FOG Computing - FOG COPUTING

computer science (Shetty Institute of Technology)

A SEMINAR REPORT

ON

FOG COMPUTING

Submitted in partial fulfillment of the requirements for the

award of the degree of

Bachelor of Technology

In

Computer Science and Engineering

Submitted By

ARAVAPALLI SAI RAVI TEJA

18031A0501

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

University College of Engineering Narasaraopet

Jawaharlal Nehru Technological University Kakinada

Narasaraopet – 522 601

Guntur District, Andhra Pradesh

2021-2022

Department of Computer Science and Engineering

University College of Engineering Narasaraopet

Jawaharlal Nehru Technological University Kakinada

Narasaraopet – 522 601

Guntur District, Andhra Pradesh

CERTIFICATE

This is to certify that the dissertation entitled "**FOG COMPUTING**" that is being submitted by **ARAVAPALLI SAI RAVI TEJA 18031A0501** in partial fulfillment for the award of **Bachelor of Technology** in **Computer Science and Engineering** to the **University College of Engineering Narasaraopet, Jawaharlal Nehru Technological University Kakinada** is a record of Bonafede work carried out by him/her under my guidance and supervision.

The dissertation has not been submitted to any other university/institute for the award of any degree.

Supervisor	**Head of the Department**
Mr Ch Rakesh	Dr G Madhavi
Asst. Professor of CSE	Asst. Professor of CSE
UCEN JNTUK.	UCEN JNTUK.

DECLARATION

I hereby declare that the work described in this project report entitled "**FOG COMPUTING**" which is submitted by me in partial fulfillment for the award of Bachelor of Technology (B Tech.) in the Department of **Computer Science and Engineering** to the **University College of Engineering Narasaraopet, Jawaharlal Nehru Technological University Kakinada,** Andhra Pradesh.

The work is original and has not been submitted for any Degree/Diploma of this or any other university.

Place: Narasaraopet

Date:

Signature of the student

ARAVAPALLI SAI RAVI TEJA

18031A0501

ACKNOWLEDGEMENTS

It is needed with a great sense of pleasure and immense sense of gratitude that we acknowledge the help of these individuals. We owe many thanks to many people who helped and supported us during the writing of this report. We take privilege to express our heartfelt gratitude to Project Supervisor and our Head of the Department **Dr. G. Madhavi**, for her valuable suggestions and constant motivation that greatly helped us in successful completion of the project. We express our sincere thanks to **Prof. Ch. Srinivas Rao**, Principal, University College of Engineering Narasaraopet-JNTUK, for providing us with a good infrastructure and environment to carry out this project. We are thankful to all faculty members for extending their kind cooperation and assistance. Finally, we are extremely thankful to our parents and friends for their constant help and moral support.

ARAVAPALLI SAI RAVI TEJA

18031A0501.

CONTENTS

ABSTRACT

"Fog computing" means localizing at the edge of the network, some functions and resources that techies have developed over the years as cloud computing. Simply it is removing cloud from network core to network edge. To understand Fog computing let us try to understand cloud computing briefly.

Cloud computing can simply be described as computing platform based on the internet. In the past, people depended on physical computer storage or servers to run their programs. However, with the introduction of cloud computing, people as well as business enterprises can now access their programs through the internet.

Due to this ease, software companies and other agencies are shifting more towards cloud computing environment. Secondly, to achieve better operational efficiency in many organizations, small or medium agencies is using Cloud environment for managing their data.

Cloud computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and others which rely on the Internet. It also provides an easy way for accessing, managing and computation of user data, but it also has its own severe security risks.

Very common risks now days are data theft attacks. Data theft is considered one of the top threats to cloud computing by the Cloud Security Alliance a company deploying security solutions in the cloud.

To deal with such cases and malicious intruders there are some techniques which are used to secure user data. A new technology called “Fog computing” is gaining attention of the cloud users nowadays. Secondly, the pay-as-you-go" Cloud computing model is an efficient alternative to owning and managing private data centers (DCs) for customers facing Web applications and batch

processing. It, frees the enterprise and the end user from the specification of many details.

This bliss becomes a problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements. An emerging wave of Internet deployments, most notably the Internet of Things (IoTs), requires mobility support and geo-distribution in addition to location awareness and low latency.

Fog computing improves the Quality of service and also reduces bandwidth latency. According to Cisco, due to its wide geographical distribution the Fog computing is well suited for real time analytics and big data. Fog computing is regarded as a paradigm that extends Cloud computing and its services to the edge of the network. Similar to Cloud, Fog provides data, computes, stores, and application services to end-users. Fog, simply because the fog is a cloud close to the ground. Whereas the cloud is "up there" in the sky somewhere, distant and remote and deliberately abstracted, the "fog" is close to the ground, right where things are getting done. This simply means taking it from the network core to the network edge.

It consists not of powerful servers, but weaker and more dispersed computers of the sort that are making their way into appliances, factories, cars, streetlights and every other piece of our material culture. Cheap sensors generate lots of "big" data, and it's surprisingly useful. So-called predictive analytics lets companies like GE know which part of a jet engine might need maintenance, even before the plane carrying it has landed.

Analysts say that the future of much enterprise computing remains in the cloud, but the real transformative computing of the future is going to happen right here, in the objects that surround us—in the fog.

Fog Computing is not cannibalizing the cloud, rather it enables a new breed of applications and services, there is a fruitful relationship between the Cloud and the Fog, particularly when it comes to data management and analytics.

CHAPTER ONE

1.0 INTRODUCTION

We are all aware of the Twitter incident. Where several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed. This is an example of a data theft attack from the Cloud.

As Cloud computing achieves popularity and gain attention in business organizations. It is offering a variety of services to the users. It becomes an ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. It is now a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and others which rely on the Internet. It is seen as a delivery platform in which resources are effectively provided as a service to the client through the Internet.

The benefits are enormous. However, experts say when techniques and devices of Internet of things (IoT), get more involved in people's life, current Cloud computing paradigm would hardly satisfy their requirements of mobility support, location awareness and low latency. Limitations of the cloud would be pronounced. Apart from Security issues which range from: Data Breaches, Data Losses, Account or Service Traffic Hijacking, Insecure Interfaces and APIs, and finally Denial of Service. Others are the requirement of high capacity (bandwidth) client access link and high latency.

