International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.04,Issue.14,
June-2015,
Pages:2620-2626

www.ijsetr.com

Perspective of Decoy Technique using Mobile Fog Computing with Effect to Wireless Environment

SIDDHESH P. KAREKAR[1], SACHIN M. VAIDYA[2]

[1]PG Scholar, Dept of MCA, A.C Patil College of Engineering, Navi Mumbai, India.
[2]Assistant Professor, Dept of MCA, A.C Patil College of Engineering, Navi Mumbai, India.

Abstract: Cloud computing offers to significantly change the way we use computers and access and store our personal data and business information. New computing, communications paradigms arise new data security challenges. Existing data security mechanisms like encryption were not successful in securing data manipulation attacks, especially those committed by an insider to the cloud provider. I propose a distinct approach for data security in the cloud using violative and extensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. In this paper we present a new paradigm for securing computational resources which we call decoy technology. This technique involves seeding a system with data that appears authentic but is in fact spurious. Attacks can be detected by monitoring this phony information for access events. Decoys are capable of detecting malicious activity, such as insider and masquerade attacks, that are beyond the scope of traditional security measures. They can be used to address confidentiality breaches either proactively or after they have taken place.

Keywords: CISCO, Cloud Computing (CC), Mobile Computing (MC), Mobile Cloud Computing (MCC).

I. INTRODUCTION

Organizations across the globe are becoming increasingly aware of the importance of securing their Clouds. As a consequence, worldwide sales of security software rose by 7.5% in 2011. Government agencies are particularly conscious of the need to defend their computing infrastructure. This is exemplied by the fact that the United States government increased funding for cyber security research by 35% from 2011 to 2012.Attentiveness to security practices has also risen at the individual level, as 90% of American adults now believe that a safe Internet is critical to the U.S. economy. The market of mobile phones has expanded rapidly. According to IDC, the premier global market intelligence firm, the worldwide Smartphone market grew 42.5% year over year in the first quarter of 2012. The growth of mobility has changed our lives fundamentally in an unprecedented way. According to Cisco IBSG, close to 80 percent of the world's population has access to the mobile phone and new devices like the iPhone, Android Smartphone, palmtops and tablets have brought a host of applications at the palms of people's hands.

At the same time, Cloud Computing has emerged as a phenomenon that represents the way by which IT services and Functionality are charged for and delivered. NIST (National Institute of Standards and Technology, USA) definition from September, 2011 released in its "Special Publication 800-145" of Cloud Computing is "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, applications and services) that can rapidly be provisioned and released with minimal Management effort or service provider interaction." Fog computing provides- Low latency and location awareness, it has Wide-spread geographical distribution, supports Mobility, is compromised due to the huge number of nodes. The main task of fog is to deliver data and place it closer to the user who is positioned at a location which at the edge of the network. Here the term edge refers to different nodes to which the end user is connected and it is also called edge computing. If we look according to architecture fog is situated below the cloud at the ground level. The term fog computing is given by CISCO as a new technology in which mobile devices interact with one another and support the data communication. Mobile devices (e.g., Smartphone, tablet pcs, etc) are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate rich experience of various services from mobile applications (e.g., iPhone apps, Google apps, etc), which run on the devices and/or on remote servers via wireless networks.

The rapid progress of mobile computing (MC) becomes a powerful trend in the development of IT technology as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security). The limited resources significantly impede the improvement of service qualities. Cloud computing (CC) has been widely recognized as the next generation's computing infrastructure. CC offers some

advantages by allowing users to use infrastructure (e.g., servers, networks, and storages), platforms (e.g., middleware services and operating systems), and softwares (e.g., application programs) provided by cloud providers (e.g., Google, Amazon, and Sales force) at low cost. In addition, CC enables users to elastically utilize resources in an on-demand fashion. As a result, mobile applications can be rapidly provisioned and released with the minimal management efforts or service provider's interactions. With the explosion of mobile applications and the support of CC for a variety of services for mobile users, mobile cloud computing (MCC) is introduced as an integration of cloud computing into the mobile environment. Mobile cloud computing brings new types of services and facilities for mobile users to take full advantages of cloud computing.

II. FOG COMPUTING

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. 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.

