Fog Computing

Pranati V. Patil
Computer science & Engg
College of Engg & Tech, Akola.

ABSTRACT
Fog Computing is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end users. In this article, we elaborate the motivation and advantages of Fog computing, and analyses its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. We discuss the state-of-the-art of Fog computing and similar work under the same umbrella. Security and privacy issues are further disclosed according to current Fog computing paradigm. As an example, we study a typical attack, man-in-the-middle attack, for the discussion of security in Fog computing.

General Terms
Cloud, Security, fog, privacy, Compute, Accountability.

Keywords
Internet of things, Fog, cloud, smart grid.

1. INTRODUCTION
CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things (IoT), to run directly at the network edge. Customers can develop, manage and run software applications on Cisco IOx framework of networked devices, including hardened routers, switches and IP video cameras. In Fog computing, services can be hosted at end devices such as set-top-boxes or access points. The infrastructure of this new distributed computing allows applications to run as close as possible to sensed actionable and massive data, coming out of people, processes and thing. Such Fog computing concept, actually a Cloud computing close to the 'ground', creates automated response that drives the value. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Both Cloud and Fog provide data, computation, storage and application services to end-users. However, Fog can be distinguished from Cloud by its proximity to end-users, the dense geographical distribution and its support for mobility. We adopt a simple three level hierarchy[2].Figure1.

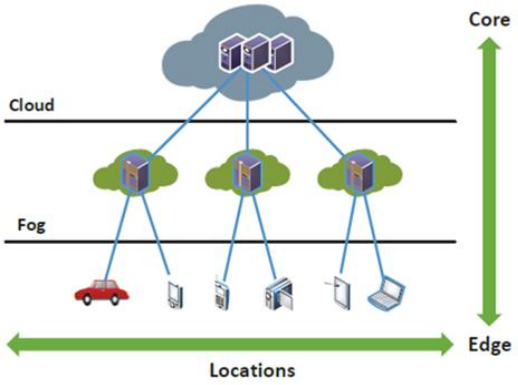

Fig.1. Fog between edge and cloud.

2. NEED OF FOG
In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current "pay-as-you-go" Cloud computing model becomes an efficient alternative to owning and managing private data centers for customers facing Web applications and batch processing .Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomes a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements. When techniques and devices of IoT are getting more involved in people's life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location awareness and low latency. Fog computing is proposed to address the above problem. As Fog computing is implemented at the edge of the network, it provides low latency, location awareness, and improves quality-of-services (QoS) for streaming and real time applications[2]. Typical examples include industrial automation, transportation, and networks of sensors and actuators. Moreover, this new infrastructure supports heterogeneity as Fog devices include end-user devices, access points, edge routers and switches. The Fog paradigm is well positioned for real time big data analytics, supports densely distributed data collection points, and provides advantages in entertainment, advertising, personal computing and other applications. Fog computing extends the paradigm to the edge of the network. while fog and cloud using same resources(networking, computing, storage) and share many of the same mechanism and attribute(virtualization, multi-tenancy) the extension is a non trivial one in that there exist some fundamental differences stemming from the reason fog computing developed: to address and services that do not fit the paradigm of cloud[4].

3. FOG COMPUTING – A NATURAL BRIDGE BETWEEN CLOUD AND IoT

A new trend could be observed in joint relation with cloud – it was the beginning of December 2013, discussing about a new concept which behind exotic name founded the premises for distributed cloud models. In February 2015 we could describe Fog Computing as essential bridge between the infinite power of the Cloud and an almost infinite number of intelligent edge-points, conventionally conglomerated in IoT concept.

Fig.2. Bridge between fog and cloud.

