ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

Fog Computing: Security, Issues and Its Challenges

[1] K.Anusha [2] Ayushi Verma [3] Aditi Soni [4] Punyaban Patel
[1][2][3] UG Students [4] Professor
Department of Computer Science and Engineering
Chhatrapati Shivaji Institute of Technology,
Durg, Chhattisgarh, India

Abstract: **-- Fog computing is an exemplification that extends cloud computing, also known as the Edge computing which works on the edge of the cloud. It provides data storage, fast data service, application services and more security in the cloud environment to the users. It overcome all the flaws of the cloud computing. Fog computing is brain behind the IoT. As compare to cloud, more network equipments are connected to computer and data centers in the Fog computing. In this paper, it describes briefly about Fog computing and analyses in-depth wise about the security, issues and its challenges.**

Key Words: **-- Fog Computing, Internet of Things(IoT), cloud computing**

I. INTRODUCTION

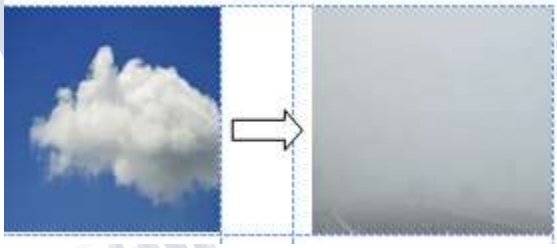
CISCO introduce a new technology fog computing to extends the capabilities of cloud in the year 2014, because in today's world cloud is widely use to store the data but it suffers from some issues like latency, mobility and location awareness and also has some security risks therefore FOG comes to provide better services to the user at the edge. Data is now being delivered in large quantities to many more users. To optimize the concept of the cloud, organizations need a way to deliver content to end users through a more geographically distributed platform [8]. Fog works between the end devices and cloud computing data centers through node which keeps less security issues and reduces latency and it places all the resources and processes at the edge of the cloud. Fog computing is not a different technology from cloud but it works from core of the network to the edge of the network.

1.1 Cloud Computing

Cloud Computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and other which rely on the Internet [3]. Cloud computing is a technique that based on Internet. It provides resources and services to its users through the internet for computation and other devices. We can say Cloud is a delivery platform for resources.

1.2 Fog Computing

Fog computing is also termed as Fogging or Edge computing, which provides an intelligent and appropriate platform for Internet of Things (IoT). It is considered as an extension of the cloud computing paradigm (shown in Figure 1.1) from the core of network to the edge of the network and has highly virtualized platform that provides computation, storage, and networking services between end devices and traditional cloud servers [1].



Cloud ***Fog***

Figure 1.1: Extension of Cloud to Fog

1.3 Architecture of Fog Computing

The system level architecture of Fog computing consists of four layers as shown in Figure 1.2. It extends the capability of cloud by introducing an

(i) First layer: end users

First layer consist of edge devices such as gateways, sensors, embedded systems, actuators and multiple kinds of applications are installed in the end devices to improve their functionality. In this layer, user's request are made from mobile and other devices request and send it to fog nodes to provide the desired data from cloud and to access data from cloud. Intermediate fog layer between the cloud and end users

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

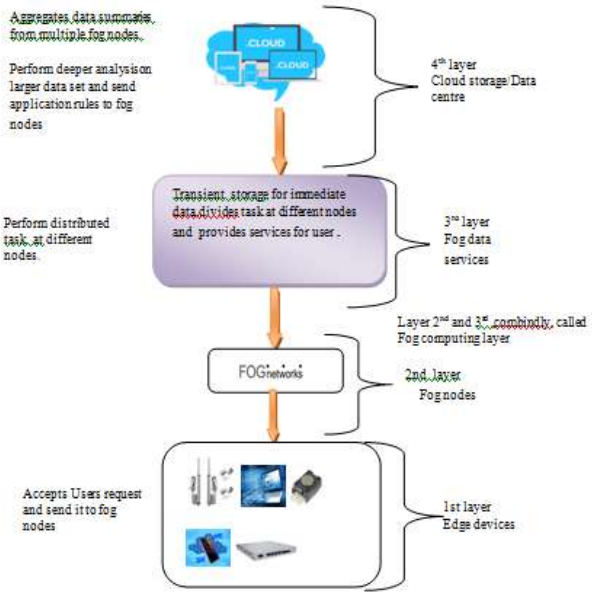


Figure 1.2: System Layered Architecture of Fog Computing

(ii) Second layer: fog nodes

Fog is highly virtualized environment and work is distributed among various fog nodes that reduces gap between cloud and end users. Its servers are provided at public places and local premises which have various kinds of fog nodes between cloud and edge through wireless services such as Wi-Fi, cellular or through remote sensing. Its nodes, can be homologize, are capable to store wide variety and large amount of data with high velocity generated from end user's request. A fog node gives response in milliseconds or seconds for requested data from end user.

