ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

An Assessment on Enhancement of Cloud Using Fog Computing by Administering Decisive Latency and Portability with Decoy Technology

B.Deepthi Reddy[1], D.Sravanthi[2], B.Vijay Kumar[3].

Assistant Professor, Department of Information Technology, JBIET, Hyderabad, Telangana, India[1]

Assistant Professor, Department of Information Technology, JBIET, Hyderabad, Telangana, India[2]

Assistant Professor, Department of Information Technology, JBIET, Hyderabad, Telangana, India[3]

ABSTRACT: Increasing the usage of cloud computing in today's business sectors, but there are still issues unsolved due to inherent problems of cloud computing such as undecisive latency, lack of portability support and location-awareness. Fog computing can address those problems by providing elastic resources and services to end users at the edge of network. Applications and services that require very low and predictable latency, the Cloud frees the user from many implementation details, including the precise knowledge of where the computation or storage takes place. The main goal of fog computing is to deliver large quantities of data to more users. It will help optimize traditional cloud which uses a geographically distributed platform that can introduce additional latency. Fog computing will help distribute data and move it closer to the end user to support better data streaming and mobile computing. We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker.

KEYWORDS: Fog Computing**,** Cloud computing**,** latency, mobility, decoy.

I.INTRODUCTION

Cloud Computing is a combination of a number of computing strategies, Service Oriented Architecture ,virtualization and other internet of things. It is considered as a delivery platform in which resources are provided as a service to the client through the Internet. Although, Cloud Computing provides an easy way for accessing, managing and computation of user data, but it also has some severe security risks. There are some traditional security mechanism such as identity, authorization and authentication, but now these are not sufficient. 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 .Moreover, if the attacker is an insider than the chances of data theft increase as the insider may already have some personal information.

A new technology called Fog computing is gaining attention to the cloud users from the attackers. Like 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 portability. 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. By enhancing the cloud, Fog computing improves the Quality of service and also reduces latency.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

II. LITERATURE SURVEY

Figure 1: The Fog Extends The Cloud Closer To Devices Producing Data

IoT means everything talks to the cloud and all that big data we accumulate makes society more efficient than ever. One problem that we ran into with that plan was a lack of bandwidth. Solving the bandwidth problem that we're encountering with "the cloud" is remarkably simple. We simply create something called "fog computing" and insert it between "the cloud" and all our "IoT devices". It turns out that when you move a computer within close proximity of the device it's communicating with, the bandwidth improves. "Fog computing" is simply moving some of the computing power closer to the devices so that "the cloud" doesn't have to be consulted for every little minor detail. Many smaller time-sensitive computational decisions can be made by an intermediary device that then aggregates all the data it learns and sends that up to the cloud. It's kind of like decentralized computing all over again.

	Distance between Fog Nodes and IoT Devices	**Fog Aggregation Nodes**	**Cloud**
Response Time	Milli Seconds To Sub Seconds	Seconds To Minutes	Minutes ,Days,Weeks
Application Examples	M2M Communications,Telemedicine,Training	Visualization Simple Analytics	Big Data Analytics,Graphical Dashboards
StorageDuration of IOT Data	Transiant	Hours,Days,weeks	Months or Years
Geographic Coverage	One City Block	Wider	Global

Table 1:Fog Nodes Extends Cloud To The Network Edge

Here "fog nodes" that sit near all the IoT devices and then "fog aggregation nodes", a concept that is pretty much equivalent to how workstations communicated with servers back in the day. the real opportunity lies in configuring the "nodes" and optimizing their performance.

The primary difference between your IoT device communicating with a node versus the cloud is that bi-directional communication with a node can take milliseconds while conversing in the same manner with the cloud can take minutes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

