ACADEMY OF TECHNOLOGY

G.T.ROAD (ADISAPTAGRAM),
AEDCONAGAR
HOOGHLY-712121 WEST BENGAL,
INDIA

Seminar Report On:

FOG COMPUTING BASED ON IOT

**Under the Guidance of Prof.
SANJIB MITRA**

By

Subhayan Bhowmick

University Roll: 16900317005

Tamojit Saha

University Roll: 16900317002

DEPT: ECE 3RD YEAR

ACADEMY OF TECHNOLOGY

Certificate

This is to certify that this seminar report entitled " **Fog Computing** " is a bonafide record of the work done by **Tamojit Saha and Subhayan Bhowmick** under our guidance towards partial fulfilment of the requirements for the award of **Bachelor of Technology Degree** in **Electronics & Communication Engineering**, from MAKAUT during the year 2017-20.

Prof. Sanjib Mitra
Assistant Professor
(Seminar Guide)

Prof.Abhijit Bannerjee
Assossiate Professor
(Head of Department)

Acknowledgement

The satisfaction that accompanies the successful completion of this project would be incomplete without the mention of the people who made it possible, without whose constant guidance and encouragement would not have been possible to prepare this report.

First and foremost, I wish to express my sincere gratitude to our Principal, **Amitava Seal** for his constant support and encouragement in preparation of this report and for making available library and laboratory facilities needed to prepare this report.

I would like to thank **Prof. Abhijit Bannerjee**, our Head Of the Department (ECE), for his valuable suggestions and guidance throughout the period of this report.

I would also like to express my sincere gratitude to the seminar co-ordinators **Prof. Sanjib Mitra**, Assistant Professor, ECE Department for his unflagging support and continuous encouragement throughout the period of seminar as well as during the preparation of report.

Place : Naihati

Date : 17-03-2019

Yours Sincerely,

Tamojit Saha

Subhayan Bhowmick

Contents

Abstract:

Fog computing is a new paradigm that extends the Cloud platform model by providing computing resources on the edges of a network. It can be described as a cloud-like platform having similar data, computation, storage and application services, but is fundamentally different in that it is decentralized. In addition, Fog systems are capable of processing large amounts of data locally, operate on premise, are fully portable, and can be installed on heterogeneous hardware. These features make the Fog platform highly suitable for time and location-sensitive applications. For example, Internet of Things (IoT) devices are required to quickly process a large amount of data. This wide range of functionality driven applications intensifies many security issues regarding data, virtualization, segregation, network, malware and monitoring. This paper surveys existing literature on Fog computing applications to identify common security gaps. The majority of Fog applications are motivated by the desire for functionality and end-user requirements, while the security aspects are often ignored or considered as an afterthought. This paper also determines the impact of those security issues and possible solutions, providing future security-relevant directions to those responsible for designing, developing, and maintaining Fog systems.

Nowadays huge amount of data is stored on cloud. Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. Because of these new computing and communication paradigm there arise data security challenges. In this paper, we proposed a system for securing data stored in the cloud using decoy technology. In this we monitor data access in the cloud and detect abnormal data access. When unauthorised access is detected that user’s activity will be tracked in log details table. Based on the activities performed by unauthorized user admin can blocked or delete that user. When a new user enters into this System, he have to register first. After successfully registered, that user will get a key through mail. And during login, if the user enter wrong password continuously more than three times, he will get access and his activity will be tracked on log details table in the database. And after this, whatever activities he is doing that also will be tracked in the log table .If he downloads any file, he won’t get original file. Instead of that he will get decoy file. If a user entered correct password and he will get access .If that user wants to download any file, and he entered wrong key more than three times, in first three cases in the action column invalid will be entered and in the fourth case wrong key and that user will get decoy file .In every case it Now will execute user behaviour algorithm. When a user edit password he enters wrong key more than three times, then edit pwd wrong key will be entered. And user will get message that password updated successfully. But in actual case it is not updating.

With the rapid growth of Internet of Things (IoT) applications, the classic centralized cloud Computing paradigm faces several challenges such as high latency, low capacity and network failure. To address these challenges, fog computing brings the cloud closer to IoT devices. The fog provides IoT data processing and storage locally at IoT devices instead of sending them to the cloud. In contrast to the cloud, the fog provides services with faster response and greater quality. Therefore, fog computing may be considered the best choice to enable the IoT to provide efficient and secure services for many IoT users. This paper presents the state-of-the-art of fog computing and its integration with the IoT by highlighting the benefits and implementation challenges. This review will also focus on the architecture of the fog and emerging IoT applications that will be improved by using the fog model.

Finally, open issues and future research directions regarding fog computing and the IoT are discussed.

Theory:

Fog computing is a decentralized computing architecture whereby data is processed and stored between the source of origin and a cloud infrastructure. This results in the minimisation of data transmission overheads, and subsequently, improves the performance of computing in Cloud platforms by reducing the requirement to process and store large volumes of superfluous data. The Fog computing paradigm is largely motivated by a continuous increase in Internet of Things (IoT) devices, where an ever increasing amount of data (with respect to volume, variety, and velocity) is generated from an ever-expanding array of devices.

IoT devices provide rich functionality, such as connectivity, and the development of new functionality is often data motivated. These devices need computing resources to process the acquired data; however, fast decision processes are also required to maintain a high-level of functionality. This can present scalability and reliability issues when utilising a standard client-server architecture, where data is sensed by the client and processed by the server. If a server was to become overloaded in a traditional client-server architecture, then many devices could be rendered unusable. The Fog paradigm aims to provide a scalable decentralised solution for this issue. This is achieved by creating a new hierarchically distributed and local platform between the Cloud system and end-user devices, this platform is capable of filtering, aggregating, processing, analysing and transmitting data, and will result in saving time and communication resources. This new paradigm is named *Fog computing*, initially and formally introduced by Cisco.