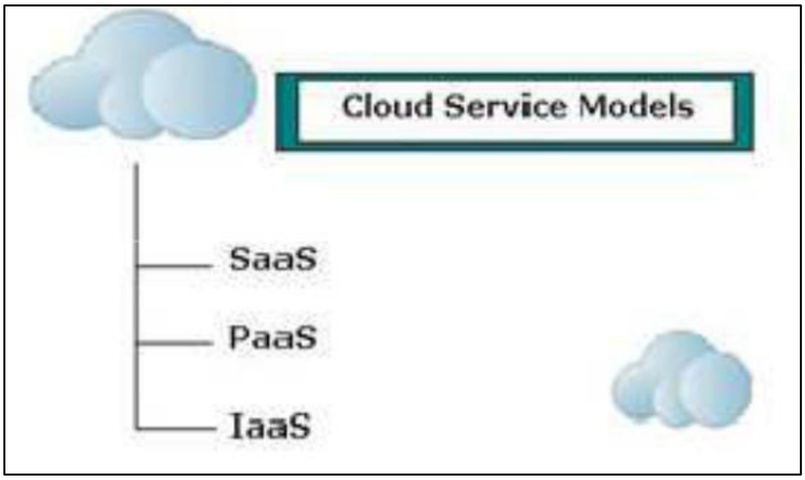
Fog Computing in extending cloud concepts to the edge of the network, is not only promising Low latency and location awareness, Wide-spread geographical distribution; Mobility; Very large number of nodes, Predominant role of wireless access, Strong presence of streaming and real time computing and Heterogeneity. It promises security to the cloud.

This paper is organized as follows. Chapter One illustrates the Application strategy and benefits of Cloud computing, it also defines the meaning of Internet of things (IoT) and the Fog as the natural component of the platform required for the support for the Internet of Things. Chapter Two introduces Fog computing paradigm and its applications in complementing Cloud computing and handling its Challenges. It also discusses fog computing strategy in providing security to Cloud. The conclusion summarizes our discussions about the state of the Fog Computing and discussion of future work.

Defining Cloud Computing

Cloud computing, I have earlier, defined as a technology that uses internet and remote servers to store information and application. It is an infrastructure that provides helpful, on demand network services to use numerous resources with less effort.

Cloud Computing is a combination of several computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and others which rely on the Internet. It is considered as a delivery platform in which resources are provided as a service to the client through the Internet.



Cloud services

The cloud computing service comes in basic models, and these are:

1) **Software as a Service (SaaS):** In this model, a pre-made application, along with any operating system, required software, network and hardware are provided. There is no requirement of purchasing a software license, and the vendors run the software application for you.
2) **Platform-as-a-service (PaaS):** The vendor provides and manages the database, operating system, and everything else needed to run on certain platforms and the customer installs or develops his own software and applications.
3) **Infrastructure as a Service (IaaS):** The customer installs or develops its own operating systems, software and applications. In this rather than purchasing data center space, software, servers, and network equipment, for these services the vendor provides and bills to clients for the number of resources consumed.

Samples of the cloud services are Yahoo e-mail, Google, Gmail and Hotmail. Others Include Amazon, IBM, Apple iTunes Shop, etc.

BENEFITS OF CLOUD COMPUTING

The benefits of cloud computing are enormous this include :

- Online development and deployment tool
- Online Manipulation and configuration of applications
- Applications serve as utilities over the internet
- No software required
- Resources are available on the network
- On demand self service
- Cost efficiency
- High flexibility and availability

The" pay-as-you-go" Cloud Computing model which is an alternative to owning and managing private data centers (DCs) for customers facing Web applications and batch processing. Cloud experts understand that several factors contribute to the economy of scale of mega DCs: higher predictability of massive aggregation, which allows higher utilization without degrading performance; convenient location that takes advantage of inexpensive power; and lower OPEX achieved through the deployment of homogeneous compute, storage, and networking components. Cloud computing frees the enterprise and the end user from the specification of many details. These are major factors of its proliferation.

Internet of things (IoT) what is it?

Cloud computing and Internet of Things (IoT) are two different technologies, which are already part of our life. Their massive adoption and use is expected to increase, making them important components of the future Internet.

The Internet of Things (IoT) is said to be a paradigm that is based on intelligent and self-configuring nodes (things) interconnected in a dynamic and global network infrastructure. It represents one of the most disruptive technologies, enabling ubiquitous and pervasive computing scenarios. IoT is generally characterized by real world and small things with limited storage and processing capacity, and consequential issues regarding reliability, performance, security, and privacy.

On the other hand, Cloud computing has virtually unlimited capabilities in terms of storage and processing power, is a more matured technology, and has most of the IoT issues at least partially solved.

Currently, it is said that there is no universally accepted definition of IoT or a “thing.” Mark Weiser pioneered the technology behind IoT in the early 1990s, and as it has evolved, the concept has been called ubiquitous computing, pervasive computing, ambient computing – and now the Internet of Things (IoT), a term RFID pioneer Kevin Ashton claims to have coined in 1999. Some of the available definitions of IoT are as follows:

Wikipedia: The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure

IEEE IoT Initiative (working draft):

i) Small environment scenario: a network that connects uniquely identifiable "Things" to the Internet; the "Things" have sensing/ actuation and potential programmability capability; Information about the "Thing" can be collected; The state of the "Thing" can be changed from anywhere, at any time, by anything.

Cisco:

ii) **Internet of Things** (IoT) is when the Internet and networks expand to places such as manufacturing floors, energy grids, healthcare…

For us to understand IoT I had to edit Bennie Cha's (a reporter with recode .net) work, she says:

Smart locks, smart thermostats, smart cars — you've probably heard some of these terms lately, and you're going to hear them even more as the year goes on. But what are these things exactly— and what makes them so *smart*? These devices are all part of an emerging category called the Internet of Things, or IoT for short. At its very basic level, IoT refers to the connection of everyday objects to the Internet and to one another, with the goal being to provide users with smarter, more efficient experiences. Some recent examples of IoT products include the Nest Protect smoke detector and August door locks. But as with any new technology, IoT can be confusing and intimidating for the average consumer, especially as debates swirl around standardization, security and privacy, and company after company piles on to this fast-growing trend. This compiled FAQ on IoT helps to explains how it works, how these products are being used in the real world, and some of the issues and challenges facing the category.

Several companies and groups working on IoT products and standards, include Apple, SmartThings, the Internet of Things Consortium, AllSeen Alliance, the Open Interconnect Consortium and the Thread Group

What Exactly Is the Internet Of Things?

IoT is therefore a network of physical objects or “Things” embedded with electronics, SW, Sensors and connectivity to enable it to achieve value and service by exchanging data with the manufacturer, operator and/or other connected devices through advanced communication protocols without human operation

Walt Mossberg of recode .net described it this way: “ a whole constellation of inanimate objects being designed with built-in wireless connectivity, so that they can be monitored, controlled and linked over the Internet via a mobile app.”

The types of objects span from a wide range of categories, wearables to light bulbs to home appliances (like the coffee maker, washing machine, and even your car) — really, anything. IoT is also being applied to vertical markets like the medical and health-care industry and to transportation systems.