(iii) Third layer: fog data services

The basic task of this layer is to divide the task among various fog nodes i.e.it interacts with fog nodes. Its services are providing temporary data storage, help to access faster for user by performing large computations in shorter time, thus reduces latency and if requested data can not acceptable for user then it reduces data rate, size of file, graphics and provides security improves the services for end users. The objective of this layer is to provide services and to distribute task execution at various fog nodes overall reduces the cost of using cloud.

(iv)Fourth layer: Cloud /data centre

Cloud contains large volume of data, resources and provides large numbers of services to the fog node by which the cloud will be not overloaded when the end user demand services. Perform deeper analysis on larger data set and send application rules to fog nodes. So, fog concept is introduced in between the cloud and edge devices, for the convenience of end users when they make request, fog accepts and provide desired results to end users.

1.4 Applications

There are various kind of applications could be benefited by the Fog computing. These are;

- ***Medical Field***: In Medical Field, medical equipment is connected to the fog network which stores the patient's information in the fog.
- ***Government Services:*** The essential and latent information of the government which is stored and secured by the fog networks.
- ***Education:*** It is the new technology to study easily and required information can be getting through network of fog and any educational institute can use the networks to provide online study resources to the students.
- ***Public Relation:*** The fog networks is used to communicate to the people online and can get their location, their identity and the conversation is secured using fog services by providing encryption.
- ***Cognitive Systems***: Cognitive Systems are applied in wearable devices such as Google Glasses helps people to reduce mental acuity which performs action such as recognizing the name of the person met but don't remembered.
- ***Air Pollution:*** Air Pollution can be reduced by vehicular networks in which each vehicle consists of a gas sensor. Sensors can sense the pollution and the data is received by the fog nodes installed at the traffic junction.
- ***Processing and caching***: user's request goes to fog boxes and modify request according to user acceptable form by reducing data size, graphics etc.

II. LITERATURE REVIEW

Many literatures are available in Fog computing. Few of them have been discussed in this paper. Park, Y. Et al. (2012) [22] has been developed a technique that was a software decoy used for securing

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

fog data. They proposed a system based on decoy technique which aims to deceive insider attacks and to detect the exfiltration of proprietary source code. This deception technique confuses the insider and also obfuscation helps the secure data by hiding it and making bogus information for insider.

In [22], the authors have been proposed a new technique that Fog computing which the extended paradigm of cloud is computing. They implemented security by using a technique Decoy which was given by Park, Y. Et al. (2012) [22]. They used two techniques User Behaviour Profiling and Decoy. In User Behaviour Profiling they checked how, when and the amount of information a user is accessing. This technique is used to monitor their user's activity. . The second technology is decoy in which information which is bogus or we can say fake such as honey files, honey pots, etc. are used to confuse the attacker or malicious intruder by depicting the information in such a way that it seems real[22].

In [23], the authors Madsen and Albeanu.G,has been described about the challenges faced in current computing paradigm and how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is done on the dense geographical distribution of resources or networks instead of a centralized one. Four layer architecture is followed in fog computing platforms.

The author Jayshree Khandagaleet. al.[21] has been discussed about monitoring data access in the cloud and detect abnormal data access by tracking the user's activity. If any user download the document, or files they won't get original file instead they get a decoy file. The main modules of this methodology are user and admin.

K. Hong et al.[18] proposed the concept of mobile Fog .Mobile Fog is a high level programming model consisting of aset of event handlers and functions for future Internet applications. They also proposed using parallel resources tomitigate large speed of mobile and taking several predictions for each time step.

Yifan, T.Etet. al. [19] has been discussed a new technique Jungle Computing which is a concept of distributive computing. Cloud and Fog belongs to utility computing which is a type of distributive computing. It combines several distributed and high performance computing systems to reduce programming complexity.