Fog computing provides many benefits to individuals and organizations through offering highly available and efficient computing resources with an affordable price. Many cloud services are available in current commercial solutions, but they are not suitable for latency, portability and location-sensitive applications, such as IoT, Wearable computing, Smart Grids, Connected Vehicles and Software-Defined-Networks. Latency depends on the speed of Internet connection, resource contention among guest virtual machines (VM) and has been shown to increase with distance. Furthermore, such applications generate large volumes of varied data in a high velocity, and by the time data reaches a cloud system for analysis, the chance to inform the IoT device to take reactive action may be gone. For example, consider IoT devices in the medical domain where the latency of acting on the sensed data could be life-critical.

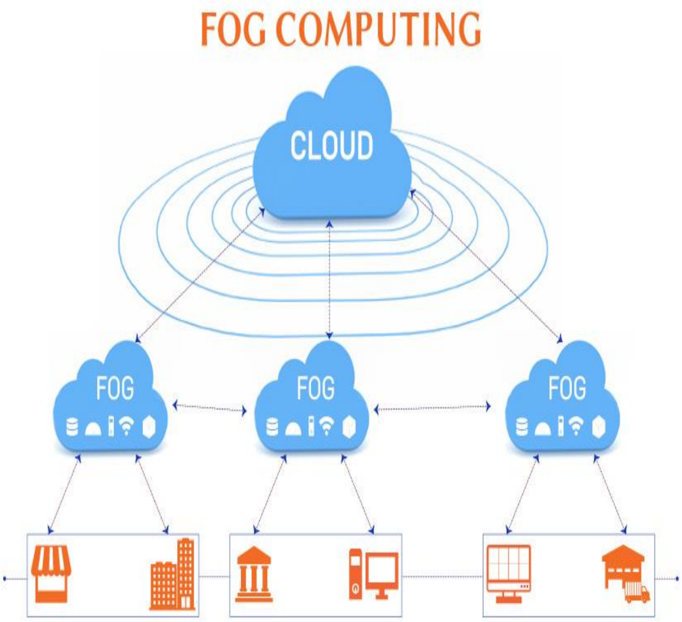
Cisco pioneered the delivery of the Fog computing model that extends and brings the Cloud platform closer to end-user's device to resolve aforementioned issues. According to, a Fog system has the following characteristics:

- It will be located at the edge of network with rich and heterogeneous end-user support;
- Provides support to a broad range of industrial applications due to instant response capability;
- It has its own computing, storage, and networking services;
- It will operate locally (single hop from device to Fog node);
- It is highly a virtualized platform; and
- Offers inexpensive, flexible and portable deployment in terms of both hardware and software.

Besides having these characteristics, a Fog system is different from Cloud computing in various aspects and poses its own advantages and disadvantages. Some of the more prominent are detailed in the below list.

- A Fog system will have relatively small computing resources (memory, processing and storage) when compared to a Cloud system, but the resources can be increased on-demand;
- They are able to process data generated from a diverse set of devices;
- They can be both dense and sparsely distributed based on geographical location;
- They support Machine-to-Machine communication and wireless connectivity;
- It is possible for a Fog system to be installed on low specification devices like switches and IP cameras; and
- One of their main uses is currently for mobile and portable devices.

Fog Computing looks for the convergence of many existing technologies. So it is better we have a brief overview of these technologies that provides roots for its emergence.
Like Cloud systems, a Fog system is composed of Infrastructure, Platform, and Software-as-a-Service (IaaS, PaaS, and SaaS, respectively), along with the addition of Data services. The technical architecture of a Fog platform, The Fog IaaS platform is created using Cisco IOx API, which includes a Linux and CISCO IOS networking operating system. Any device, such as switches, routers, servers and even cameras can become a Fog node that have computing, storage, and network connectivity. Fog nodes collaborate among themselves with either a Peer-to-Peer network, Master-Slave architecture or by forming a Cluster. The Cisco IOx APIs enable Fog applications to communicate with IoT devices and Cloud systems by any user-defined protocol. For developing Fog applications in PaaS environment, Cisco DSX is used to create a bridge between SaaS (which actually offers Metal-as-a-Service) and many types of IoT devices. It provides simplified management of applications, automates policy enforcement and supports multiple development environments and programming languages. The data service decides the suitable place (Cloud or Fog) for data analysis, identifies which data requires action and increases security by making data anonymous. Fog devices are geographically distributed over heterogeneous platforms, spanning multiple management domains. That means data can be processed locally in smart devices rather than being sent to the cloud for processing. The purpose of fog computing in the IoT is to improve efficiency, performance and reduce the amount of data transferred to the cloud for processing, analysis and storage. Therefore, the data collected by sensors will be sent to network edge devices for processing and temporary storage, instead of sending them into the cloud, thus reducing network traffic and latency.



Characteristics of Fog Computing:

Essentially, fog computing is an extension of the cloud but closer to the things that work with IoT data. Fog computing acts as an intermediary between the cloud and end devices which brings processing, storage and networking services closer to the end devices themselves. These devices are called fog nodes. They can be deployed anywhere with a network connection. Any device with computing, storage and network connectivity can be a fog node, such as industrial controllers, switches, routers, embedded servers and video surveillance cameras.

Fog computing is considered to be the building blocks of the cloud, the characteristics of fog computing can be summarized as follows:

Location awareness and low latency: Fog computing supports location awareness in which fog nodes can be deployed in different locations. In addition, as the fog is closer to end devices, it provides lower latency when processing the data of end devices.