What's happened with Fog Computing in this very short period? Cloud computing confirmed most of tech and market predictions, being involved in all major technology trends, from Big Data and Analytics, to Mobility, M2M, and Internet of Everything… In parallel with this, IoT concept gains an explosive development, having as main engine exponential increasing of data volumes provided by more and more population and large variety of intelligent devices. In January 2014 Cisco reveled his own fog computing vision, designed on the idea of bringing cloud computing capabilities to the edge of the network, much closer to the growing number of user devices that are consuming cloud services and generating the increasingly massive amount of data. Short time after, Cisco unveiled the company's IOx platform, designed to bring distributed computing to the network edge. According Cisco, Fog Computing extends the cloud computing paradigm to the edge of the network. While fog and cloud use the same computing, storage or network resources, and share many of the same mechanisms and attributes, like multi-tenancy and virtualization. Now we could speak about a Fog Computing ecosystem based on Fog conceptually extension of Cloud computing – covering in a denser way wider geographic locations, and concentrations of Fog devices – much more heterogeneous in nature, ranging from end-user terminals, access points, to networks edge routers and switches. Provided data should be processed locally in smart devices rather than being sent for processing in the cloud. Fog computing is one approach to dealing with the demands of the ever-increasing number small connected devices, sometimes referred to as the Internet of Things (IoT)[1].

In the IoT scenario, a thing is any natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. Some such things can create a lot of data. Mr. Michael Enescu offered as example a jet engine, which can create 20 terabytes of engine performance data in one hour. Sending all data to the cloud and receiving the data back involve increasing demand for bandwidth, considerable amount of time, and induced latency. In a Fog Computing environment, a big part of local data processing would take place in a router, rather than having to be transmitted.

Resuming, the main characteristics of the Fog are:

1. Low latency and location awareness;
2. Wide-spread geographical distribution;
3. Wide area and real time Mobility access;
4. Increasing number and diversity of nodes;
5. Essential access to wireless;
6. Strong presence of streaming and real time applications,
7. Heterogeneity of devices and data sources.

The most illustrative example of Fog computing models in real success stories for IoT are related to projects for Connected Vehicles, Smart Grid, Smart Cities, Education, Ecology, or Health Care. As described in the Cisco research group article the Connected Vehicle deployment could displays various connectivity scenarios: cars to cars, cars to access points (Wi-Fi, 3G, LTE, roadside units [RSUs], smart traffic lights), and access points to access points. The Fog has a number of attributes that make it the ideal platform to deliver a rich menu of SCV services in infotainment, safety, traffic support, and analytics: geo-distribution (throughout cities and along roads), mobility and location awareness, low latency, heterogeneity, and support for real-time interactions.

A smart traffic light system is based on smart traffic light nodes, which interacts locally with a number of terrain sensors which are detecting the presence of pedestrians and bikers, and measures the distance and speed of approaching vehicles. It also interacts with neighboring lights to coordinate the green traffic wave. Based on this information the smart light sends warning signals to approaching vehicles, and even modifies its own cycle to prevent accidents.

3.1 A Internet of Things (IoT)

The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet. The Internet of Things (IoT, sometimes Internet of Everything) is the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices based on the infrastructure of International Telecommunication Union's Global Standards Initiative. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

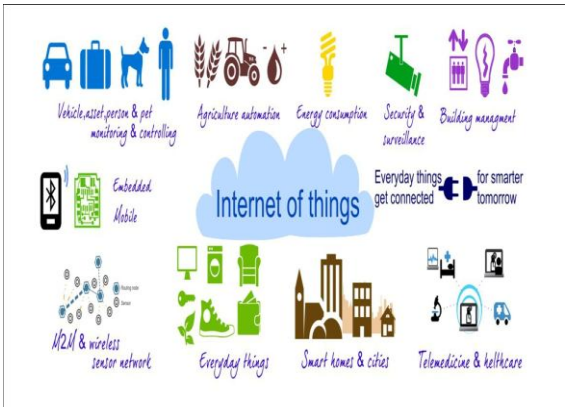

Fig.3. Internet of things.

The term "Internet of Things" was coined by British entrepreneur Kevin Ashton in 1999.Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid and expanding to the areas such as Smart city[1].

4. CLOUD VS FOG

The below tables show us the comparison between cloud and fog. As per the tables given below the latency and delay jitter of the cloud computing is high but the fog computing is very low. Location of services of cloud computing is within the internet but of fog computing is at the edge of local network. Security in fog computing can be defined but in cloud computing we can't defined it. Real time interactions are supported by both cloud and fog computing. Data and applications are processed in a cloud, which is time consuming task for large data. Rather than presenting and working from a centralized cloud, fog operates on network edge. So it consumes less time. There is a high probability of attack on data in cloud computing and fog computing having less probability of attack on data. In cloud computing slow response time and scalability problems as a result of depending servers that are located at a remote place. By setting small servers called edge server in visibility of user, it is possible for fog computing platform to avoid response time and scalability issues[3].