III. SECURITY

The threats to the cloud come due to the growing popularity and need of the services at an accurate level. Fog computing is the extended part of cloud computing which works on the edge of the cloud. It provides security to the end user by securing data transfer. Cloud computing suffering from security issues whereas fog computing introduced certain features to provide better security services to the user through cloud. Some methods have been proposed to provide security to the end users by giving encryption authentication of the data in the cloud which is recognized by sensors and biometric authentications like face authentication, fingerprint authentication and touch based authentication [1]. The cloud has a centralize data center and fog works between user and the cloud network. The cloud network uses to store personal and business information, systems and application soft wares and other various types of data & information. Fog contains the data and delivers closure to the users. So, the data theft attack reduces because the whole data are placed at a centralized cloud. In cloud, there is a possibility to attacked on these information to overcome this attack fog secure the data by using decoy technology, which gives disinformation against attacks and also possible to find the insider attacker by this technology. Many of the proposals are failed due to some reasons including insider attack, misconfigured services, buggy codes, etc. The damage to the data is difficult to control but can be limited by security features.

i. ***User Behaviour Profiling***: User Profiling is used to access the user's information in cloud. This technique is used in fraud detection applications to know how many documents are read and data to be transferred.

ii. ***Decoy:*** Decoy Information includes decoy documents, honeypots can be used to detect unauthorized access to information. This technique is used to integrate with user behaviour profiling technology to secure user information in the cloud.

The CSA (Cloud security Alliance) listed some of the security threats to the cloud as:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

i. ***Data Breaches:*** In Data Breaches, the protected or confidential data which is stored in the cloud can be viewed, stolen or copied by unauthorized user or individual.

ii. ***Account Hijacking***: In Account Hijacking, Phishing, and social engineering are still successful, and cloud services add a new dimension to the threat because attackers can eavesdrop on activities, manipulate transactions, and modify data[24].

iii. ***Malicious Insider:*** The Insider may be employee, administrator or the person who has full knowledge of the company. The malicious agenda may be from data theft to revenge.In cloud the insider can dissipate the infrastructure or manipulate the data and the systems that are dependent on the cloud services using encryption[24].

IV. ISSUES AND ITS CHALLENGES

Issue 1: Fog Networking

Fog work at the edge of the Internet, therefore fog network is heterogeneous .It is not easy to operate such a huge network for connectivity and providing services upon IoT at large scale. To increase network scalability and reduce networking cost, would be create flexible and easy maintaining network environment, it will be possible by emerging techniques such as SDN and NFV. Challenges: To manage huge networks for connectivity, providing services and increase network scalability by techniques such as SDN and NFV.

Issue 2: Data Management in a distributed fog Network

FOG computing provides all its services at the edge of network which is called nodes and these FOG nodes are distributed between cloud and the user. The services and the application objective of the fog is widely distributed [6]. Hence the data management is necessary in such type of distributed environment. Challenges: To improve transfer of data provided by fog nodes.

Issue3: Storage capacity

In ordain to obtain high band width and efficient storage utilization, it is important to investigate how much data placed in fog network since the data locality for computation is very vital [1]. The data is distributed on the several nodes, if the position of data is not determine it is difficult to reduce latency and definitely adds delay to services.

Challenges: To determine the storage capacity of fog nodes and to increase the storage capacity.

Issues 4: Security

Fog computing work at the several level of fog nodes, it is too difficult to provide authentication on the several nodes. Other constraints with the data security, to overcome data larceny in a cloud we preside with the edge computing .but if the data theft offensive is an insider then the data theft will be increases because the insider already have some individual information about data. Nobody is identified when attack is happen [2][3].

Challenges: To minimise the insider attacks by providing every time verification codes while transferring data.

Issues 5: Connectivity

Fog distributes task at different nodes but connectivity of this nodes with edge devices and cloud is too complicated.

Challenges: To provide better connectivity of fog layer with cloud and edge.

Issues 6: Interaction

Fog and cloud computing, both, accommodate different works, so that it is difficult to design an interface between fog and cloud server that could be able to share the work load.

Challenge: Like Fog which is an interface between end user and cloud. Similar to that we have to make an interface between cloud and Fog which overcomes all flaws of the fog.

V. PROS AND CONS

The Pros and cons of Fog computing over others are as follows:

Pros:

- Data privacy: fog computing provide a security environment in the cloud because it is work as an intermediate between end user and cloud server.
- Low latency: Because of high bandwidth the data transmission is very easy therefore fog computing

not suffers from high latency, data transmission simply fast enough.

- ♣ Mobility: Using LISP protocol fog devices provide mobility techniques like decouple host identity to location identity [6].

- ♣ Edge location: fog network work at the edge of the cloud which provides local awareness and fast provisions to the users.

Cons:

- ♣ Set up of fog network is not simple.
- ♣ Connectivity of several nodes are complicated.
- ♣ Wide network management.