Geographical distribution: In contrast to the centralized cloud, the services and applications provided by the fog are distributed and can be deployed anywhere.

Scalability: There are large-scale sensor networks which monitor the surrounding environment.

The fog provides distributed computing and storage resources which can work with such Large-scale end devices.

Support for mobility: One of the important aspects of fog applications is the ability to connect directly to mobile devices and therefore enable mobility methods, such as locator ID separation protocol (LISP) which needs a distributed directory system.

Real-time interactions: Fog computing applications provide real-time interactions between fog nodes rather than the batch processing employed in the cloud.

Heterogeneity: Fog nodes or end devices are designed by different manufacturers and thus come in different forms and need to be deployed according to their platforms. The fog has the ability to work on different platforms.

Interoperability: Fog components can interoperate and work with different domains and across different service providers.

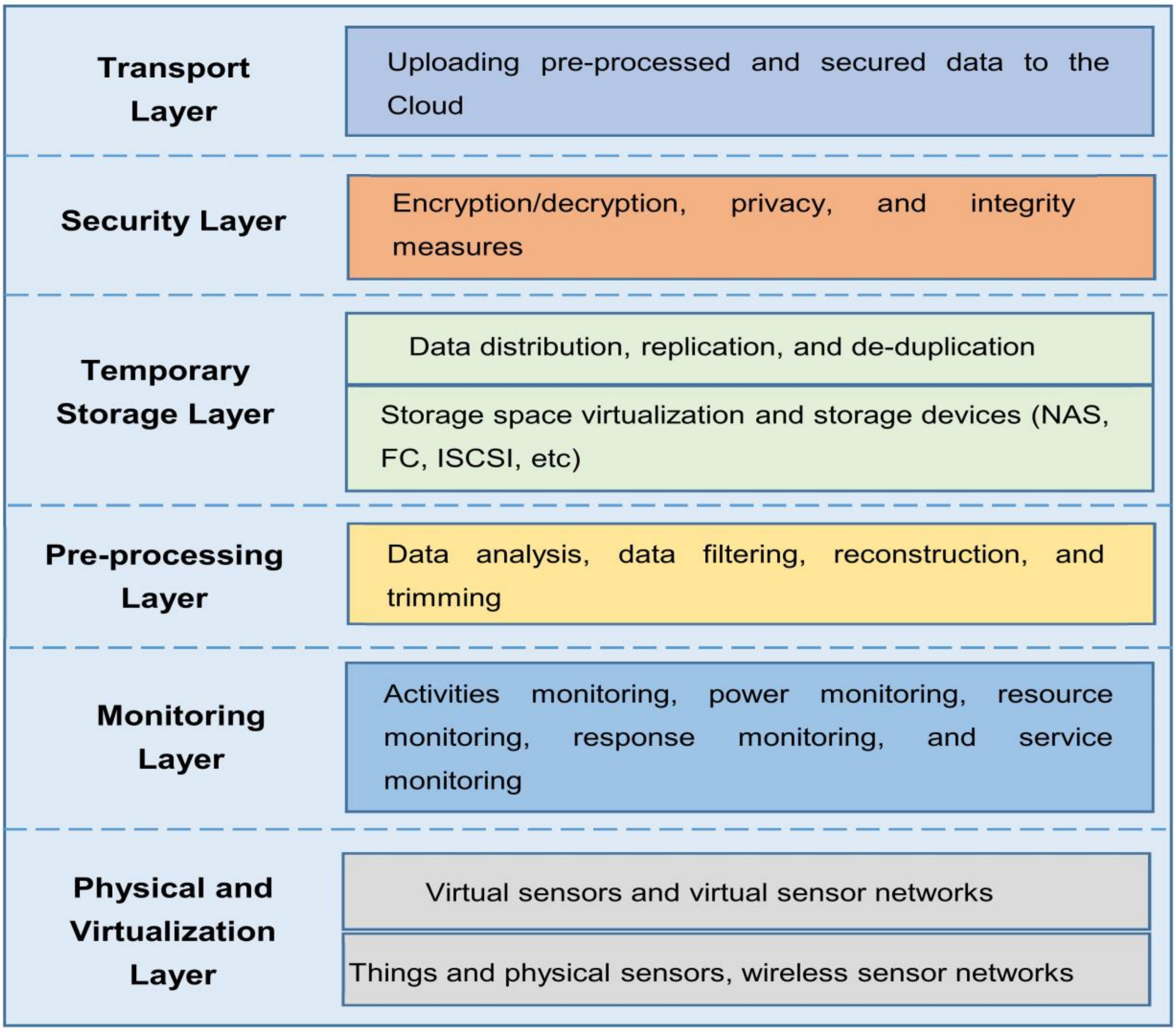
Support for on-line analytics and interplay with the cloud: The fog is placed between the cloud and end devices to play an important role in the absorption and processing of the data close to end devices.

Some other characteristics are:

- Large scale fog networks, fog nodes can move across the network seamlessly using Access Points and proxies.
- It is not devised for batch processing type requirements.
- Ubiquitous wireless access.
- It requires high Interoperability across fog services providers.
- Fog computing supports interaction with Cloud and analytic services.

Architecture of FOG Computing:

Fog computing is an approach that takes some of a data centre's operations to the edge of the network. The fog provides limited computing, storing and networking services in a distributed manner between end devices and the classic cloud computing data centres. The primary objective of fog computing is to provide low and predictable latency for time-sensitive IoT applications the architecture of fog computing consists of six layers—physical and virtualization, monitoring, pre-processing, temporary storage, security and transport layer.