III. ARCHITECTURE OF ENHANCEMENT OF CLOUD USING FOG

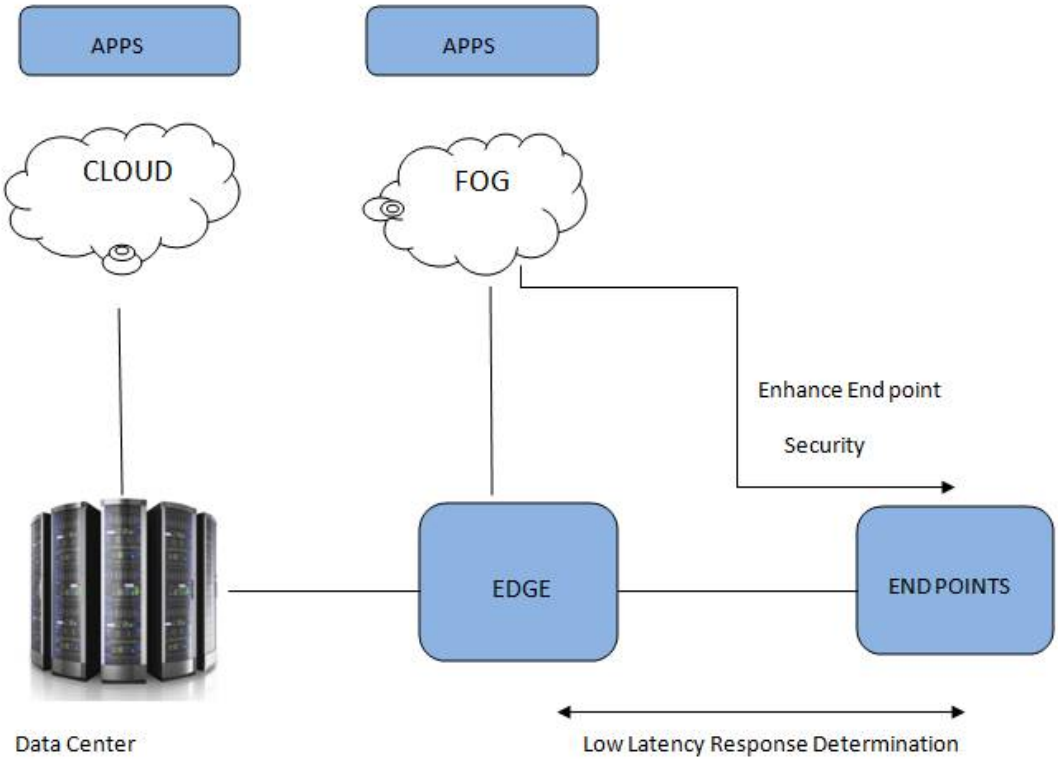

Figure 2: Architecture of enhancing Cloud using Fog

Capitalizing on the IoT requires a new kind of infrastructure. Today's cloud models are not designed for the volume, variety, and velocity of data that the IoT generates. Handling the volume, variety and velocity of IoT data requires a new computing model.

The main requirements are to:

- **Minimize latency:** Milliseconds matter when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make the difference between averting disaster and a cascading system failure.
- **Conserve network bandwidth:** Offshore oilrigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary, because many critical analyses do not require cloud-scale processing and storage.
- **Address security concerns:** IoT data needs to be protected both in transit and at rest. This requires monitoring and automated response across the entire attack continuum: before, during, and after.
- **Operate reliably:** IoT data is increasingly used for decisions affecting citizen safety and critical infrastructure. The integrity and availability of the infrastructure and data cannot be in question.
- **Collect and secure data across a wide geographic area with different environmental conditions:** IoT devices can be distributed over hundreds or more square miles. Devices deployed in harsh environments such as roadways, railways, utility field substations, and vehicles might need to be ruggedized. That is not the case for devices in controlled, indoor environments.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

IV SECURITY MECHANISM

Security mechanism makes use of two concepts known as user behavior profiling and decoys. Users who access cloud to view their own data and also perform data dynamics are expected to have some specific patterns of usage. Such users are known as normal users. This normal behavior of users is profiled in the first phase. Then decoy information is kept in file system besides throwing various society equations. The insider theft attackers generally do not have the behavior of normal user. For this reason they are attracted to use decoy information. As the decoy information is not the real data there is no problem when hacker uses it or steals it. However, the navigational patterns of the malicious insider can be compared with the navigational patterns of genuine users. The abnormal behavior has to be suspected.

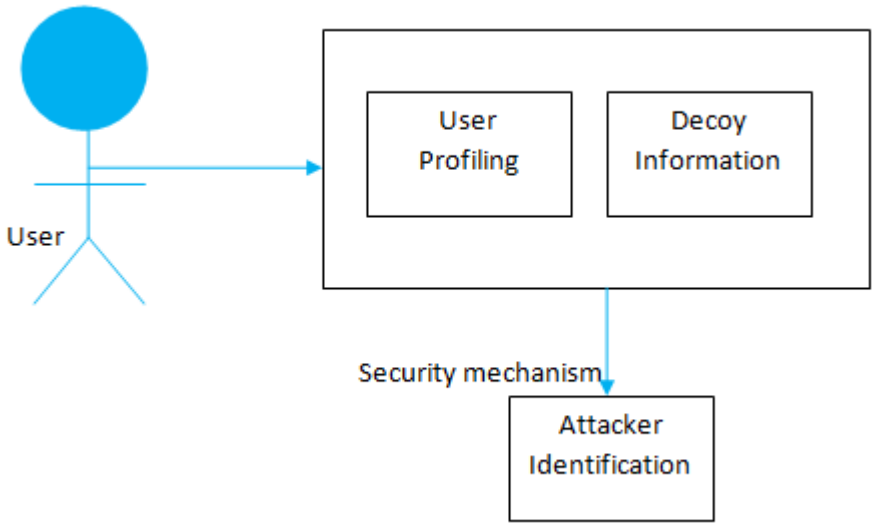

Figure 3: Security Mechanism

1) User Behavior Profiling: It is expected that access to a user's information in the Cloud will exhibit a normal means of 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.