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 is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, compute, storage, and application services to end-users. The difference is Fog provides proximity to its end users through dense geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network. Fog computing improves the Quality of service and also reduces latency. According to Cisco, due to its wide geographical distribution the Fog computing is well suited for real time analytics and big data. While Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization. Madsen.H and Albeanu. G presented the challenges faced by current computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is mainly done for the need of the geographical distribution of resources instead of having a centralized one.

A multi-tier architecture is followed in Fog computing platforms. In first tire there is machine to machine communication and the higher tiers deal with visualization and reporting. The higher tier is represented by the Cloud. They said that building Fog computing projects are challenging .But there are algorithms and methodologies available that deal with reliability and ensure fault tolerance. With their help such real life projects are possible. Z. Jiang et al. 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. Godoy et al. explained that there is a need of such profiling strategies or methods through which user profiling can be done. As there is a huge amount of information available on the web or Internet therefore from last few years personal information agents are helping the users to manage their information. They said earlier only supervised learning technique was used in general. But for moving the information agents to the next level authors are focusing on assessment of semantically useful user profiles. They said that account hijacking is a disadvantage for such user profiling.

Sabahi, F. mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. He discussed about the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology offering the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown. Considering all these requirements, this prototype is created which includes two main steps: first is to create users and generate patterns of their different access behaviors, next step is monitoring the user access patterns which is done using CUSUM that is cumulative summation algorithm to find the accuracy of the procedure.

A. Applications of Fog Computing

1. Smart Grid:

- 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.
- 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.

2. Smart Traffic Lights and Connected Vehicles:

- 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.
- 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 WiFi, 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.

3. 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 behaviours 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.

4. Decentralized Smart Building Control:

- 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.

III. DECOY TECHNIQUE

Decoys are typically thought of as larger- scale, lower fidelity systems intended to change the statistical success rate of tactical attacks. The basic idea is to fill the search space of the attacker's intelligence effort with decoys so that detection and differentiation of real targets becomes difficult or expensive. In this approach, the attacker seeking to find a target does a typical sweep of an address space looking for some set of services of interest. DWALL and Responder are also useful for high fidelity deceptions, but these deceptions require far more effort. Tools like "Nmap" map networks and provide lists of available services, while more sophisticated vulnerability testing tools identify operating system and server types and versions and associate them with specific vulnerabilities. Penetration testing tools go a step further and provide live exploits that allow the user to semi-automatically exploit identified vulnerabilities and do multistep attack sequences with automated assistance. These tools have specific algorithmic methods of identifying known systems types and vulnerabilities, and the characteristics of the tools are readily identified by targets of their attacks if properly designed for that purpose.

The defender can then simulate a variety of operating systems and services using these tools so that the user of the attack tools makes cognitive errors indirectly induced by the exploitation of cognitive errors in their tools. The deceived attacker than proceeds down defender- desired attack graphs while the defender traces the attacks to their source, calls in law enforcement or other response organizations, or feeds false information to the attacker to gain some strategic advantage. In at least one case, defenders included Trojan horse components in software placed in a honeypot with the intent of having that software stolen and used by the attackers. The Trojan horse contained mechanisms that induced covert channels in communication designed to give the so called defenders an attack capability against the (so-called) attackers' systems. Of course not all decoys are so high quality. Simple decoys like Deception ToolKit are simple to detect and defeat. Yet after more than seven years of use, they are still effective at detecting and defeating low quality attackers that dominate the attack space.

Such tools are completely automatic and inexpensive to operate, don't interfere with normal use, and provide clear detailed indications of the presence of attacks in a timely fashion. While they are ineffective against high skills attackers, they do free up time and effort that would otherwise be spent on less skilled attackers. This is similar to the effectiveness of decoys in military systems. Just as typical chaff defeats many automated heat or radar seeking attack missiles, simple informational deceptions defeat automated attack tools. And just as good pilots are able to see past deceptions like chaff, so skilled information attackers are able to defeat see past deceptions like Deception ToolKit. And just as chaff is still used in defeating missiles despite its

limitations, so should simple deceptions be used to defeat automated attack tools despite their limitations. As long as the chaff costs less than the risks it mitigates, it is a good defense, and as long as simple deceptions reduce risk by more than the cost to deploy and operate them, they are good defenses as well. Higher quality decoys are also worthwhile, but as the quality of the decoy goes up, so does its cost. While some of the more complex decoy systems like DWALL provide more in- depth automation for larger scale deceptions, the cost of these systems is far greater than Deception ToolKit as well. Lower fidelity systems like IR or Responder cost under $10,000 and cover the same sized address space. While Responder and IR can be used to implement the DWALL functions, they also require additional hardware and programming to achieve the same level of fidelity. At some point the benefits of higher fidelity decoys are outweighed by their costs.