Okay, how does this make things easier for me?

One of the better-known examples is the Nest thermostat. This Wi-Fi-connected thermostat allows you to remotely adjust the temperature via your mobile device and learn your behavioral patterns to create a temperature-setting schedule.

The potential value is that you can save money on your utility bill by being able to remotely turn off your air conditioner, which you forgot to do before leaving the house. There’s also a convenience factor. Nest can remember that you like to turn down the temperature before going to bed and can automatically do that for you at a set time.

Another company, SmartThings, which Samsung acquired in August, offers various sensors and smart-home kits that can monitor things like who is coming in and out of your house and can alert you to potential water leaks, to give homeowners peace of mind.

As the IoT category expands and the products become more sophisticated, one can envision a scenario where your fitness tracker detects that you’ve fallen asleep and then automatically turns off your TV and lights. Or, before hitting the road, your car could pull up your work calendar and automatically provide the best route to your meeting or send a note to relevant parties if you’re running late.

On a broader scale, it is being used by cities to monitor things like the number of available parking spaces, air and water quality, and traffic.

How does IoT work?

First, there’s the underlying technology, the various wireless radios that allow these devices to connect to the Internet and to each other. These include more familiar standards like Wi-Fi, low-energy Bluetooth, NFC and RFID, and some that you’ve probably haven’t heard of, like ZigBee, Z-Wave and 6LoWPAN (have your eyes glazed over yet?).

Then there are the things themselves, whether they’re motion sensors, door locks or light bulbs. In some cases, there may also be a central hub that allows different devices to connect to one another. Finally, there are cloud services, which enable the collection and analysis of data so people can see what’s going on and act via their mobile apps.

What companies are working on IoT?

Big names like Samsung, LG, Apple, Google, Lowe’s and Philips are all working on connected devices, as are many smaller companies and startups. Research group Gartner predicts that 4.9 billion connected devices will be in use this year, and the number will reach 25 billion by 2020.

So, can all IoT devices talk to each other?

This is where things get a little more complicated. With so many companies working on different products, technologies and platforms, making all these devices communicate with each other is no small feat — seamless overall compatibility likely won’t happen.

Several groups are working to create an open standard that would allow interoperability among the various products. Among them are the AllSeen Alliance, whose members include Qualcomm, LG, Microsoft, Panasonic and Sony; and the Open Interconnect Consortium, which has the support of Intel, Cisco, GE, Samsung and HP.

While their end goal is the same, there are some differences to overcome. For example, the OIC says the AllSeen Alliance doesn’t do enough in the areas of security and intellectual property protection. The AllSeen Alliance says that these issues have not been a problem for its more than 110 members. It’s not clear how the standards battle will play out, though many believe we’ll end up with three to four different standards rather than a single winner (think iOS and Android). In the meantime, one-way consumers can get around the problem is by getting a hub that supports multiple wireless technologies, such as the one offered by SmartThings.

These products seem to be collecting a lot of data. Should I be worried about security and privacy?

The various amounts of data collected by smart home devices, connected cars and wearable's have many people worried about the potential risk of personal data getting into the wrong hands. The increased number of access points also poses a security risk.

The Federal Trade Commission has expressed concerns and has recommended that companies take several precautions in order to protect their customers. The FTC, however, doesn't have the authority to enforce regulations on IoT devices, so it's unclear how many companies will heed its advice.

Of the companies I've talked to, all said that security and privacy were of the utmost importance. For example, Apple requires that companies developing products for its HomeKit platform include end-to-end encryption and authentication and a privacy policy. The company also said it doesn't collect any customer data related to HomeKit accessories.

After all, making sure your kids get home safe from school is one thing, but cooking a pot roast in a Wi-Fi connected crockpot is another.

Integrating Cloud and IoT

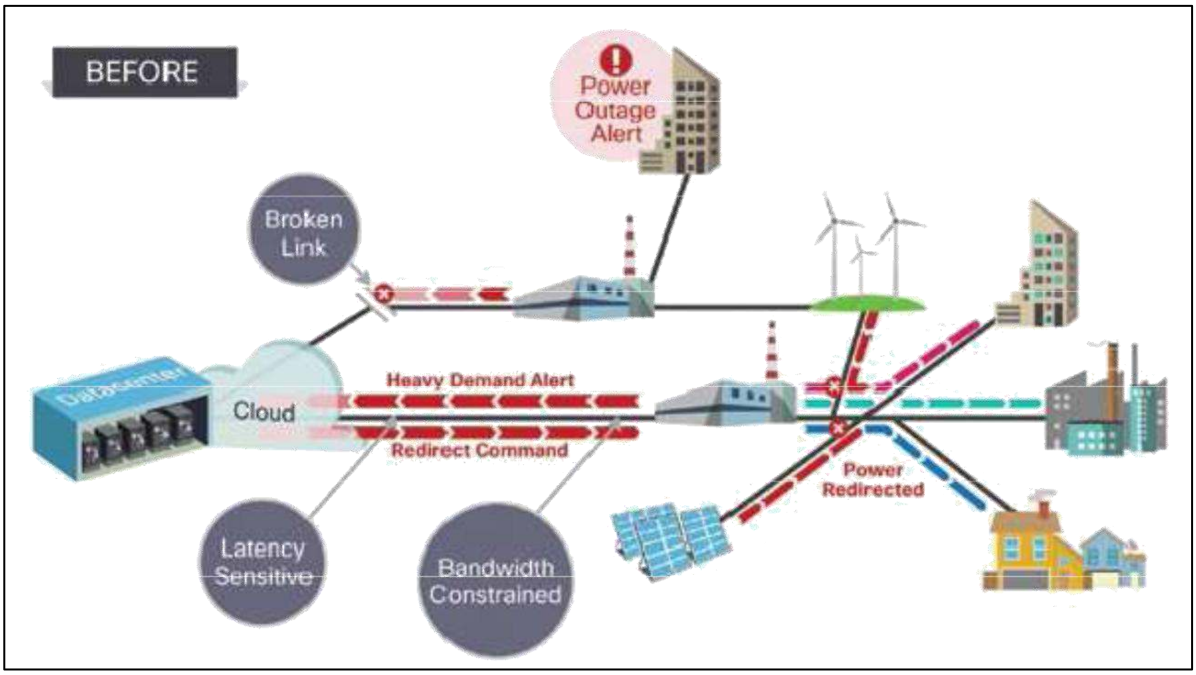
Having explained IoT we can see that the two worlds of Cloud and IoT have seen an independent evolution. However, several mutual advantages deriving from their integration have been identified in literature and are foreseen in the future. On the one hand, IoT can benefit from the virtually unlimited capabilities and resources of Cloud to compensate its technological constraints (e.g., storage, processing, energy). Specifically, the Cloud can offer an effective solution to implement IoT service management and composition as well as applications that exploit the things or the data produced by them. On the other hand, the Cloud can benefit from IoT by extending its scope to deal with real world things in a more distributed and dynamic manner, and for delivering new services in many real-life scenarios. The complementary characteristics of Cloud and IoT arising from the different proposals in literature are inspiring the CloudIoT phenomenon.