Layered architecture of fog computing.

The physical and virtualization layer involves different types of nodes such as physical nodes, virtual nodes and virtual sensor networks. These nodes are managed and maintained according to their types and service demands. Different types of sensors are distributed geographically to sense the surroundings and send the collected data to upper layers via gateways for further processing and filtering. While at the monitoring layer, resource utilization, the availability of sensors and fog nodes and network elements are monitored. All tasks performed by nodes are monitored in this layer, monitoring which node is performing what task, at what time and what will be required from it next. The performance and status of all applications and services deployed on the infrastructure are monitored. In addition, the energy consumption of fog nodes is monitored; since fog computing uses many devices with different levels of power consumption, energy management measures can be both timely and effective. The pre-processing layer performs data management tasks. Collected data are analysed and data filtering and trimming are carried out in this layer to extract meaningful information. The pre-processed data are then stored temporarily in the temporary storage layer. When the data are transmitted to the cloud, they no longer need to be stored locally and may be removed from the temporary storage media. In the security layer, the encryption/decryption of data comes into play. In addition, integrity measures may be applied to the data to protect them from tampering. Finally, in the transport layer, the pre-processed data are uploaded to the cloud to allow the cloud to extract and create more useful services. For efficient power utilization, only a portion of collected data is uploaded to the cloud. In other words, the gateway device connecting the IoT to the cloud processes the data before sending them to the cloud. This type of gateway is called a smart gateway. Data collected from sensor networks and IoT devices are transferred through smart gateways to the cloud. The data received by the cloud is then stored and used to create services for users. Based on the limited resources of the fog, a communication protocol for fog computing needs to be efficient, lightweight and customizable. Therefore, choosing the communication protocol depends on the application scenario of the fog.

Difference Between FOG and Cloud Computing:

The current centralized cloud computing architecture is facing severe challenges for IoT applications. For instance, it cannot support IoT time-sensitive applications such as video streaming, gaming and augmented reality. In addition, it lacks location awareness as it is a centralized model. Fog computing is able to address these challenges. Table 1 summarizes differences between cloud and fog computing.

Table 1. Comparison between cloud and fog computing.

Items	Cloud Computing	Fog Computing
Latency	High	Low
Hardware	Scalable storage and computing power	Limited storage and computing power
Location of server nodes	Within the Internet	At the edge of the local network
Distance between client and server	Multiple hops	One hop
Security measures	Defined	Hard to define
Attack on data	Less probability	High probability
Deployment	Centralized	Distributed
Working environment	Warehouse-size building with air conditioning systems	Outdoor (e.g., Streets, gardens) or indoor (e.g., Restaurants)
Location awareness	No	Yes

Fog Computing with IoT:

Fog computing acts as a bridge between IoT devices and large-scale cloud computing and storage services. According to Cisco, fog computing is a part of the cloud computing paradigm that takes the cloud closer to the edge of the network. It provides a highly virtualized model of computation, storage and networking resources between end devices and classical cloud servers.

To increase the efficiency of IoT applications, most of the data generated by these IoT objects/devices must be processed and analyzed in real-time. Fog computing will bring cloud networking, computing and storage capabilities down to the edge of the network, which will address the real-time issue of IoT devices and provide secure and efficient IoT applications.

Fog computing provides different services and applications with widely distributed deployments. The fog has the ability to provide efficient real-time communication between different IoT applications, such as connected vehicles, through the proxy and access points positioned according to long highways and tracks. Fog computing is considered to be the best choice for applications with low latency requirements such as video streaming, gaming, augmented reality, etc.

The integration of fog computing with the IoT will bring many benefits to various IoT applications. The fog supports real-time interactions between IoT devices to reduce latency, especially for time-sensitive IoT applications. In addition, one of the important features of fog computing is the ability to support large-scale sensor networks, which is a big problem with the ever-growing number of IoT devices, which will soon be counted in billions. Fog computing can provide many benefits to various IoT applications, as shown in Figure.