A. Properties of Decoy

- It is easy to see that some decoy material is more applicable to certain scenarios than others. Similarly, certain genres of decoys may be more applicable to specific corporate environments. In order to design decoys that are as effective as possible, it is also beneficial to analyze them in a more general sense by considering characteristics that are independent of a particular context. As initially explored by Bowen et. al in , several abstract properties exist that define how a decoy should operate under ideal circumstances. Some of these attributes concern the relationship between adversaries and decoy data, while others pertain to the interactions between legitimate users and deceptive material.
- A perfectly believable decoy "would precisely conform to all of these guidelines, though practical restrictions prevent this from occurring in most situations. Although there exists some overlap between these traits, it is also worth noting that they are not completely orthogonal. For example, believability and differentiability are in contention to some extent.

B. Believability:

- One of a decoy's primary functions is to be believable. Upon inspection, a decoy should appear authentic and trustworthy. In the absence of any additional information, it should be impossible to discern a spurious decoy from authentic data.
- Believability can be formalized via the following thought experiment. Consider a pool of files, some of which contain real data and some of which are fabricated decoys. Select a decoy file and real piece of data from this pool, and present it to an adversary.
- The selected decoy can be considered perfectly believable if this attacker has an equal probability of selecting the decoy and the legitimate document. This characteristic is of critical importance to externally observable features of decoys.
- In comparison, the believability of document content is of a lower priority. This is because an attacker would have already triggered an alert when opening the document by the time this information came in to play.

C. Enticingness:

- This property takes our idealized decoy material one step further. Decoys should not only appear valid, but also attract an adversary's attention.
- This, of course, will be heavily influenced by an adversary's objectives. Some malicious actors will be motivated by financial gain, and thus would be interested in documents containing monetary information.
- A document's level of enticingness can be thought of as the probability that an adversary would be interested in its exfiltration.
- A collection of interesting documents is the subset of documents for which this probability is above a certain threshold. In these terms, it is desirable that the probability of accessing any fake document which a decoy distribution system generates is at least equal to the real documents that are in the adversary's pool of interest.

D. Conspicuousness:

- Conspicuousness is closely related to enticingness, as both influence the odds of an attacker accessing a document. Enticingness models how curious an adversary is about a decoy, while conspicuousness concerns how easy a decoy is to access.
- A conspicuous document is one that is easy to find and access. Conspicuousness can be thought of as the amount of effort an adversary must put in to discovering a decoy, or more formally, the number of actions that are required to access it.
- This characteristic captures the fact that decoy documents should be placed in obvious locations such as a user's desktop. It also demonstrates that it is helpful to place documents in high traffic file system locations, including working folders where files that are accessed on a day-to-day basis are stored.
- File system searches are also user actions that may result in the presence of decoys. Conspicuous decoys should therefore be easily located by search queries.

E. Detectability:

- The aforementioned decoy properties all concern the relationship between decoy documents and a potential attacker. Detectability, on the other hand, describes the ability of decoys to notify their owner when they have been accessed. An ideal decoy system would issue an alert each and every time a decoy is accessed, but technical challenges, including network availability and variability between software platforms, mean that this may not always be possible in practice.
- Monitoring software can be placed in the operating system to detect predetermined tokens placed within decoys when they are opened. Further, operating system auditing can be enabled to record decoy interactions.
- It is particularly critical that decoy access events are detectable while an attack is taking place. Continuing to monitor this information allows for confidentially

violations to be handled after adversarial action has been carried out.

- Decoy material usage should thus continue to raise alerts after such data has been exfiltrated. Although it may be possible to evade detection in a particular practical decoy deployment, utilizing an extensive monitoring network will at the very least increase the time and effort that is required to execute an attack. This will make exfiltration more difficult and slow down or discourage adversaries as a net effect.