VI CONCLUSION

This paper elaborated in brief about the applications and system layered architecture of fog computing. Also included several security, privacy issues and its challenges. We take issues with security concept such as to secure data storage by user behaviour profiling and decoy technique and needed new think to adapt new challenges.

REFERENCES

[1] Shanhe Yi, Cheng Li and QunLi.,"A Survey of Fog Computing: Concepts, Applications and Issues",10th International Conference Proceedings, WASA 2015, Qufu, China, August 10-12, 2015.

[2] Pranati V. Patil.,"Fog Computing", IJCA Journal,2015.

[3] Manreetkaurand and Monika Bharti.," Fog Computing Providing Data Security", International Journal of Advanced Research in Computer Science and Software Engineering Research ,

[4] C.Saste, P.V.Madhwai, N.B.Lokhand and V.N.Chothe.," Fog Computing: Comprehensive Approach ForAvoiding Data Theft Attack Using Decoy Technology"

[5] SonaliKhairnar and DhanashreeBorkar "Fog Computing: A New Concept To Minimize The Attacks and to Provide Security in Cloud Computing Environment".

[6] Nisha Peter and Nisha Peter, "FOG Computing and Its Real Time Applications", International Journal of Emerging Technology and Advanced, Volume 5, Issue 6, June 2015.(ISSN 2250-2459, ISO 9001:2008 Certified Journal)Engineering Website: www.ijetae.com

[7] NiranjanamurthyM ,Kavitha P , PriyankaKasana and Vishnu S N "Security :Research Study On Fog Computing For Secure Data".

[8]file://D:/FOG/Welcome%20to%20the% 20Fog %20%E2%80%93%20A%20new%20type%20of%20distributed%20computing.html.

[9] Ivan Stojmenovic, "The Fog Computing Paradigm: Scenarios and Security Issues".

[10] Tom H. LuanxiangGao, ZhiLiz,Yang, Xiang, Guiyi Wey, and LiminSunzFog,"Computing: Focusing on Mobile Users at the Edge", School of Information Technology, Deakin University, Melbourne Burwood, VIC 3125, Australia y School of Computer Science and Information Engineering, Zhejiang Gongshang University, Zhejiang, China z Institute of Information Engineering, Chinese Academy of Sciences, Beijing, Chin

[11]MugenPeng and Zhongyuan Zhao, "Fog Computing Based Radio Access Networks: Issues and Challenges".

[12]FlavioBonomi, Rodolfo Milito, Jiang Zhu andSateesh "Fog Computing and Its Role in the Internet ofThings".

[13] Salvatore J. Stolfo and Malek Ben Salem, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud".

[14] Amir VahidDastjerdi, Harshit Gupta, Rodrigo N. Calheiros, Soumya K. Ghosh, and RajkumarBuyya, "Fog Computing: Principles, Architectures, and Applications".

[15] "Offensive Decoy Technology For Cloud Data Attacks 1Lingaswami, 2G." International Journal of P2P Network Trends and Technology (IJPTT) Page

430,Volume 3 Issue 10 - Nov 2013 ISSN: 2249-2615. http://www.ijpttjournal.org

[16] ThogarichetiAshwini, Mrs.Anuradha.S.G.," Fog Computing to protect real and sensitivity information in Cloud", International Journal of Electronics and Computer Science Engineering www.ijecse.orgISSN-2277-1956 ISSN 2277-1956/V4N1-19-29 2.

[17] Mohammad Abdullah Al Faruque, Member, IEEE,andKoroshVatanparvar, Student Member, IEEE." Energy Management-as-a-Service Over Fog Computing Platform" IEEE Internet Of Things Journal, Vol. Xx, No. Xx, August 2015.

[18]K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B.Koldehofe, "Mobile fog: A programming model for large-scale applications on the internet of things," in Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing, ser.MCC'13. ACM, 2013.

[19]Yifan Wang and TetsutaroUehara.,"Fog Computing:Issues and challenges in security and Forensics".

[20] JayshreeKhondagale, Deepak Fodse, PoonamSul, PritaPatil, "Fog Computing".

[21]P.Jyothi1, R. Anuradha2, Dr.Y.Vijayalata, "Minimizing Internal Data Theft in Cloud Through Disinformation Attacks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2,Issue9,September2013. http://www.ijarcce.com

[22] Park, Y., &Stolfo, S. J. "Software decoys for insider threat", In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, (pp. 93-94).

[23] Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on.IEEE, 2013

[24]http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html