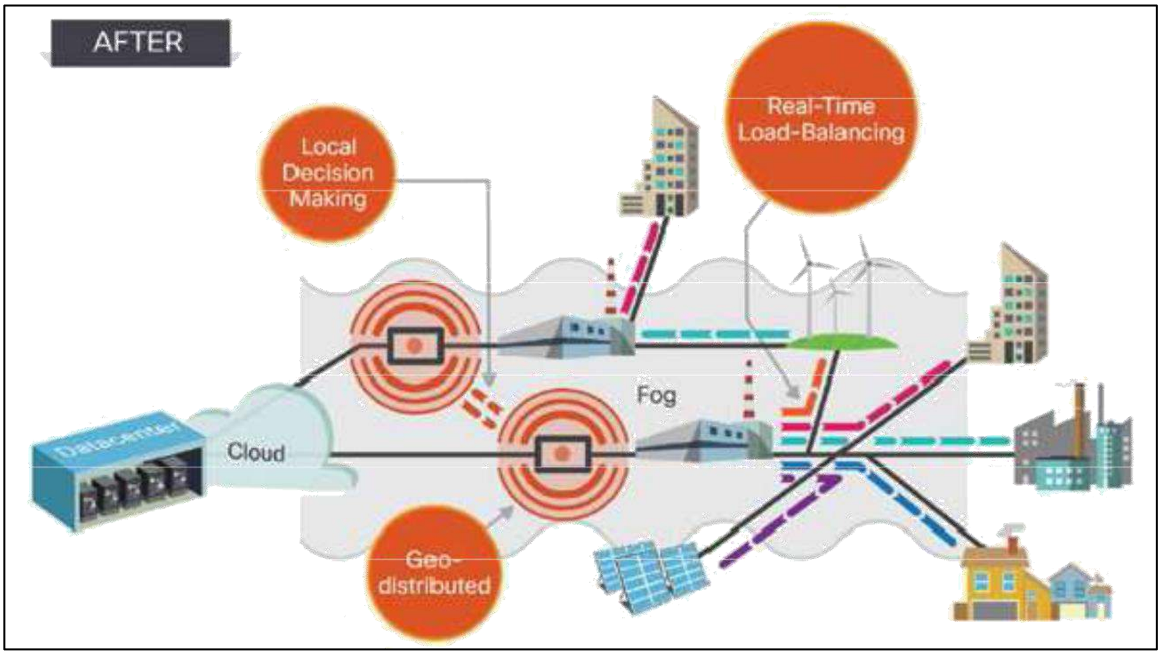
Essentially, the Cloud acts as intermediate layer between the things and the applications, where it hides all the complexity and the functionalities necessary to implement the latter. This framework will impact future application development, where information gathering, processing, and transmission will produce new challenges to be addressed, also in a multi-cloud environment.

Hence the emergence of the integration is witnessing CloudIoT paradigms such as smart services and applications which include :

- **SaaS** (Sensing as a Service), providing ubiquitous access to sensor data.
- **SAaaS** (Sensing and Actuation as a Service) enabling automatic control logics implemented in the Cloud.
- **SEaaS** (Sensor Event as a Service), dispatching messaging services triggered by sensor events.
- **SenaaS** (Sensor as a Service), enabling ubiquitous management of remote sensors.
- **DBaaS** (Databases as a Service) , enabling ubiquitous database management.
- **DaaS** (Data as a Service), providing ubiquitous access to any kind of data.
- **EaaS** (Ethernet as a Service) providing ubiquitous layer-2 connectivity to remote devices.
- **IPMaaS** (Identity and Policy Management as a Service) enabling ubiquitous access to policy and identity management functionalities.
- **VSaaS** (Video Surveillance as a Service, providing ubiquitous access to recorded video and implementing complex analyses in the Cloud.

It said that ongoing research specifies the need for Standards. Even though the scientific community gave multiple contributions to the deployment and standardization of IoT and Cloud paradigms, a clear necessity of standard protocols, architectures and APIs is being demanded in order to facilitate the interconnection among heterogeneous smart objects and the creation of enhanced services, which realize the CloudIoT paradigm. Nevertheless, security, which trails every networked environment, is a major issue for CloudIoT. Indeed, both its IoT side (i.e., Radio Frequency Identification (RFID), Wireless Sensor networks (WSN)) and its Cloud side are vulnerable to a number of attacks. In IoT context, encryption can ensure data confidentiality, integrity, and authenticity. However, it cannot handle insider attacks (e.g. during WSN reprogramming) more so it is difficult to implement on computation-constrained devices. RFID has been identified to be the most vulnerable component, since no higher level of intelligence can be enabled on it. Also, security aspects related to Cloud require attention since Cloud handles the economics, along with data and tools. Moreover, Cloud platforms need to be enhanced to support the rapid creation of applications, by providing domain specific programming tools and environments and seamless execution of applications, harnessing capabilities of multiple dynamic and heterogeneous resources, to meet Quality of Service (QoS) requirements of diverse users. Cloud scheduling algorithms need to manage task duplication for failure management, in order to deliver these services in a reliable manner. Moreover, they should be able to handle QoS parameters.


BEFORE
Power Outage Alert
Broken Link
Datacenter
Cloud
Heavy Demand Alert
Redirect Command
Power Redirected
Latency Sensitive
Bandwidth Constrained


AFTER
Local Decision Making
Real-Time Load-Balancing
Fog
Datacenter
Cloud
Geo-distributed

CHAPTER TWO

2.1. Introduction to Fog Computing:

Fog computing is an extension of classic Cloud computing to the edge of the network (just as fog is a cloud close to the ground). It has been designed to support IoT applications which is characterized by latency constraints, requirement for mobility and geo-distribution. Even though computing, storage and networking are resources of both the Computing solutions, Fog Computing, has peculiar characteristics: edge location and location awareness implying low latency; geographical distribution and a very large number of nodes when compared to centralized Cloud; support for mobility (through wireless access) , real-time interaction (instead of batch processes) and support for interplay relationship with the Cloud.

Secondly, the problem of providing security of confidential information remains a core issue that, to date has not provided the levels of assurance most people desire. It is fair to say all the standard approaches have been demonstrated to fail from time to time for a variety of reasons, including insider attacks, mis-configured services, faulty implementations, buggy code, and the creative construction of effective and sophisticated attacks not anticipated by the designers of security procedures.

