Survey of Enhancing Security of Cloud Using Fog Computing

Prasad Dharmadhikari[1], Mandar Dunde[2], Arpit Bhatnagar[3], Abhishek Singh[4]

Department of Computer Engineering,
NBNSSOE, Ambegaon, Pune-411041

Abstract: **Nowadays Fog Computing has become a vast research area in the domain of cloud computing. Due to its ability of extending the cloud services towards the edge of the network, reduced service latency and improved Quality of Services, which provides better user experience. However, the qualities of Fog Computing emerge new security and protection challenges. The Current security and protection estimations for cloud computing cannot be straightforwardly applied to the fog computing because of its portability and heterogeneity. So these issues in fog computing arises new research challenges and opportunities. This survey features about existing security concerns for fog computing and new proposed system to tackle some of the issues in fog computing related to security and privacy, thereby enhancing the cloud security.**

Keywords: **Fog Computing, Cloud computing, Security, Privacy, psychometric test, Profile behaviour techniques.**

I. Introduction

Fog computing is service started by networking giant, CISCO. Fog computing encourages the virtualized operation of processing, storage, and networking services between end devices and cloud computing data centers. Fog computing is a medium weight and intermediate level of processing. Fog computing quickens awareness and response to events by skipping the round trip to cloud for analysis. It keeps away the costly bandwidth additions. Ultimately, the organizations that adopt the fog computing gain deeper and faster insights and increased business agility. The Open Fog Consortium, aims to standardize and promote fog computing in various fields. Open Fog Consortium workgroups are working towards creating an open architecture for fog computing to enable interoperability and scalability. Fog Computing allows devices to connect directly with their destination with ease and permits them to handle their connections. Fog Computing is a highly virtualized platform that provides the computing and storage facilities between End Users and Cloud Data Center. Fog Computing has following characteristics:

- Low latency and location awareness
- End device mobility
- Wireless access
- Capacity of processing high number of nodes
- Real time application
- Heterogeneity

II. EXISTING RESEARCH

- ***Fog Network Scalability:*** [4] Due to dynamic nature and collaborative property of fog nodes, one common password does not provide high security due to many attacks, and also the authentication scheme based on key exchange, due to its slow and numerous processing is not appropriate. To overcome above pitfalls, an efficient and secure authentication facility has been proposed which allows End users to verify its identity with any fog node mutually.

- ***Privacy preserving Schemes:*** [4] There are various privacy maintaining strategies and algorithms are postulated to preserve the End user secrecy. Some of them are as follows:
  1) Identity Authentication Scheme
  2) Data Encryption Scheme
  3) Data Integrity checking Scheme
  4) Advanced Encryption Standard algorithm
  5) Secure Hash algorithm

  These schemes and algorithms provide better security to End Users data.

- ***Fog forensics:*** [4] Fog forensics is defined as use of digital forensics in fog computing. Fog forensics can ***be*** considered as similar to cloud forensics, as the forensic drawbacks of cloud forensics are similar to fog forensics rather more significant than cloud. For ex. as the fog servers are massively distributed unevenly, the retrieval of log data and further generating the digital evidence from the same is a challenging task. And the last but not least, due to large no fog nodes the dependability issue becomes more difficult in fog forensics.

- ***Fog Computing in IOT:*** [7] The presence of IOT in almost every sector has drastically improved quality of services and significantly reduced the costs. But it has also generated a huge amount of sensitive and public data which has to be properly collected, organized and analyzed. Though cloud computing serves as good option for above purpose, the rigorous evolution of fog computing which possesses additional layer for computing the data and sending the results to the cloud makes an even better, cost efficient and low latency replacement to the cloud.

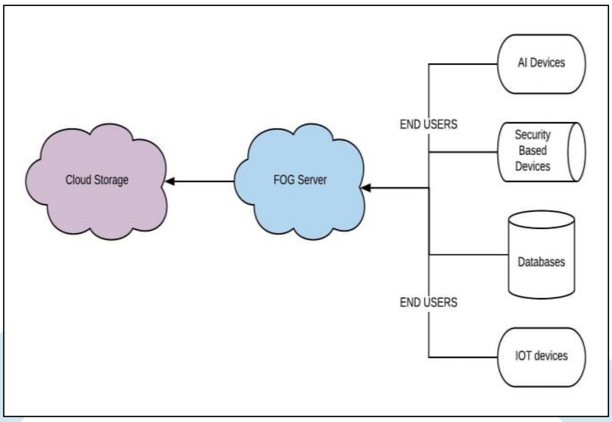

Figure 1: Existing Fog Computing Architecture

Tier 1-End Devices: [4] This level comprises of IoT-empowered gadgets including sensor hubs, EU's shrewd hand-held gadgets and others. These end gadgets are frequently named as Terminal Nodes (TNs). It is accepted that these TNs are outfitted with Global Positioning System.