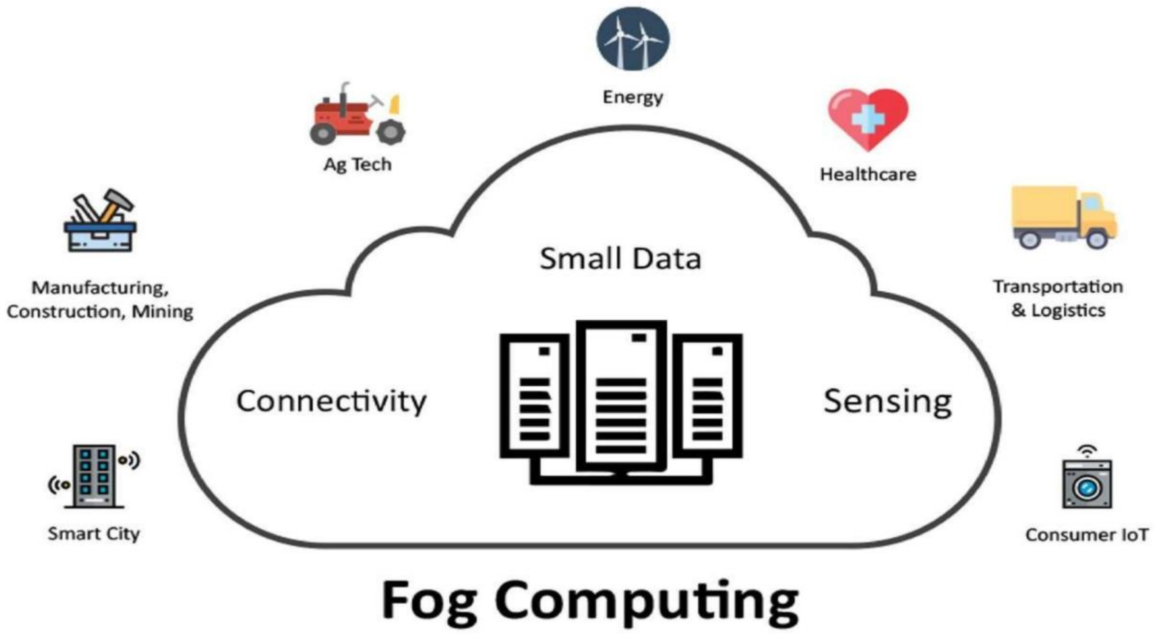


Figure 3. Fog computing supports many IoT applications to provide better service to customers.

Fog computing can provide effective ways to overcome many limitations of existing computing architectures that rely only on computing in the cloud and on end-user devices that are related to IoT devices.

According to M. Chiang and T. Zhang , fog computing can solve many of IoT challenges as described in Table 2.

Table 2. Fog computing provides new solutions to many IoT challenges.

IoT Challenge	How the Fog Can Solve the Challenge
Latency constraints	The fog performs all computation operation such as managing and analyzing data and other time-sensitive actions close to end users, which is the ideal solution to meet latency constraints of some of IoT applications.
Network bandwidth constraints	Fog computing enables hierarchical data processing along the cloud to IoT devices. This allows data processing to be carried out depending on application demands, required to be uploaded to the cloud, which will save network bandwidth.

Resource-constrained devices	Fog computing can be used to perform operations that need huge resources on behalf of resource-constrained devices when such operations cannot be uploaded to the cloud. Therefore, this allows reducing devices' complexity, lifecycle costs and power consumption.
Uninterrupted services	Fog computing can run independently to ensure continuous services even when it has irregular network connectivity to the cloud.
IoT security challenges	Resource-constrained devices have limited security functions; therefore, fog computing acts as the proxy for these devices to update the software of these devices and security Credentials. The fog can also be used to monitor the security status of nearby devices.

This section describes articles which discuss the convergence of the IoT with fog computing. As fog computing is still a recent research topic, there is a lack of concrete solutions supporting this computing paradigm. In this section, we survey existing works that discuss the integration of fog computing with the IoT in various applications.

FOG Layers:

Device layer:

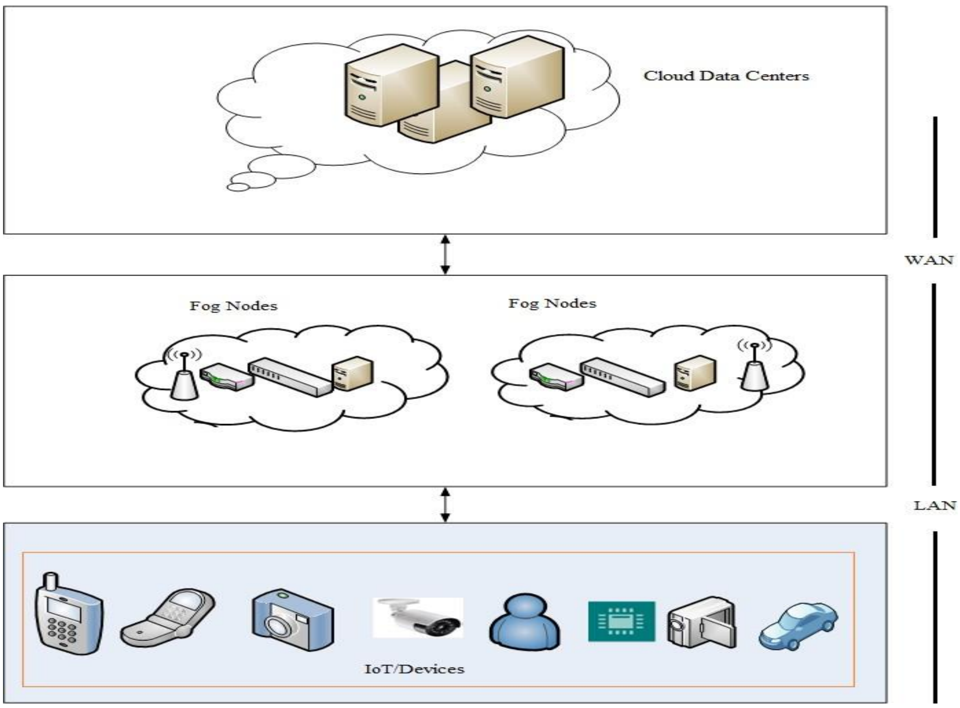
Device layer contains different IoT devices and end devices such as mobile phone, smart vehicles, smart cards etc. These devices are distributed geographically. Generally the terminal devices sensed information from different physical objects or events. The information are Collected and sent to the top layer for further processing and storage.

Fog layer:

The fog computing layer is deployed between cloud and IoT devices. This layer plays an important role in the transmission between the cloud computing layer and the device layer. Fog layer contains network devices such as router, access points, gateways, switches, and video surveillance cameras. These de- vices act as a fog server, geographically distributed among end devices and cloud. Fog servers collect information's from end devices. Also, they have the ability to manage the process and temporally store sensed information. The fog server performs real-time analyses as well as accomplished latency sensitive information. Fog server can be also used statically at a fixed point. for example inside a shop installed similar to as a Wi-Fi or mobile placed on a moving vehicle like system Greyhound Blue system

Cloud layer:

The cloud layer is the top layer in the fog computing environ-ment. It corresponds to cloud intelligence and can store and process massive amounts of data, depending on the capabilities of the data center. The cloud data center is responsible for analyzing and making all decisions and is responsible for permanent storage. The cloud can also assign part of the task to the fog node because fog is often more meaningful for local analysis and quick decision making. If the fog does not re- quire in-depth analysis, it only needs to actively filter the local data and selectively retransmit the data to the cloud. There- fore, transmission efficiency can be significantly improved for widely distributed networks.