Building a trustworthy cloud computing environment is not enough, because accidents do occur, and when they do, information gets lost, there is no way to get it back. Fog experts say we needs to prepare for such accidents.

A lot of research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However, these mechanisms have not been able to prevent data compromise. Van Dijk and Juels have shown that fully homomorphic encryption, often acclaimed as the solution to such threats, is not a sufficient data protection mechanism when used alone.

Fog computing proposes a completely different approach to securing the cloud using decoy information technology and user profiling. It uses this technology to launch a disinformation attack against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.

The profile technique, which is done by accumulating volumetric information of how many documents are typically read and how often, can serve to detect abnormal Cloud access. This is based partially upon the scale and scope of data transferred.

FOG Computing

By extending cloud computing to the edge of the network while providing low latency, location awareness and real time computing support, It has been designed to support IoT applications, characterized by latency constraints and requirement for mobility and geo-distribution. In Combining User Behavior Profiling with Decoy Technology for Masquerade Detection, this is the solution that fog computing is using to complement the cloud and extend security to it. Herald! Pervasive Computing.

Goals of Fog Computing:

There are several designing goals for an adequate fog computing platform.

1. Latency: It is fundamental for fog computing platform to offer end user low-latency-guaranteed applications and services. The latency comes from the execution time of a task, the task offloading time, the time for cyber foraging and speed of decisions making, etc.
2. Efficiency. While at first glance the efficiency may have its own impact on latency, it is more related to the efficient utilization of resources and energy. The reasons are obvious and quite different from counterparts in cloud computing scenarios:

   a) not all fog nodes are resource rich; some of them have limited computation power, memory and storage.

   b) most of fog nodes and clients are battery-powered, such as hand-hold devices, wearables, and wireless sensor units.
3. Generality. Due to the heterogeneity of fog node and client, we need provide same abstract to top layer applications and services for fog clients. General application programming interfaces (APIs) should be provided to cope with existing protocols and APIs (e.g. Machine-2-machine protocols, smart vehicle/smart appliance APIs etc.

Applications of Fog Computing:

Experts say that the most helpful way to look at the fog concept is to examine specific **use cases applied to the IoT**. In certain cases, it may well be best to move towards a localized or partially localized resource - and in other circumstances, it might all be best uploaded to a web-scale cloud platform. One component in fog could be ‘smarter' routers with more application-level functionality - so long as the security is fit for purpose.

Smart Grid: 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 will automatically switch to alternative energies like solar and wind. 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.

Smart Traffic Lights and Connected Vehicles: Video camera that senses an ambulance flashing lights can automatically change streetlights to open lanes for the vehicle to pass through traffic. Smart streetlights interact locally with sensors and detect presence of pedestrian and bikers, to measure the distance and speed of approaching vehicles.

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.

Wireless Sensor and Actuator Networks:

It is said that 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 device can control the measurement process itself, the stability and the oscillatory behaviors by creating a closed loop.

Decentralized Smart Building Control:

The applications of this type are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases 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 techniques at Fog devices to react to data Fog computing extends the Cloud Computing solutions to applications and services. Its defining characteristics include,

a) Low latency and location awareness.
b) Wide-spread geographical distribution.
c) Mobility.
d) Very large number of nodes,
e) Predominant role of wireless access,
f) Strong presence of streaming and real time
g) Heterogeneity.

Fog Computing enables a new breed of devices, particularly when it comes to data management and analytics. The use of wide spread of Edge network can be shown in the Internet Of Things.

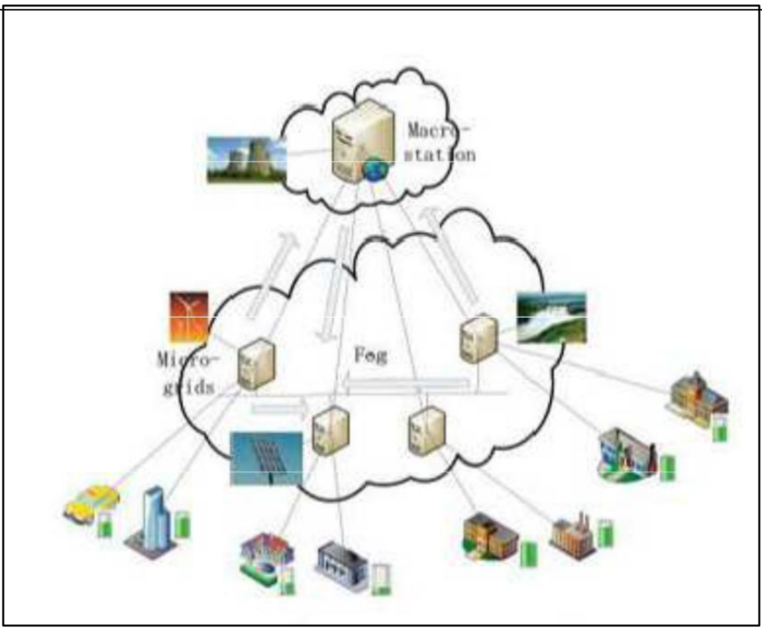


Figure presents the idealized information and computing role of Fog Computing. Compute, storage, and networking resources are the building base of Fog. Edge of the Network", however, implies several characteristics that Cloud do not offer.

Let us list some of the pointers and motivating examples as represented in the IJECE journal:

(**International Journal of Electrical and Computer Engineering (IJECE)**)

Edge location, location awareness, and low latency. The origins of the Fog can be traced to early proposals to support endpoints with rich services at the edge of the network, including applications with low requirements (e.g., gaming, video streaming, augmented reality).

Geographical distribution: In sharp contrast to the more centralized Cloud, Fog demand widely distributed deployments.

Large-scale sensor networks to monitor the environment, and the Smart Grid are other examples of inherently distributed systems, requiring distributed computing and storage resources.

Support for mobility: It is essential for many Fog applications to communicate directly with mobile devices therefore support mobility techniques, such as the LISP protocol 1, that decouple host identity from location identity, and require a distributed directory system

Interoperability and federation: Seamless support of certain services (streaming is an example) requires the cooperation of different providers

Fog computing is a term for an alternative to cloud computing that puts some kinds of transactions at the edge of a network, rather than establishing channels for cloud storage and utilization. Proponents of fog computing argue that it can reduce the need for bandwidth by not sending every bit of information over cloud channels, and instead aggregating it at certain access points, such as routers. This allows for a more strategic compilation of data that may not be needed in cloud storage right away, if at all. By using this kind of distributed strategy, project managers can lower costs and improve efficiencies.