Tier 2-Fog: [4]This tier is also known as fog computing layer. The fog nodes in this layer are outfitted with network devices such as router, gateway, switch, and Access Points (APs). These fog nodes can collectively share storage and computing facilities.

Tier 3-Cloud: [4]Traditional cloud servers and cloud DC reside in top-most tier. This tier has sufficient storage and computing resources.

[4] A fog-cloud interface provides end-to-end services including distribution of cloud services to the fog. In fog computing, several nodes or systems are scheduled to collaborate with each other to share data storage and computing tasks. Therefore, the design of fog-fog interface and protocol that enables different fog nodes to collaborate with each other is a important challenge. In addition, fog interface utilizes the resource efficiently.

Advantages of Fog Computing:

- ***Efficient Data Management:*** Fog applications can be programmed to control, reduce and arrange data produced by End Users. Required data is collected, analyzed at the network edge.
- ***Improved Security and Privacy:*** Various security and privacy preserving schemes such as Biometric Authentication, privacy protection cryptology, User profiling and behavior techniques can be applied to fog computing. So, Organizations can yield benefits without sacrificing the customer security and privacy.
- ***Lower Operating Expenses:*** Fog data services can operate on low bandwidth thereby saving network bandwidth, as less of the data is analyzed and stored. Due to this, organizations' operating expenses are drastically reduced.
- ***Grater Business Agility***: By using correct set of tools and techniques, programmers can easily develop fog applications and deploy them whenever needed.

Security and Privacy issues in Fog Computing:

- ***Trust:*** [4] Verification plays an important role in installing initial relations between end devices and fog nodes. Fog devices that provides services to end devices should be able to authenticate whether devices are genuine or not. This requires robust trust model to ensure reliability and security in Fog Network. The main issue is how to measure the trust in fog service and what are its attributes.
- ***Authentication:*** [4] Authentication of networked devices opted to fog services is one of the first necessity of fog network. To access the services of a fog network, a device must authenticate itself to fog network to stop entry of unapproved nodes. Successive requirement of authentication becomes the impressive difficulty as the devices involved in the network are obliged in different ways including power, computing and storage.

- ***Secure communications:*** End Devices interact with fog nodes to offload a storage or processing request. These communications are secured. But other communications such as communication between constraint-end devices and communication between fog nodes are not. The end devices, sometimes, may not be aware of existing fog network, so messages sent by such devices cannot be secured by using traditional cryptographic techniques. [4]

- ***End Users Privacy:*** In fog computing, securing the privacy is more challenging because fog devices are in close contact with end users and may gather private data considering the identity and usage of utilities. Fog nodes are unevenly distributed in vast areas, promoting to lose compact control, which further becomes an easy breach for an intruder. [4]

- ***Malicious Attacks:*** fog computing atmosphere can be made susceptible to harmful attacks such as Man in the middle attack, Denial of service attack etc. because of lack of mutual authentication, The DOS (Denial of Service Attack) becomes easy to perform. This can also be a compromised attack using a node which is not functioning properly for making successive requests to storage or processing services, and thereby stalking the requests made by other legitimate devices. [4]

III. PROPOSED SYSTEM

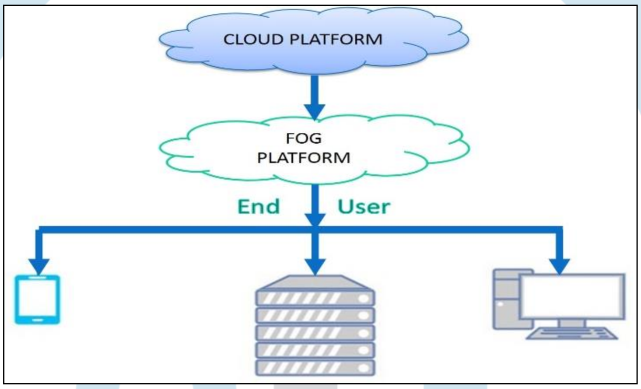

Figure 2: Proposed System Architecture

Proposed System Architecture: Dissimilar to traditional data centers, fog servers are topographically distributed over heterogeneous platforms, traversing multiple management domains. CISCO is keen on creative proposals that encourage service mobility across platforms and technologies that saves End User and content security and privacy across domains.