F. Variability:

- Although a decoy distribution system should strive to make its fake documents seem as authentic as possible, it would certainly be undesirable if precisely the same well-crafted decoy file were placed repeatedly throughout a given system or network. This would greatly simplify the task of distinguishing between legitimate data and the planted decoys that serveas monitors.
- In general, there should be as much variability between decoy documents as there exists in the pool of documents that they are intended to detect. That is, the task of identifying a decoy should not be reducible to identifying a particular invariant that exists between all generated decoys.
- A different way to conceptualize variability is to consider the task of an adversary who wishes to extract information from a system while remaining undetected.
- Variability among decoys essentially means that decoys should remain believable even after the presence of other decoys has been revealed.

F. Stealth:

- While it is clearly desirable that every decoy access event be perceptible to the owners of a system, care must be taken lest the alarms that accomplish this arouse suspicion.
- An overt mechanism for issuing alert beacons would provide adversaries with an obvious signal thatan element contains a trap, which completely violates the property of decoy variability. The messages that are transmitted by decoys must therefore be as subtle and covert as possible.
- Raising an alert that decoy content has been accessed necessarily involves taking some action, however.
- Even if precautions are taken, there is always the possibility that this act will be perceptible to a malicious actor. It is therefore also desirable to trigger beacon events as early as possible to prevent their interception.

G. Non-interference:

- This property is the first to describe how decoys should coexist with legitimate users who are not masquerading with assumed credentials.
- An optimal masquerader detection network would not affect the habits of typical users in any way. By inserting decoy material into an operating environment, however, we introduce the possibility that this data will confuse users or otherwise hinder their ability to complete their everyday tasks.
- If a file system is populated with decoy documents that serve as intrusion sensors, for example, the probability that the file system's primary owner is able to access a particular standard document should remain the same as it was prior to the introduction of the decoy content.
- Introducing decoy applications to a mobile device's operating system should not impact a user's ability to access real applications as they normally would.

H. Differentiability:

- A decoy can be considered fully differentiable if a real user will always succeed at this task. Balancing the differentiability for authentic users against believability for adversaries is one of the most critical aspects of any practical decoy deployment system.
- Though this may seem quite challenging, in practice, there are many properties that may be utilized to assist decoy designers in this regard. Legitimate users should be very familiar with detailed aspects of their data.
- They will also utilize their system in fairly predictable ways. Masqueraders, on the other hand, will have a limited knowledge of the files they are trying to exfiltrate.
- This gap in knowledge can be leveraged to increase decoy differentiability without affecting believability in the process.

I. Shelf Life:

- The data that is relevant to a normal user's tasks gradually changes as new events occur. The timeliness of data is perhaps even more relevant to attackers, who frequently wish to abscond with the most recent data that they can possibly access.
- The freshness of material that a decoy contains therefore plays a large part in determining how it will be perceived and how closely it will react the aforementioned desirable characteristics.
- This creates a very appealing target by leading adversaries to believe that the decoy content has been added even more recently than the authentic data that a system contains. Of course, as time moves on and data is updated while new files are created, these decoys will lose effectiveness.
- This can be seen as a shelf life during which decoys maintain an optimal level of functionality and after which their efficiency begins to diminish.

IV. ANALYSIS AND PLAY BETWEEN FOG AND CLOUD

While Fog nodes provide localization, therefore enabling low latency and context awareness, the Cloud provides global centralization. Many applications require both Fog localization, and Cloud globalization, particularly for analytics and Big Data. Here we consider Smart Grid, which data hierarchies help illustrate further this interplay. Fog collectors at the edge ingest the data generated by grid sensors and devices. Some of this data relates to protection and control loops that require real-time processing (from milliseconds to sub seconds). This first tier of the Fog, designed for machine-to-machine (M2M) interaction, collects, process the data, and issues control commands to the

actuators. It also filters the data to be consumed locally, and sends the rest to the higher tiers. The second and third tier deal with visualization and reporting (human-to machine [HMI] interactions), as well as systems and processes (M2M). The time scales of these interactions, all part of the Fog, range from seconds to minutes (real-time analytics), and even days (transactional analytics). As a result of this the Fog must support several types of storage, from ephemeral at the lowest tier to semi-permanent at the highest tier. We also note that the higher the tier, the wider the geographical coverage, and the longer the time scale. The ultimate, global coverage is provided by the Cloud, which is used as repository for data that that has a permanence of months and years, and which is the bases for business intelligence analytics. This is the typical HMI environment of reports and dashboards the display key performance indicators.