For example, some experts use the example of a high-performance piece of equipment that generates a lot of data about its performance and use. When this data does not need to be sent to the cloud, it can be sent to fog computing systems and aggregate it somewhere near the edge of the network. Fog computing also has applications related to the Internet of things (IoT), which describes systems in which more and more appliances and pieces of equipment are connected to the global Internet.

The main Feature of Fog Computing is its ability to support applications that require low latency, location awareness and mobility. This ability is made possible by the fact that fog computing systems are developed closer to the End users in a widely disturbed manner. Fog computing nodes thus hosted possess sufficient computing power and storage capacity to handle the resource intensive user request.

Bandwidth problems

Experts have discussed Fog computing architecture and further used it for improving Web site's performance with the help of edge servers. They said that the emerging architecture of Fog Computing is highly virtualized. They presented that their idea that the Fog servers, monitor the requests made by the users and keep a record of each request by using the user’s IP address or MAC address. Furthermore, when a user requests for same website increases than a given number (N is tunable parameter) then the user’s browser can cache the common CSS and JS files and then onwards send them externally. They also mentioned that it is possible to measure page rendering speed with the help of snippets.

Perhaps someday 100% of data may reside in the cloud. However, the truth is, getting data into and out of the cloud is harder than most engineers, or at least their managers, often are willing to admit**. The problem is bandwidth**. If you're company is simply seeking to save the cost and headache of storing data, the cloud is great as long as all you need to do is transfer data back and forth via high-speed wiring or network.

In a world of mass connectivity, in which people need to get information on an array of mobile devices bandwidth is pretty slow from the network core. Any business that sends data to mobile devices, be it airline reservation systems for consumers or business data for a mobile sales force, grapples with the limitations of wireless networks.

Fog Security

The problem of providing security of confidential information remains a core security problem that, till date, has not provided the level of assurance that people desire. Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls. It is fair to say all the standard approaches have been demonstrated to fail from time to time for a variety of reasons including, insider attacks, mis-configured services, faulty implementation buggy code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures.

Cloud services are typically made available via a community cloud, private cloud, hybrid cloud or public cloud. General services provided by a public cloud will be offered over the internet and are operated and owned by a cloud service provider. Some examples include services at the general public, such as e-services, or social networking sites. The infrastructure is operated solely for a specific organization or a third party. In a cloud community, several organizations share the service and are made available only to those groups. The cloud service provider may be own and operate the infrastructure.

The users use to store personal data, business information in the cloud computing. With this are security challenges arrived in computing that the data in cloud i.e., the personal information and business information is attacked. To overcome this, Fog computing implements decoy information to secure data in the cloud. This technology launches disinformation against malicious insiders, preventing real sensitivity data to worthless data.

The twitter incident mentioned earlier where the attacker used a Twitter administrator's password to gain access to twitter's corporate documents hosted on Google's infrastructure as Google Docs is an accident. One needs to prepare for such accidents. The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen information to the attacker. This can be achieved through a fog's preventive' disinformation attack.

Fog Security strategy uses two methods for effective defense, these are user profiling and Decoys to secure their users information.

User Behavior Profiling: Given that access to a user's information will exhibit normal access. User profiling is a well-known technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security check is commonly used in fraud detection applications. Such profiles would naturally include volume of information accessed, how many documents are typically read and how often.

Secondly, legitimate users of a computer system are familiar with the position of their files on a system. Any search for specific files is likely to be targeted and limited. A masquerade, however, which gets access to the victim's system illegitimately, is unlikely to be familiar with the structure and contents of the file system. Their search will be widespread and untargeted. Based on these key assumptions, they profile user search behavior and developed user models trained with a one class Modeling technique, namely one-class support vector machines. The importance of using one-class modeling stems from the ability of building a classifier without having to share data from different users. The privacy of the user and their data is therefore preserved.

Decoys: Decoy information, using decoy documents, honey-files, honeypots, and other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's ex-filtrated information. Serving decoys will confound and confuse an adversary into believing they have useful information, when they have not. This technology is usually integrated with user behavior profiling technology to secure a user's information in the Cloud.

This technique places traps within the file system. The traps are decoy files downloaded from a Fog computing site, an automated service that offers several types of decoy documents such as tax return forms, medical records, credit card statements, e-bay receipts, etc. The decoys, then, serve dual purposes:

1) To validate whether data access is authorized when abnormal information access is detected.
2) To Confuse the attacker with bogus information. The decoy documents carry a keyed-Hash Message Authentication Code (HMAC) usually hidden in the header section of the document and computed over the file's contents using a key unique to each user.

The advantages are:

a) The detection of masquerade action.

b) The confusion of the attacker with the additional costs incurred to distinguish real from bogus information.

c) The deterrence effect which plays a significant role in preventing masquerading action by risk-averse attackers.

How HMAC works

A hash function h(m) is a message digest; in some sense, the message is condensed. Hash functions are routinely used to check integrity or for error detection of transmitted messages. For any communication between Nkechi and Bola they must agree on a hash function. This is how it is done.

If Nkechi is sending a message to Bola, she would create a hash of the message and transmit it along with the message. After receiving the message, Bola creates a hash message that she received using the hash function that she and Nkechi have agreed to use. The two hashes should be the same. If they are, Bola can assume that the message has not been altered intentionally or unintentionally during transmission. Technically, hash functions allow authentication to occur without double encryption of the entire message. An illustration below explains this.

When Nkechi and Bola agree on a hash function. Then Nkechi can (for security) send her message using Bola’s public key. Also, she creates a hash of the plaintext and (for authentication) sends it using her private key. Using her private key, Bola decrypts the ciphertext encrypted with her public key and creates a hash of the plaintext using the hash function that she and Nkechi have agreed to use. Bola also decrypts the ciphertext of the hash using Nkechi’s public key. The two hashes should be the same. If they are, Bola then assumes that the message is secure and that it came from Nkechi.

Message authentication codes (MAC) check both integrity and authenticity. MACs require the parties in the communication to agree on an algorithm and possess a secret key. The MAC algorithm uses the secret key and the message as input, and it outputs a message authentication code. Authorized receivers who possess the secret key can input the key and the message that they received and check their calculation of the MAC against the MAC transmitted with the message.

If the two MACs agree, the receiver can be fairly sure of both the integrity and authenticity of the message.

Cryptographic hash functions and block ciphers are often used to construct MAC algorithms. Cipher suites typically contain key exchange algorithms, signature algorithms, and cryptographic hash functions.

Hash functions should accept messages of any length as input, produce a fixed-length output, and be fast. A hash function that will be used for cryptographic purposes should have some other properties:

- It should be one-way. Knowing an output h of the hash function it should computationally be infeasible to find a message m which hashes to that output, i.e., for which h(m) = h. (This property is called pre-image resistant.)
- It should also be second pre-image resistant – give n a message m1, it should be computationally infeasible to find another message m2 with m m 1 2 ≠ having h h (m m 1 2) =( ) .
- It should be strongly collision free. It should be computationally not feasible to find two different inputs that have the same hash; i.e., it should be computationally not feasible to find messages m m 1 2 ≠ having h h (m m 1 2) = ( ) .