Table 1: Comparison of cloud and fog.

Requirements	**Cloud computing**	**Fog computing**
Latency	High	Low
Delay jitter	High	Very low
Location of service	Within the internet	At the edge of local network
Distance between server and client	Multiple hopes	One hope
Security	Undefined	Can be defined
Attack on data	High probability	Very low probability
Location awareness	No	Yes
Geo – Distribution	Centralized	Distributed
No. of server nodes	Few	Very large
Support for mobility	Limited	Supported
Real time interaction	Supported	Supported
Types of last mile connectivity	Leased line	Wireless

Table 2: Comparison of cloud and fog.

Cloud computing	**Fog computing**
Data and applications are processed in a cloud, which is time consuming task for large data.	Rather than presenting and working from a centralized cloud, fog operates on a network edge. So it consumes less time.
Problems of bandwidth, as a result of sending every bit of data over cloud channels.	Less demand of bandwidth, as every bit of data's were aggregated at certain access point instead of sending over cloud channels.
Slow response time and scalability problem as a result of depending servers that are located at remote place.	By setting small servers called edge server in visibility of the users, it is possible for fog computing platform to avoid response time and scalability issues.

5. ADVANTAGES AND DISADVANTAGES OF FOG COMPUTING

5.1 Advantages

1. The detection of masquerade activity.
2. The confusion of the attacker and the additional costs incurred to distinguish real from bogus information.
3. The deterrence effect which although hard to measure play a significant role in preventing masquerade activity by risk – averse attackers.
4. Edge application services significantly decrease the data volume that must be moved, the consequent traffic, and the distance the data must go, thereby reducing transmission costs, shrinking latency, and improving quality of service (QoS).
5. Edge computing eliminates, or at least de-emphasizes, the core computing environment, limiting or removing a major bottleneck and a potential point of failure.
6. Security is also improved as encrypted data moves further in, toward the network core. As it approaches the enterprise, the data is checked as it passes through protected firewalls and other security points, where viruses, compromised data, and active hackers can be caught early on.
7. Finally, the ability to "virtualized" (i.e., logically group CPU capabilities on an as-needed, real-time basis) extends scalability. The edge computing market is generally based on a "charge for network services" model, and it could be argued that typical customers for edge services are organizations desiring linear scale of business application

performance to the growth of, e.g., a subscriber base.

8. The significant reduction in data movement across the network resulting in reduced congestion, cost and latency, elimination of bottlenecks resulting from centralized computing systems, improved security of encrypted data as it stays closer to the end user reducing exposure to hostile elements and improved scalability arising from virtualized systems.
9. Edge computing, in addition to providing sub-second response to end users, it also provides high levels of scalability, reliability and fault tolerance.
10. Consumes less amount of band width[10][11].

a. Disadvantages

1. Nobody is identified when attack is happen.
2. It is complex to detect which user is attack.
3. We cannot detect which file was hacking[10].

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

11. APPLICATION OF FOG COMPUTING

Following are the some application of fog computing.

1. Connected Cars: Fog computing is the ideal for the connected vehicles(CV) because real time interactions will make communication between cars, access points and traffic lights as safe and efficient as possible. Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles. As shown in Figure, intelligent lighting turns on once a sensor identifies movement and switches off as traffic passes. Neighboring smart lights serving as Fog devices coordinate to create green traffic wave and send warning signals to approaching vehicles. Wireless access points like Wi-Fi, 3G, road-side units and smart traffic lights are deployed along the roads. Vehicles-to-Vehicle, vehicle to access points, and access points to access points interactions enrich the application of this scenario[5][4].

Fig.4. Connected Cars.

2. Smart Grids: Fog computing allow fast, machine to machine (M2M) handshakes and human to machine interactions (HMI) which would work in cooperation with the cloud. Energy load balancing applications may run on network edge devices, such as smart meters and micro-grids Based on energy demand, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind. As shown in Figure, Fog collectors at the edge process the data generated by grid sensors and devices, and issue control commands to the actuators. They also filter the data to be consumed locally, and send the rest to the higher tiers for visualization, real-time reports and transactional analytics. Fog supports ephemeral storage at the lowest tier to semi-permanent storage at the highest tier. Global coverage is provided by the Cloud with business intelligence analytics[1][7].