High-performance servers, edge router, access points and gate- way etc. operated by the different operating system which has a different level of computation power and storage capabilities. Fog computing also provide virtualized platform. Some virtual nodes such as computing nodes and virtual network nodes can also be used as fog nodes. Therefore, fog nodes is heterogeneous.

- Mobility support
  Mobility support plays a vital role for some fog computing applications to empower direct communication with mobile devices through the use of protocols. For example, the Cisco Locator / ID separation protocol, which uses a distributed di- rectory system to separate the host's identity from the site's identity.
- Close to the end user
  To eliminate delays in data transmission fog allows data to be closer to users than stored in remote data centers.

However, despite its power, the cloud model is not applicable to environments where operations are time-critical or internet connectivity is poor. This is especially true in scenarios such as telemedicine and patient care, where milliseconds can have fatal consequences. The same can be said about vehicle to vehicle communications, where the prevention of collisions and accidents can't afford the latency caused by the roundtrip to the cloud server. "The cloud paradigm is like having your brain command your limbs from miles away —it won't help you where you need quick reflexes. "Moreover, having every device connected to the cloud and sending raw data over the internet can have privacy, security and legal implications, especially when dealing with sensitive data that is subject to separate regulations in different countries. IoT nodes are closer to the action, but for the moment, they do not have the computing and storage resources to perform analytics and machine learning tasks. Cloud servers, on the other hand, have the horsepower, but are too far away to process data and respond in time. The fog layer is the perfect junction where there are enough compute, storage and networking resources to mimic cloud capabilities at the edge and support the local ingestion of data and the quick turnaround of results. The variety of IoT systems and the need for flexible solutions that respond to real-time events quickly make Fog Computing a compelling option.

Components:

We suggest a fog computing platform be composed of the following components, as shown in Figure. We briefly explain several important components.

Authentication and Authorization: The access of fog computing services and resources needs to be authenticated and authorized. One related work has proposed an access control scheme for authorization of heterogeneous resources. Fog computing also opens the door for new authentication and authorization schemes since it is close to end users and can identify user using access pattern, mobility pattern and trusted secure devices.

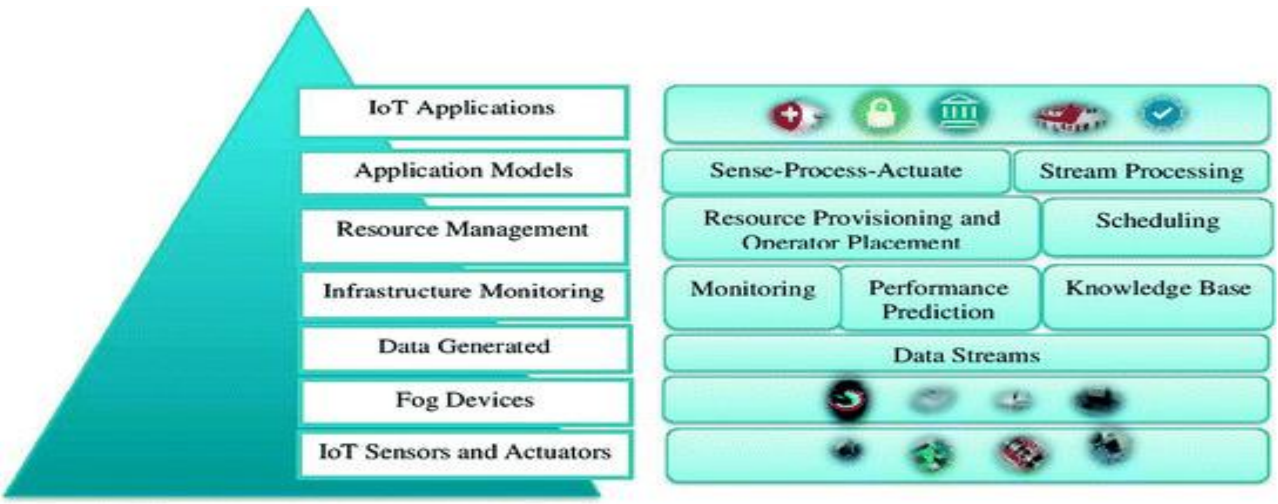
Offloading Management: Offloading is an important component that has impact on all design goals. There are extensive existing research on this topic, as we have surveyed in. The offloading in fog computing needs to solve several problems:

1) what kinds of information are needed in offloading decisions,
2) how to partition application for offloading, and
3) how to design optimal offloading scheme.

Location Services:

Location services need to maintain a location list of neighbour nodes (mobile and non-mobile node), track mobile end users, and share location information among involved fog nodes. It maps network locations with physical locations, and adopts mobility model provided by end user or learns the mobility model if possible. The tracking and mapping on mobile nodes will need information from multiple layers (physical (ultrasound, wireless signal and signature, GPS, IMU sensor), network (IP address), and application (social activities)), which will call for new design for this component.

System Monitor:



System monitor is a standard com- ponent in cloud infrastructures, which can provide useful information such as work load, usage, energy to help lots of decision making and pricing. We highlight this component in fog computing platform since it provides crucial information for other components.