Normally, the number of inputs is much larger than the number of outputs; so, collisions will occur but collisions should be unlikely. There are two widely used families of cryptographic hash functions

- the MD family (MD = message digest) and
- the SHA family (SHA = secure hash algorithm).

Rivest and RSA laboratories developed MD4 and now MD5. The original MD has never been published; MD2 was the first of the family to appear, and it was followed by MD4. The National Security Agency developed SHA-1 and SHA-2. Around February 2005, problems with SHA-1 became public.

The use of search behaviour anomaly detection with trap-based decoy files should provide stronger evidence of intrusion, and therefore improve a detector's accuracy. Experts hypothesize that detecting abnormal search operations performed prior to an unsuspecting user opening a decoy file will corroborate the suspicion that the user is indeed impersonating another victim-user.

This use case covers the threat model of illegitimate access to Cloud data. More so, an accidental opening of a decoy file by a legitimate user might be recognized as an accident if the search behavior is not deemed abnormal. In other words, detecting abnormal search and decoy traps together may make a very effective masquerade detection system.

To overcome error, fog computing provides solution that suggest that user profiles are accurate enough to detect unauthorized Cloud access .When such unauthorized access is detected, one can respond by presenting the user with a challenge question or with a decoy document to validate whether the access was indeed unauthorized, similar to how we used decoys in a local file setting, to validate the alerts issued by the anomaly detector that monitors user file search and access behaviour. Combining these two techniques helps to improve detection accuracy.

Why Fogging?

Fog developers believes its model provides benefits in advertising, computing, entertainment and other applications, well positioned for data analytics and distributed data collection points. End services like, set-up-boxes and access points can be easily hosted using fogging. It improves QoS and reduces latency. The main task of fogging is positioning information near to the user at the network edge.

Fogging Advantages:

1. It reduces data movement across the network resulting in reduced congestion, cost and latency, elimination of bottlenecks which results from centralized computing systems, improved security of encrypted data as it stays closer to the end user while reducing exposure to hostile elements and improved scalability arising from virtualized systems.
2. It removes the core computing environment, thereby reducing a major block and a point of failure.
3. It improves the security, since data is encoded as it is moved towards the network edge.
4. Edge Computing, in addition to providing sub-second response to end users, will also provide high levels of scalability, reliability and fault tolerance.
5. It will consume less amount of band width.

Fogging Disadvantages:

It suffers certain limitations on the selections of technology platforms, web applications or other services.

Cloud Computing vs Fog Computing

Architects of Fog Computing claim that it is going to complement Cloud, however a comparison as illustrated from Table 1 and Table 2 mostly with the IoT or IoE, can be seen that Cloud Computing characteristics have very severe limitations with respect to quality of service demanded by real time applications resulting from IoT which require almost immediate action by the server.

Table 1:

Requirements	**Cloud Computing**	**Fog Computing**
Latency	High	Low
Delay Jitter	High	Very low
Location of Service	Within the internet	At the edge of the local network
Distance between client and server	Multiple hops	One hope
Security	Undefined	Can be defined
Attack on data enroute	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 interactions	Supported	Supported
Real time interactions	Supported	Supported
Type of last mile connectivity	Leased line	Wireless

Table 2:

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 network edge. So it consumes less time.
Problem of bandwidth, as a result of sending every bit of data over cloud channels.	Less demand for bandwidth, as every bit of data's were aggregated at certain access points instead of sending over cloud channels.
Slow response time and scalability problems as a result of depending servers that are located at remote places.	By setting small servers called edge servers in visibility of users, it is possible for a fog computing platform to avoid response time and scalability issues.

Analysis of Fog Computing in the Age of IoT

Fog computing performs better than cloud computing in meeting the demands of the emerging paradigms. But experts say, it cannot totally replace cloud computing as it will still be preferred for **high end batch processing** jobs that are very common in the business world.

Hence, we can say that fog computing and cloud computing will complement each other while having their own advantages and disadvantages. Edge computing plays a crucial role in Internet of Things (IoT). Studies related to security, confidentiality and system reliability in the fog computing platform is absolutely a topic for research and will be allowed to evolve and be discovered. Fog computing will g row in helping the emerging network paradigms that require faster processing with less delay and delay jitter and security while cloud computing would serve the business community meeting their high-end computing demands lowering the cost based on a utility pricing model

In the emerging markets

Sandeep Mathur writing about the emerging markets stated in Forbes magazine that, ("In the United States, cloud computing is essentially an additional—albeit welcome—option for businesses to choose (or not) from a mature palette of available technologies. In India, cloud is still viewed as a somewhat disruptive force. Many businesses, academic communities, and even governments are excited about the scalability, flexibility, and utility-based pricing that cloud offers. At the same time, they're concerned about the social and economic challenges presented by this new computing paradigm.

Spotlighting the contrast in another way, cloud adoption by U.S. businesses tends to be driven by the economic considerations of individual organizations. In India, whenever cloud is discussed, cost is of course important. However, cloud is also thought of within the context of India's focus on achieving its developmental goals. Namely, how can cloud help India grow its economy and enhance its standing as a global leader in innovation?

For India, cloud appears to be an obvious fit, as it can help remove barriers to costly technology, opening opportunities for new services and products. A key objective is to encourage small business owners, new entrepreneurs, non-profit organizations and academia to collaborate and share knowledge.

We like to say that, as a nation, the cloud is the force-multiplier that India must embrace with purpose and clarity.

OK, now that I've discussed the perspective that will inform attendees of Oracle Cloud World New Delhi, let's look at developing-nation adoption within a global context. In its IDC Predictions 2014, the market research firm International Data Corp. predicts that worldwide spending on the cloud, including cloud services and enabling technologies, will grow by 25% in 2014, reaching a staggering $100 billion.

Emerging markets, unburdened by the legacy of older systems in their IT infrastructure, have historically leapfrogged more mature markets. They have the potential to be nimbler in embracing new technologies. Historically, we've seen this pattern most notably in mobile communications and mobile business applications. Cloud similarly offers an opportunity for far-sighted countries to achieve leadership positions.

