033), Warsaw, Poland.
19. [Amir VahidDastjerdi](https://arxiv.org/find/cs/1/au:+Dastjerdi_A/0/1/0/all/0/1), [Harshit Gupta](https://arxiv.org/find/cs/1/au:+Gupta_H/0/1/0/all/0/1), [Rodrigo N. Calheiros](https://arxiv.org/find/cs/1/au:+Calheiros_R/0/1/0/all/0/1), [Soumya K. Ghosh](https://arxiv.org/find/cs/1/au:+Ghosh_S/0/1/0/all/0/1), [RajkumarBuyya](https://arxiv.org/find/cs/1/au:+Buyya_R/0/1/0/all/0/1). “Fog Computing: Principles, Architectures, and Applications” in Internet of Things: Principles and Paradigms, Volume 2. R. Buyya and A. Dastjerd, Ed. Morgan Kaufmann Publications, 2016, pp 61-75.
20. [Mohammed A. Hassan](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Mohammed%20A.%20Hassan.QT.&newsearch=true), [MengbaiXiao,](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Mengbai%20Xiao.QT.&newsearch=true)[Qi Wei](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Qi%20Wei.QT.&newsearch=true),[Songqing Chen](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Songqing%20Chen.QT.&newsearch=true). “Help your mobile applications with fog computing” in [Sensing, Communication, and Networking - Workshops (SECON Workshops), 2015 12th Annual IEEE International Conference](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7323762), Seattle, Washington.

1. [OnsBibani](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Ons%20Bibani.QT.&newsearch=true),[Carla Mouradian](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Carla%20Mouradian.QT.&newsearch=true),[Sami Yangui](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Sami%20Yangui.QT.&newsearch=true),[Roch H. Glitho](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Roch%20H.%20Glitho.QT.&newsearch=true),[Walid Gaaloul](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Walid%20Gaaloul.QT.&newsearch=true),[Nejib Ben Hadj-Alouane](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Nejib%20Ben%20Hadj-Alouane.QT.&newsearch=true),[Monique Morrow](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Monique%20Morrow.QT.&newsearch=true),[Paul Polakos](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.Paul%20Polakos.QT.&newsearch=true). “A Demo of IoT Healthcare Application Provisioning in Hybrid Cloud/Fog Environment” in [Cloud Computing Technology and Science (CloudCom), 2016 IEEE International Conference](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=7823365), Luxembourg, Luxembourg
2. S. Yi, C. Li, and Q. Li, "A survey of fog computing," pp. 37–42, Jun. 2015. [Online]. Available: http://dl.acm.org/citation.cfm?id=2757397. Accessed: Mar. 5, 2017.
3. DocPlayer, "Cisco fog computing solutions: Unleash the power of the Internet of things - PDF,". [Online]. Available: http://docplayer.net/20003565-Cisco-fog-computing-solutions-unleash-the-power-of-the-internet-of-things.html. Accessed: Mar. 6, 2017.
4. [Online]. Available: <http://catai.net/blog/wp-content/uploads/2017/02/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf>.
5. X. Hou, Y. Li, M. Chen, D. Wu, D. Jin and S. Chen, "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures," in *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3860-3873, June 2016. doi: 10.1109/TVT.2016.2532863
6. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7415983&isnumber=7493708>
7. G. Suciu, V. Suciu, A. Martian, R. Craciunescu, A. Vulpe, I. Marcu, S. Halunga and O. Fratu, "Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications", 2017.
8. Yi, Shanhe, et al. "Fog computing: Platform and applications." Hot Topics in Web Systems and Technologies (HotWeb), 2015 Third IEEE Workshop on. IEEE, 2015.
9. M. Ben-Salem and S. J. Stolfo, “Modeling user search-behavior for masquerade detection,” in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 6–12
10. M. Ben-Salem and S. J. Stolfo, “Combining a baiting and a user search profiling techniques for masquerade detection,” in *Columbia University Computer Science Department, Technical Report # cucs-018-11*, 2011. [Online]. Available:<https://mice.cs.columbia.edu/getTechreport.php?techreportID=1468>
11. Stantchev, Vladimir, et al. "Smart Items, Fog and Cloud Computing as Enablers of Servitization in Healthcare." Sensors & Transducers (1726-5479)185.2 (2015).
12. Dubey, Harishchandra, et al. "Fog data: Enhancing telehealth big data through fog computing." *Proceedings of the ASE BigData & SocialInformatics 2015*. ACM, 2015.