Resource Management:
The resource management will be responsible for most tasks related to resource discover, resource allocation, the dynamic joining and leaving of fog node, and provisioning and maintaining the resource pool in a distributed manner.VM Scheduling: The VM scheduling needs a brand new design due to fused input of system usage, work load stats, location information and mobility model. New scheduling strategies are needed to provide optimal solution for schedul- ing VMs.

Application:

There are many significant areas where fog computing can play a vital role in different IoT applications. This section provides an overview of various IoT applications that can benefit from fog computing.

Connected Car:
According to Cisco, autonomous vehicles is a new trend for cars. There are many beneficial features, which depend on the fog and Internet connectivity that can be added to cars such as automatic steering and “hands-free” operation or self-parking features which mean that there is no need for a person behind the wheel to park the vehicle.

In the next few years, it is expected that all new cars will have the ability to communicate with nearby cars and the Internet. Fog computing will be the most efficient solution for all Internet-connected vehicles, since it provides a high level of real-time interaction. In addition, it will allow cars, access points and traffic lights to interact with each other to deliver a good service to users.

With the use of the fog instead of the cloud, collisions and other accidents can be reduced as it does not suffer from the latency of the centralized cloud approach, enabling it to start literally saving lives.

Smart Traffic Lights:
Fog computing allows traffic signals to open roads depending on sensing flashing lights. It senses the presence of pedestrians and cyclists and measures the distance and speed of the nearby vehicles. Sensor lighting turns on when it identifies movements and vice-versa.

Smart traffic lights may be considered to be fog nodes which are synchronized with each other to send warning messages to nearby vehicles. The interactions of the fog between the vehicle and access points are improved withWiFi, 3G, smart traffic lights and roadside units.

Smart Home:
The IoT has many sensors and devices connected in the home. However, these devices come from different vendors and have different platforms, making it difficult to get them to work together. In addition, some tasks need a large amount of computation and storage. Fog computing solves many of these issues. It integrates all different platforms and empowers smart home applications with flexible resources.

Fog computing has many benefits for home security applications. It provides a unified interface to integrate all different independent devices. In addition, it provides elastic resources to enable storage, real-time processing and low-latency.

Wireless Sensor and Actuator Networks:
One of the key features of WSNs is the ability to increase battery life by functioning at mostly

low power. Actuators are used to manage the measurement operation and changing behaviour forming a closed-loop system. Actuators may be considered to be fog nodes that provide different actions to control end devices with sensors. These WSNs require less bandwidth, less energy and very low processing power.

Healthcare and Activity Tracking:

Fog computing plays a vital role in healthcare. It provides real-time processing and event responses which are critical in healthcare. In addition, the interaction of a large number of healthcare devices for remote storage, processing and medical record retrieval from the cloud requires a reliable network connection which is not available. It also addresses issues regarding network connectivity and traffic.

IoT and Cyber–Physical Systems:

The integration of fog computing with the IoT and cyber–physical systems (CPSs) is becoming possible. The IoT is a network that is able to interconnect all world devices together with an identified address using the Internet and telecommunications.

On the other hand, the CPS is a combination of physical and computational elements. The integration of CPSs with the IoT will convert the world into a computer-based physical reality. Fog computing is designed with the notion of embedded systems, for instance, connected vehicles, medical devices and others. With the combination of fog computing with the IoT and CPS, it will become possible to develop intelligent medical devices, smart buildings, and agricultural and robotic systems.

Augmented Reality:

Augmented reality (AR) refers to systems that add virtual information to the real world. AR has become an important application due to computing devices become smaller, faster and more ubiquitous. AR applications are extremely latency-sensitive since a small delay in the application response can damage the user experience. Fog computing has the ability to be a key player in the AR domain by employing both the fog and cloud servers to enable real-time applications.

A scientist designed an augmented brain–computer interaction game (ABCI) based on fog computing. They have demonstrated that a combination of fog and cloud servers can provide a continuous real-time game.

Network Function Virtualization (NFV):

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

Software-defined Networking (SDN):

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

Advantage:

Fog computing have several advantages over its ancestor, cloud computing. Basic cloud computing technology is utilized by fog computing at its core. It helps to boost usability and accessibility in different computing environments. The advantages that fog computing offers are as follows-

Greater Business Agility:

By utilizing the right set of tools, developers can seamlessly develop fog applications and deploy them whenever needed. Fog applications drive the machine to function in a way according to customers need.

Better Security:

Fog nodes can be protected using the same controls, procedures, and policy you use in other areas of IT environment.

Deeper Insights with Privacy Control:

The sensitive data can be analyzed locally instead of sending it to the cloud for analysis. The IT team can keep track and control the devices that collect, analyze and store data.

Reduced Operation Cost:

Fog computing can save network bandwidth by processing selected data locally, instead of sending it to the cloud for analysis.

Load balancing:

Load balancing improves the distribution of workloads across multiple computing resources

Maximize network bandwidth utilization:

Monitor network's connection to identify applications or programs that take up too much of bandwidth, so we can adjust their settings and features.

Enhanced Quality of Service (QoS):

ensuring customer service it is necessary to assess not only individual agent performance but also the quality management.

Latency Reduction:

Reducing the amount of server latency will help load your web resources faster, thus improving the overall page load time

Disadvantage:

Although the fog computing paradigm offers many benefits for different IoT applications, it faces many challenges that stand in the way of its successful deployment. These challenges include scalability, complexity, dynamicity, heterogeneity, latency and security.

It is obvious that fog computing is a new technology that needs more research to address all the challenges previously mentioned. This section provides an overview of open issues and future research directions related to fog computing and its integration with the IoT.