2) Decoy Technology: Decoy information, such as decoy documents, are delivered to the attacker when an unauthorized access is detected. The file which sent to attacker is in encrypted format. However, when adversaries try to use the system, they are definitely attracted towards decoy information as their job is to explore sensitive data and steal it for monetary and other benefits. The decoy technology is very useful as it deceives malicious insiders. When the decoy technology is used along with user profiles, it is possible to know the suspected behavior of users and that way it is possible to prevent insider data theft attacks. We makes use of the two approaches together to detect insider data theft attacks. When a rogue insider tries to use Cloud for data dynamics, he gets attracted to bogus information which appears sensitive and useful to hackers. This way the proposed application deceives malicious users to behave that way and avoid insider theft attack.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

V. BENEFITS OF FOG COMPUTING

- With fog computing being closer to the edge, massive real-time data analytics will become a reality due to the increase in speed.
- Companies will be able to support location-based mobility faster since they will not have to traverse the entire Internet to get data.
- IDS can be deployed on fog node system side to detect intrusive behavior by monitoring and analyzing log file, access control policies and user login information.
- It provides new opportunities to investigate how fog computing can help with intrusion detection on both client side and the centralized cloud side.
- **Greater business agility:** With the right tools, developers can quickly develop fog applications and deploy them where needed. Machine manufacturers can offer MaaS to their customers. Fog applications program the machine to operate in the way each customer needs.
- **Better security:** Protect your fog nodes using the same policy, controls, and procedures you use in other parts of your IT environment. Use the same physical security and cybersecurity solutions.
- **Deeper insights, with privacy control:** Analyze sensitive data locally instead of sending it to the cloud for analysis. Your IT team can monitor and control the devices that collect, analyze, and store data.
- **Lower operating expense:** Conserve network bandwidth by processing selected data locally instead of sending it to the cloud for analysis.

VI. CONCLUSION

The goal of fog computing isn't to replace the cloud. It is merely designed to improve the client experience by isolating the data that needs to live on the edge and bringing it closer to the user. In this paper, we present a novel approach to securing personal and business data in the Cloud. By monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. These two approaches together could prevent insider data theft attacks. The user profile management ensures that the legitimate users' behavior and navigational patterns are recorded. The decoy technology allows the application to keep decoy information or bogus information in the file system to deceive insider data theft attackers.

REFERENCES

[1]. K.p.saharan and Anuj Kumar. Article: Fog in Comparison to Cloud: A Survey. International Journal of Computer Applications122(3):10-12, July 2015.
[2]. T.Rajesh Kanna, M. Nagaraju , Ch. Vijay Bhaskar. Secure Fog Computing: Providing Data Security. International Journal of Research in Computer and Communication Technology, Vol 4, Issue 1, January – 2015.
[3]. R. Buyya and A. Dastjerdi, Internet of Things: Principles and Paradigms, Morgan Kaufmann, 2016.
[4]. Pranati V. Patil Computer science & Engg College of Engg & Tech, Akola. Fog Computing. International Journal of Computer Applications (0975 – 8887) National Conference on Advancements in Alternate Energy Resources for Rural Applications (AERA-2015).
[5]. Ivan Stojmenovic, "The fog computing Paradigm : Scanerios And Security Issues", SIT, Deakin University, Burwood, Australia and SEECS, University of Ottawa, Canada.
[6]. Shanhe Yi, Zhengrui Qin, and Qun Li College of William and Mary Security and Privacy Issues of Fog Computing: A Survey
[7]. http://www.vxchnge.com/blog/fog-computing-explained.
[8]. https://www.quora.com/What-is-the-difference-between-mist-fog-smog-haze-and-vog.
[9]. http://www.slideshare.net/priyankareddy14/fog-computing-provide-security-to-the-data-in-cloud.
[10]. Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli Cisco Systems Inc. 170 W Tasman Dr. San Jose, CA 95134, USA Fog Computing and Its Role in the Internet of Things.