There are two techniques involved in proposed system to increase the cloud security and privacy:

1) ***User Profile Behavior System:*** The access to a user's data in the Cloud will present a genuine access. User profiling is an outstanding tool that can be applied here to model, how and when, and in the cloud it discovers how much a user accesses to their data. The mostly used strategy of behavior based security is utilized to search fraud detection. Unapproved users of computer system know about the files on that system. Any search for particular files is like to be targeted and limited. An imposter, who gets access to victim's system in an unauthorized manner, is probably not going to be familiar with the contents and structure of file system. Their pursuit is probably going to happen and untargeted. In proposed system, user search developed and behavior user models trained with one class support vector machines. In this way, the privacy of the user and their information is to be preserved.[10]

2) ***Decoy Technology:*** Fake information, such as fake documents, honeypots and other counterfeit data can be created on demand and utilized for identifying unauthorized access to data. Serving distractions will confound an adversary into believing in useful information have been ex-filtered. This technology has to be integrated with User profile behavior system to secure user data in the cloud. Whenever an illegal user access to cloud is detected, the cloud may provide fake information in return. The genuine user recognizes the fake information is being provided by cloud. [8]

The decoy technology serves two purposes:

1) To check whether the information access is authorized if suspicious data access is detected and

2) Misleading the attacker with counterfeit information

Combination User profile Behavior System and Decoy Technology: Combining the user profile behavior system and decoy technology will result in producing a concrete evidence of unlawful and unauthorized access of data and also advantageous to improve correctness of detection.[10]

IV. CONCLUSION

Security and privacy issues are studied in detail. However all of them are not worthy for fog computing due to its various characteristics. In addition the fog computing architecture along with its advantages is also studied. To overcome the security issues in cloud a new system capable of dealing with the security issue of cloud is also proposed. The main aim of this survey is to solve different challenges in security and privacy in fog computing.

REFERENCES

[1] S. Singh, Y. Chiu, Y. Tsai and J. Yang, “. Mobile Edge Fog Computing in 5G Era: Architecture and Implementation”, IEEE International Computer Symposium (ICS), pp. 731-735, Dec. 2016.

[2] Guenter I. Klas, “Fog computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium, ETSI MEC and Cloudlets”, Nov.22, 2015.

[3] OpenFog Reference Architecture. Accessed: Jul. 23, 2017.[Online].Available:https://www.openfogconsortium.org/ra/

[4] Mithun Mukherjee[1], Rakesh Matam[2],, "Security and Privacy in Fog Computing: challenges"

[5] Security and trust issues in Fog computing: A survey
PeiYun Zhang , MengChu Zhou , Giancarlo Fortino

[6] M.H. Ghahramani, M.C. Zhou, C.T. Hon, Toward cloud computing QoS architecture:Analysis of cloud systems and cloud services, IEEE/CAA J. Autom. S in.4 (1) (2017) 5–17.

[7] Mirjana Maksimović “Implementation of Fog Computing in IOT-Based Healthcare System”.

[8] “Decoy Technology in Fog Computing” Arwinder Singh, Abhishek Gautam, Hemant Kumar

[9] S. Ivan, W. Sheng, The fog computing paradigm scenarios and security issues, in: Proc. of the 2014 Federated Conference on Computer Science and Information Systems, 2014, pp. 1–8.

[10] G. Dileep Kumar, Kolla Morarjee , “Insider Data Theft Detection Using Decoy And User Behavior Profile”

[11] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, “Fog Computing: Mitigating Insider Data theft Attacks in Cloud”.

[12] Tom H. Longxiang Gao, Yang Xiang, Zhi Li, Limin Sun, “Fog Computing: Focusing on Mobile Users at the Edge”, 6th Feb 2015.

[13] Miss. Shafiyana Sayyad, Mr.Anil Bhandare, Mr. Deepak Yelwande, “Fog Computing: Software decoys for insider threat”, Volume 2 issue 3 March 2015.

[14] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, USA

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

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