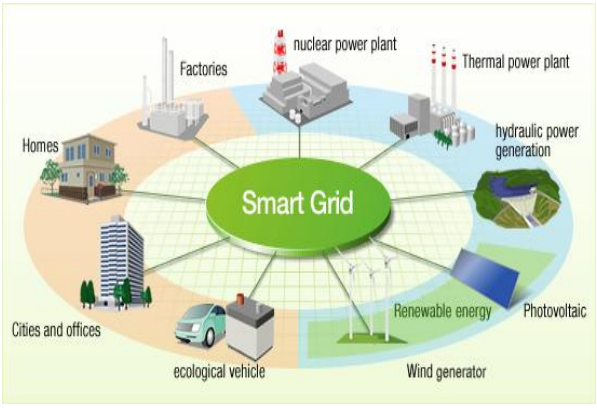

Fig.5. Smart Grid.

3. Health care: The cloud computing market for healthcare is expected to reach $5.4 billion by 2017, and fog computing would allow this on a more localized level.

4. Wireless Sensor and Actuator Networks: Traditional wireless sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors. In this scenario, actuators serving as Fog devices can control the measurement process itself, the stability and the oscillatory behaviors by creating a closed-loop system. For example, in the scenario of self-maintaining trains, sensor monitoring on a train's ball-bearing can detect heat levels, allowing applications to send an automatic alert to the train operator to stop the train at next station for emergency maintenance and avoid potential derailment. In lifesaving air vents scenario, sensors on vents monitor air conditions flowing in and out of mines and automatically change air-flow if conditions become dangerous to miners[1][7].

5. Smart Cities: Fog computing would be able to obtain sensor data on all levels of activities of cities and integrate all the mutually independent network entities within. The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements. Sensors will use distributed decision making and activation at Fog devices to react to data. The system components may then work together to lower the temperature, inject fresh air or open windows. Air conditioners can remove moisture from the air or increase the humidity. Sensors can

also trace and react to movements (e.g, by turning light on or off). Fog devices could be assigned at each floor and could collaborate on higher level of actuation. With Fog computing applied in this scenario, smart buildings can maintain their fabric, external and internal environments to conserve energy, water and other resources[2].

Fig.6. Smart Cities.

12. PRIVACY

Today, we constantly leak personal information by using different products, platforms and services. We may think were in charge of our shopper cards and our mobile apps and our smart fridges, but lets not fool ourselves. The information is not ours. It belongs to Google, and IBM, and Cisco Systems and the global Mega Corp that owns your local supermarket. If you don't believe us, just try removing your data from their databases. Users are becoming increasingly concerned about the risk of having their private data exposed. As a result, besides the technical challenges introduced by the ubiquity of devices, there is another trend that will push for a fog scenario where data is not sent to a few centralized services, but it is instead kept 'in the network' for better privacy. Data ownership will be a very important cornerstone of the fog, where some applications will be able to use the network to run applications and manage data without relying on centralized services.. Storing encrypted sensitive data in traditional clouds is an alternative to keep privacy. However, this makes it really hard to perform any processing over such data. There is important research work on this topic, for example using crypto-processors or applying special encryption functions that cipher while keeping some of its original properties, thus allowing to perform certain limited tasks on it. Still, such options have limited applicability. As a result, users will demand innovative ways to preserve their privacy from any potential big-brother-like entity. This will be a great incentive to adopt fog technologies, as they will enable the network to replace centralized services[3][9].

13. CHALLENGES AHEAD

There are many open problems that will have to be addressed to make the fog a reality. It is necessary to clearly identify them so future research works have these problems into account. The set of open challenges for the fog to become a reality is:

1) Discovery/Sync Applications running on devices may need either some agreed centralized point (e.g. establish an upstream backup if there are too few peers in our storage application).

2) Compute/Storage limitation Current trends are improving this fact with smaller, more energy-efficient and more powerful devices (e.g. one of today's phones is more powerful than many high end desktops from 15 years ago). Still new improvements are granted for non consumer devices.