However, adoption curves aren't uniform across all emerging markets, according to research from the BSA (formerly known as the Business Software Alliance). As the 2013 BSA Global Cloud Computing Scorecard [PDF download] notes, the so-called BRICS countries—Brazil, Russia, India, China, and South Africa—take up the rear in implementing policies considered crucial to incentivizing cloud adoption. All stand at the bottom half of 24 countries in the survey, which also make up 80% of the market for information and computing technologies (ICT) worldwide. (ICT is an acronym which originated in England and is generally used outside of the U.S., where IT is preferred.) As a recent analysis from the World Trade Organization [PDF download] makes clear, the following implications of the cloud are hard to ignore, especially for an India that is developing rapidly:

- The cloud has the potential to catalyze greater competition to produce value-added products of much higher quality as goods and services in the world economy become ever more dependent on ICT.
- ICT riding on the cloud is crucial to making the knowledge economy a reality. Cloud offers an important mechanism for emerging economic blocs like the BRICS nations to expand global trade. It's also key to so-called "South-South" commerce (i.e., trading between developing nations).
- Small and medium enterprises (SMEs) empowered by the cloud can stimulate job creation faster and reduce barriers to new products and business models.
- The cloud can help governments expand scale in their ability to deliver core services more economically and effectively to citizens in healthcare, telecommunications, education, financial access, and other services aimed at meeting social equity goals.

Such unlimited potential is why cloud is beginning to catch fire here. Indeed, we're already seeing numerous, promising examples of adoption.

Companies like MakeMyTrip.com, Flipkart.com and Bookmyshow.com are already leveraging the benefits of the Oracle Cloud for their businesses feeding into opportunities offered by a rapidly expanding ecommerce market in India. According to a Forrester Research report, ecommerce revenues in India are projected to reach $8.8 billion by 2016, up five-fold from $ 1.6 billion in 2012.

In other sectors, we are also seeing many successful experiments in the Indian marketplace. For example, cloud-based email and mobile applications are helping make public healthcare delivery much more effective. Indian farmers are beginning to apply cloud to support access data—literally—in the middle of their fields, obviated the need to stop work to go and access a centralized computing resource. Such successful proof-points are expected to encourage replication across the entire agricultural sector.

At Oracle, we have been part of this gradual shift in the way India is adopting these technologies and shown how this new approach to using technology can allow India to become far more competitive in the global marketplace.

The examples I've cited are part of a narrative that's strengthening and becoming part of mainstream conversation in India. The discussion, and many use cases, will take center stage at Oracle Cloud World New Delhi. If you can't be there, I'll try to return to this space with a follow-up post discussing the event, where leaders of organizations large and small will share success stories of how cloud adoption has helped to transform their businesses.")

CONCLUSION

Although cloud computing represented the first breakthrough in vaporized technology, the fog promises to take hardware and software virtualization back down to earth, where it belongs.

When it comes to agility, cost and security, the cloud has long been the gold standard for technological experts, in search of a reliable off-site infrastructure. But one of the fog's greatest value propositions is the promise of tightened security due to decreased visibility (use of stenography).

Experts say that "there's less transparency in the fog, and that's a good thing in terms of protecting data. Of course, it's easy to get lost in the murky exhaust of a new technology, and it'll be an adjustment period as we adapt to an even more nebulous infrastructure model."

As of late, the cloud has weathered its fair share of criticism for being over-rated, undefined, and little more than a metaphor, say cisco bloggers. But champions of the fog hope to keep the conversation grounded.

Fog proponents are "sure, fog computing has its drawbacks, namely that its peak performance as in the real fog is in the early morning hours. But I'm confident it's only a matter of time before it begins to really take shape."

As IoT becomes prevalent, because of the rapid increase of connected devices, two main challenges will emerge. Reliable communication will not always be possible due to network congestion or simply bad connections.

Secondly, poor network connections will be an issue particularly for short-range wireless devices. It could cost billions to implement geographically distributed wireless networks that will allow sensors to send real-time data back to the cloud. Some classes of connected devices such as remote health monitoring and emergency services require very low latency. Sending data to the cloud and back to the application would negatively play on the performance of these services.

Fog computing proponents believe that it resolves problems related to congestion and latency. It provides compute, storage, and network services at the network edge. It also provides an intelligent platform to manage the distributed and real-time nature of emerging IoEor IoT infrastructures.

Moreover, its security strategy is a welcome innovation worth trying. Cisco Development group believe that, developing these services at the edge through fog computing will lead to new business models and opportunities for network and IT operators.

REFERENCES

1. C. Atkins et al. A Cloud Service for End-User Participation Concerning the Internet of Things. In Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on. IEEE, 2013.

2. Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010.[Online].Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

3. D. Danchev, "ZDNET: French hacker gains access to twitter's admin panel," April 2009. [Online]. Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwitters- admin-panel/3292.

4. D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010.[Online].Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked-twitter-documents-to-techcrunch-isbusted.

5. F. Alagoz et al. From cloud computing to mobile Internet, from user focus to culture and hedonism: the crucible of mobile health care and wellness applications. In ICPCA 2010. IEEE, 2010.

6. G. Aceto, A. Botta, W. De Donato, and A. Pescap`e. Cloud monitoring: A survey. Computer Networks, 57(9):2093–2115, 2013.

7. I. F. Akyildiz, W. Su, Y. Sankar Subramaniam, and E. Cayirci. Wireless sensor networks: a survey. Computer networks, 2002.

8. M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online].Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidential-twitter-documents.

9. M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10.Berkeley, CA, USA:

USENIX Association, 2010, pp. 1–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934.

10. P. Allen, “Obama’s Twitter password revealed after French hacker arrested for breaking into U.S. president’s account,” March 2010. [Online].Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas Twitter-passwordrevealed-French-hacker-arrested.html.

11. P. Ballon, J. Glidden, P. Kranas, A. Menychtas, S. Ruston, and S. Van Der Graaf. Is there a need for a cloud platform for European smart cities? In eChallenges e-2011 Conference Proceedings, IIMC International Information Management Corporation, 2011.

12. **R. K. Awosan ,** Factor Analysis of the Adoption of Cloud Computing In Nigeria**, African Journal of Computing & ICT Vol 7. No. 1 - January, 2014 [Online] Available** http://www.ajocict.net/uploads/V7N1P4-2014_AJOCICT_-_Paper_4.pdf

13. **Sandeep Mathur**, “Cloud computing is a force-multiplier-for-emerging-markets”http://www.forbes.com/sites/oracle/2014/01/09/cloud-computing-is-a-force-multiplier-for-emerging-markets/

14. **Stephan Monterde**, Fog Computing Tracking technology trends that will change the future of the industry. Fostering innovation pg 19-21 2014 Available https://techradar.cisco.com/pdf/cisco-technology-radar.pdf

15. Thogaricheti Ashwini and Mrs. Anuradha S. G. ‘Fog Computing to protect real and sensitivity information in Cloud’ International Journal of Electronics and Computer Science Engineering **Available IJECSE, Volume 4, Number 1 http//www.IJECE.org**