V. MOBILE CLOUD V/S FOG

The emerging high quality multimedia applications including distributed interactive games, video on demand and streaming demand large data transfer rates with low delay, delay jitter and packet loss . In order to achieve this, it is necessary to process these applications closer to the end users. Since cloud data centers are generally located within the Internet, it is difficult to manage these factors. Hence fog computing is the practical solution for this kind of performance sensitive applications. Wireless sensor networks have been widely deployed in many environment related applications . These networks are generally characterized by low power, low bandwidth and limited processing capability nodes distributed across wide geographical areas. These networks must be supported by low latency, location aware and widely distributed systems for processing and distributing the data. These are typical characteristics of fog computing rather than cloud computing. In this section, we take an in depth look at the similarities and dissimilarities of these two technologies with respect to the demands of the emerging trends in networking. Table 1 summarizes the results of the comparison.

TABLE I: Mobile Cloud Computing v/s Fog Computing

Mobile Cloud Computing v/s Fog Computing		
Parameters	**Mobile Cloud Computing**	**Fog Computing**
Latency	High	Low
Delay Jitter	High	Very low
Location of server nodes	Within the Internet	At the edge of the local network
Distance between the client and server	Multiple hops	One hop
Security	Undefined	Can be defined
Attack on data enroute	High probability	Very low probability
Location awareness	Yes	Yes
Geographical distribution	Centralized	Distributed
No. of server nodes	Few	Very large
Support for Mobility	Limited	Supported
Real time interactions	Supported	Supported
Type of last mile connectivity	Leased line, Wireless	Wireless

Data security and integrity are two most important characteristics demanded by many Internet applications . Longer the data stays en-route, more vulnerable it is for attacks even when encrypted. Hence it is always desirable to have few hops between clients and servers. Fog computing provides the shortest possible distance while providing all the other advantages of cloud computing. Hence fog computing is preferred over traditional cloud computing in such situations. Even the availability of cloud systems located within the Internet can be attacked by miscreants using various Denial of Service (DoS) attack methods. The DoS attacks need not be carried out directly on the end systems themselves, even attacks targeted towards the intermediary devices such as routers can also be equally fatal. Hence there are many opportunities for hackers to target cloud computing systems. On the other hand fog computing nodes are highly distributed near the edge of the user networks, in order to attack the availability of these systems, it is necessary to carry out a massive attack on all the systems that are nearby a client. This needs massive resources from the attackers side too. Also there are not many intermediate devices that can be targeted by the attacker as for computing nodes are located very close to the end users. Hence it can be safely state that fog computing system is less prone to DoS attacks than cloud computing systems.

From the above discussion, it can be seen that fog computing is more responsive to user needs and emerging new computing and networking paradigms than traditional cloud computing systems. Also fog computing is more resilient, rugged and secure than cloud computing in the face of changing needs and emerging trends. On the other hand, it must also be noted that cloud computing is not without its advantages. Since fog computing requires massive geographically distributed implementation, the single nodes cannot have large amounts of resources due to financial reasons. However high end business computing such as batch processing jobs, would require large amounts of resources while not being very delay sensitive. These kinds of jobs can be handled using traditional cloud computing systems successfully more than fog nodes. Hence fog computing will never be able to replace cloud computing and become the sole cloud computing model of the future. Thus, it is safe to state that cloud and fog would exist side by side serving two different communities and complement each other where necessary.

VI. CONCLUSION

We have outlined the vision and defined key characteristics of Fog Computing, a platform to deliver a rich portfolio of new services and applications at the edge of the network. The motivating examples peppered throughout the discussion range from conceptual visions to existing point solution prototypes. We envision the Fog to be a unifying platform, rich enough to deliver this new breed of emerging services and enable the development of new applications. To summarize, this paper introduced a novel security paradigm which we refer to as decoy technology. Decoys represent a drastic departure from existing security solutions in several important ways. By placing content that is spurious yet believable and enticing in the path of potential adversaries, decoys can serve as a potent last line of defense against

attacks that traditional security mechanisms fail to adequately defend against. Decoy content can be proactively seeded throughout a system to defend against potential attacks, or fed to an adversary once malicious activity has been detected.