3) Management In addition to setting up the communication routes across end nodes, IoT/ubiquitous computing nodes and applications running on top need to be properly setup and configured to operate as desired. Having potentially billions of small devices to be configured, the fog will heavily rely on decentralized (scalable) management mechanisms that are yet to be tested at this unprecedented scale. One thing that can be predicted with certain degree of confidence is that there will be no full control of the whole fog and asymptotic declarative configuration techniques will become more common.

4) Security The same security concerns that apply to current virtualized environments can be foreseen to affect fog devices hosting applications. The presence of secure sandboxes for the execution of droplet applications poses new interesting challenges: Trust and Privacy. Before using other devices or mini-clouds in the network to run some software, isolation and sandboxing mechanisms must be in place to ensure bidirectional trust among cooperating parties. The fog will allow applications to process users data in third party's hardware/software. This of course introduces strong concerns about data privacy and its visibility for those third parties[6].

5) Standardization Today no standardized mechanisms are available so each member of the network (terminal, edge point...) can announce its availability to host others software components, and for others to sent it their software to be run.

6) Accountability/Monetization Having users able to share they spare resources to host applications is crucial to enable new business models around the concept of the fog. A proper system of incentives needs to be created. The incentives can financial or otherwise (e.g. unlimited free data rates). On the other hand the lack of central controlling entity in the fog makes it difficult to assert if a given device is indeed hosting a component (droplet) or not.

7) Programmability Controlling application lifecycle is already a challenge in cloud environments. The presence of small functional units (droplets) in more locations (devices) calls for the right abstractions to be in place, so that programmers do not need to deal with these difficult issues. Easy to use APIs for programmers will heavily rely on simple Management mechanisms that provide them with the right abstractions to hide the massive complexity of the fog. Some vendors like Microsoft have already taken some steps in positioning themselves in this space9[8].

14. CONCLUSION

The fog is nothing but the convergence of a set of technologies that have been developing and maturing in an independent manner for quite some time. The integration of these into a single IT scenario is an answer to the new requirements introduced by device ubiquity and demands for agile network and service management and data privacy. As a result the fog will dramatically shift many of our current practices at almost every layer of the IT stack, like apps development, network traffic management, network/service provision, accounting, apps collaboration mechanisms, etc. This article has provided a broad overview of this convergence and what are the common points that link all these technologies together, creating a new paradigm that some have already named as fog computing.

15. ACKNOWLEDGMENTS

It is a matter of great pleasure to highlight a fraction of knowledge, I acquired during my technical education through this seminar. This would not have been possible without the guidance and help of many people. This is where I have the opportunity of expressing gratitude from the core of my heart. Thanks are in order to all the colleagues and friends who knowingly or unknowingly helped me during this work.

16. REFERENCES

[1] F. Bonomi, R. Milito, P. Natarajan. "Fog computing – A platform For Internet Of Things And Analytics" Enterprise Networking Labs, Cisco Systems Inc., San Jose, USA

[2] Ivan Stojmenovic, "The fog computing Paradigm : Scanerios And Security Issues", SIT, Deakin University, Burwood, Australia and SEECS, University of Ottawa, Canada.

[3] Luis. Rodero-Merino," Finding your Way in the Fog: Towards a Comprehensive Definition of Fog Computing", HP LaboratoriesHPL-2014-60

[4] Sheng Wen," The Fog Computing Paradigm: Scenarios and Security Issues", School of Information Technology, Deakin University, 220 Burwood Highway, Burwood, VIC, 3125, Australia.

[5] 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.

[6] Salvatore J. Stolfo," Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud", Computer Science Department, Columbia University New York , NY, USA.

[7] Tom H. Luan, Longxiang Gao, Yang Xiang," Fog Computing: Focusing on Mobile Users at the Edge", School of Information Technology Deakin University, Burwood Melbourne, VIC 3125, Australia

[8] Luis M. Vaquero Hewlett-Packard Labs Bristol, United Kingdom,luis.vaquero@hp.com

[9] W. Wang and Z. Lu, "Survey cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[10] http://www.slideshare.net/saisharansai/fog-computing-46604121

[11] http://www.slideshare.net/professorbanafa/what-is-**fog-computing**