1. Encryption algorithms and security policies make it more difficult for arbitrary devices to exchange data. Any mistakes in security algorithms lead to exposure of data to the hackers. Other security issues are IP address spoofing, man in the middle attacks, wireless network security etc.

2. To achieve high data consistency in the the fog computing is challenging and requires more efforts.

3. Fog computing will realize global storage concept with infinite size and speed of local storage but data management is a challenge.

4. Trust and authentication are major concerns.

5. Scheduling is complex as tasks can be moved between client devices, fog nodes and back end cloud servers.

6. Power consumption is high in fog nodes compare to centralized cloud architecture.

7. Communications between the Fog and the Cloud

8. Communications between Fog Servers

9. End User Privacy

Future of FOG Computing:

Fog Computing, Cloudlet and Mobile Edge Computing share the vision of Edge Computing paradigm, however they have a different set of characteristics which sets them apart from each other that we discussed in this paper. Even though a lot of research has been put into proposing and developing these features, they are interpreted differently by different consumers. Thus, there is a lack of standardization in terms of the actual implementation of FC, Cloudlet and MEC. This lack of standardization also affects the classification of the features of each of these implementations and thus makes the decision tree sparse. With gradual research into standardization, there would be more clarity on the features and implementation of the Edge nodes, which would facilitate in developing a denser decision tree with more choices to the end user. Our contribution through the decision tree can be leveraged to build a recommender system for the choice of an EC implementation. The recommender system can take a particular use-case with a set of desired parameters or features as an input with corresponding priorities to recommend a particular implementation of EC to the consumer.

Future work will expand on the Fog Computing paradigm in Smart grid. In this scenario, two models for Fog devices can be developed. Independents fog devices consult directly with the Cloud for periodic updates on price and demands, while interconnected Fog device may consult each other.

Next, Fog Computing based SDN in vehicular networks will received due attention.

Fog computing focuses on serving customized location-based applications to mobile users. The Fog layers can be adapted by using the existing accessing networks, e.g., Wi-Fi, or emerging 5G wireless technologies with a virtualized architecture.

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

Conclusion:

Fog computing is emerging as an attractive solution to the problem of data processing in the Internet of Things. It relies on devices on the edge of the network that have more p4rocessing power than the end devices and are nearer to these devices than the more powerful cloud resources, thus reducing latency for applications. In this chapter, we introduced a reference architecture for IoT and discussed ongoing efforts in the academia and industry to enable the fog computing vision. Many challenges still remain though, with issues ranging from security to resource and energy usage minimization still in need for solutions. Open protocols and architectures are also other topics for future research that will make fog computing more attractive for end users.

Fog Computing and its applications has been discussed .Fog computing has the ability to handle the flooding of data created by Internet of Things on the edge of the network. The characteristics of fog computing like mobility, proximity to end-users, low latency, location awareness, heterogeneity and due to its real-time applications fog computing platform is considered as the appropriate platform for Internet of

Things. Fog computing is entering an exciting time, where it can positively affect operational costs. Fog computing resolves problems related to congestion, space and internet traffic. Fog computing also provides an intelligent platform to manage the distributed and real-time nature of emerging IoT infrastructures.

Developing these services at the edge through fog computing will lead to new business models and opportunities for network operators.

Fog computing, the new concept of the cloud at the edge of the network, is considered the appropriate platform for many Internet of Things services and applications along with virtualization of WSN/WSAN. Fog computing gives the cloud a companion to handle the extra bytes of data generated daily from the Internet of Things. Processing data closer to where it is produced and needed to solve the challenges of exploding data volume, variety, and velocity. It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. It also protects sensitive IoT data by analysing it inside company walls. Ultimately, organizations that adopt fog computing gain deeper and faster insights, leading to increased business agility, higher service levels, and improved safety. Hence, we can come to the conclusion that fog computing and cloud computing will complement each other while having their own advantages and disadvantages. Fog computing will grow in helping the emerging network paradigms that require faster processing with less delay and delay jitter, cloud computing would serve the business community meeting their high end computing demands lowering the cost based on a utility pricing mode.

Fog computing accelerates awareness and response to events by eliminating a round trip to the cloud for analysis.

It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. It also protects sensitive IoT data by analyzing it inside company walls. Ultimately, organizations that adopt fog computing gain deeper and faster insights, leading to increased business agility, higher service levels, and improved safety.

In summary, the purpose of this paper was to provide a review in order to summarize up-to-date research contributions on fog computing and the IoT and its applications in our world, as well as demonstrating future research directions and open issues regarding integrating fog computing with the IoT.

Reference:

I. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, USA

II. Ben-Salem M., and Stolfo Angelos D. Keromytis, “Fog computing: Mitigating Insider Data Theft Attacks in the Cloud,” IEEE symposium on security and privacy workshop (SPW) 2012.

III. Ben-Salem M., and Stolfo, “Decoy Document Deployment for Effective Masquerade Attack Detection,” Computer Science Department, Columbia University, New York.

IV. F. Bonomi, "Connected vehicles, the internet of things, and fog computing," in The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011.

V. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ser. MCC'12. ACM, 2012, pp. 13-16.

VI. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr 2010.

VII. C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storage devices," IEEE Journal of Selected Areas in Communications, 2014 to appear.

VIII. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787-2805, Oct. 2010.

IX. K. Liu, J. Ng, V. Lee, S. Son, and I. Stojmenovic, "Cooperative data dissemination in hybrid vehicular networks: Vanet as a software defined network," Submitted for publication, 2014.

X. K. Kirkpatrick, "Software-defined networking," Commun. ACM, vol. 56, no. 9, pp. 16-19, Sep. 2013.