Furthermore, by tracking decoy material, violations of confidentiality can be addressed after they have occurred. This is a capability that alternative security measures are not capable of offering. Although the deceptive techniques that form the basis of decoys have existed for ages, they have only recently been leveraged to protect computing resources. This paper discussed several dimensions along which this process can be refined and extended. It included at tributes that all high quality decoys should share as well as contexts in which decoys are particularly applicable. Decoys can be integrated as useful components of any full featured security solution and will only increase in prominence as threats against computer systems continue to grow. Mobile cloud computing is one of mobile technology trends in the future since it combines the advantages of both mobile computing and cloud computing, thereby providing optimal services for mobile users. According to a recent study by ABI Research, a New York-based firm, more than 240 million businesses will use cloud services through mobile devices by 2015. That traction will push the revenue of mobile cloud computing to $5.2 billion.

VIII. REFERENCES

[1]Tom H. Luan, LongxiangGao, Yang Xiang, Zhi Li, Limin Sun "Fog Computing: Focusing on Mobile Users at the Edge "1502.01815v1 [cs.NI] 6 Feb 2015.

[2]Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan Fog Computing: Will it be the Future of Cloud Computing? Proceedings of the Third International Conference on Informatics & Applications, Kuala Terengganu, Malaysia, 2014 pp. 8-15.

[3]Ivan Stojmenovic, Sheng Wen "The Fog Computing Paradigm: Scenarios and Security Issues" Proceedings of the 2014 Federated Conference onComputer Science and Information Systems pp. 1–8.

[4]RajashriRaut, MadhuriWaje, .SayaliKulkarni, Ajay K. Gupta"Fog Computing using Advanced Security in Cloud" International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2, February – 2014 pp. 1566-1568.

[5]Ashadeep, SachinMajithia "Enhancement In Cloud Data Security Using Fog Computing"International Journal Of Engineering Research-Online Vol.3., Issue.1, 2015 pp. 18-26.

[6]SonaliKhairnar, DhanashreeBorkar "Fog Computing: A New Concept To Minimize The Attacks And To Provide Security In Cloud Computing Environment" IJRET Volume: 03 Issue: 06 | Jun-2014 Pp.124-127.

[7]Jonathan Bar-MagenNumhauser, Jose Antonio Gutierrez de Mesa "XMPP Distributed Topology as a Potential Solution for Fog Computing"MESH 2013 : The Sixth International Conference on Advances in Mesh Networks pp 26-32.

[8]Jonathan Voris, Jill Jermyn, Angelos D. Keromytis, and Salvatore J. Stolfo "Bait and Snitch: Defending Computer Systems withDecoys".

[9]Sudha, A.Kannaki, S.JeevidhaAlleviating Internal Data Theft Attacks by Decoy Technology in Cloud IJCSMC, Vol. 3, Issue. 3, March 2014, pg.217 – 222.

[10]Manreetkaur Monika Bharti "Fog Computing Providing Data Security: A Review"IJARCSSEVolume 4, Issue 6, June 2014 pp.832-834.

[11]Manreetkaur and Monika Bharti"Securing User Data On Cloud Using Fog Computing And Decoy Technique"IJARCSMSVolume 2, Issue 10, October 2014 pg. 104-110.

[12]Hoang T. Dinh, Chonho Lee, DusitNiyato, and Ping Wang "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches" Accepted in Wireless Communications and Mobile Computing – Wiley.

[13]ThogarichetiAshwini 1, Mrs. Anuradha.S.G "Fog Computing To Protect Real And Sensitivity Information In Cloud" IJECSE IJECSE, Volume 4, Number 1.

[14]Pragya Gupta1, Sudha Gupta "Mobile Cloud Computing: The Future of Cloud" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 1, Issue 3, September 2012.

[15]AlessioBotta, Walter de Donato, Valerio Persico, Antonio Pescap´e "On the Integration of Cloud Computing and Internet of Things".

[16]Han Qi and Abdullah Gani "Research on Mobile Cloud Computing: Review,Trend and Perspectives".

[17]Salvatore J. Stolfo, Malek Ben Salem Angelos D. Keromytis "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud" IEEE Symposium on Security and Privacy Workshops pp125-128.

[18]GuilhermeSperb Machado, Thomas Bocek, Michael Ammann, Burkhard Stiller "A Cloud Storage Overlay to AggregateHeterogeneous Cloud Services" 38th Annual IEEE Conference on Local Computer Networks pp 597-605.

[19]Bonomi, "Connected vehicles, the internet of things, and fog computing,"inThe Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011.

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

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