International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

FOG Computing Future of Cloud Computing

Kshamata Shenoy[1], Prachi Bhokare[2], Unnathi Pai[3]

[1]M.E, Asst Professor Baba Saheb Gawde Institute of Technology

[2]M.E, Asst Professor Baba Saheb Gawde Institute of Technology

[3]Student of Third Year NIE College of Engineering Mysuru

Abstract: ***Fog computing extends cloud computing, cloud computing provide data, compute, storage, and application services to end-user, also the fog computing also provide the services like data, compute ,storage and application to end user. But in cloud the main problem that occurs is security and now a days security and privacy both are main concern that needed to be considered. Fog Computing is not a replacement of cloud it is just extends the cloud computing by providing security in the cloud environment. With Fog services we are able to enhance the cloud experience by isolating users' data that need to live on the edge. The main aim of the fog computing is to place the data close to the end user.The securityissues are mentioned in this paper.***

Keywords: Cloud Computing, Decoy, Fog Computing

1. Introduction

Fog computing also known as fogging is a distributed computing infrastructure in which some application services are handled at the network edge in a smart device. Fog computing is a new standard that exploits the profits of virtualized IT infrastructures closer to end users Fog computing offers an attractive mixture of computational power, storage capability, and networking facilities at the edge of the networks. The infrastructure of this new scattered computing allows applications to run as close as possible to detected actionable and considerable data, approaching people, methods and thing. Fog computing provides security in cloud environment in a greater extend. To get the benefit of this technique a user need to get registered with the fog. Once the user is ready by filling up the sign up form he will get the message or email that he is ready to take the services from fog computing.

2. Security Issues Involved in Security Model

Cloud computing having three delivery models as shown in Fig 1 through which services are delivered through the end users. These models are SaaS, IaaS, PasS which provide software. Though core cloud computing technologies such as web applications and services which use SaaS, IaasS and PaaS platforms, there are many such security requirements which are solvable only with the help of cryptographic techniques. Thus, these challenges are of special interest for further cloud computing security research.

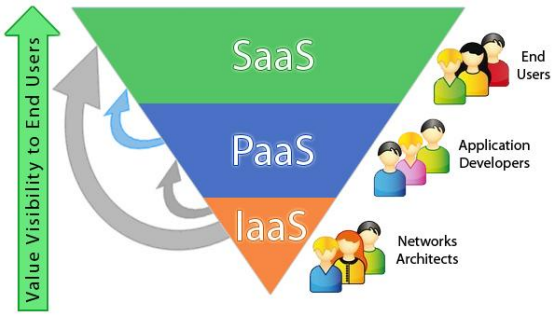

Figure 1: Cloud Computing Service Models

3. Cloud Computing Security Threats

IT security threats evolve and adapt to the new IT environment. As corporate and personal IT usage habits have changed, so too have the types of security threats present in the world. New IT practices like Cloud Computing give end-users great benefits in terms of mobility, flexibility and productivity, but they also give malicious third parties new routes to breaching security and increase risks. So while the Cloud has given users a whole new world of mobile computing, it has also created a whole new landscape for hackers and viruses to attack from.

Top seven security threats to cloud computing are discovered by cloud security alliance (CSA) are

1. Abuse and Nefarious Use of cloud computing
2. Insecure Application Programming Interface
3. Malicious Insiders
4. Shared Technology vulnerabilities
5. Data loss Leakage
6. Account service and Traffic hijacking
7. Unknown Risk Profile.

4. Fog Computing

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 [2].

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 within the Internet of Things.

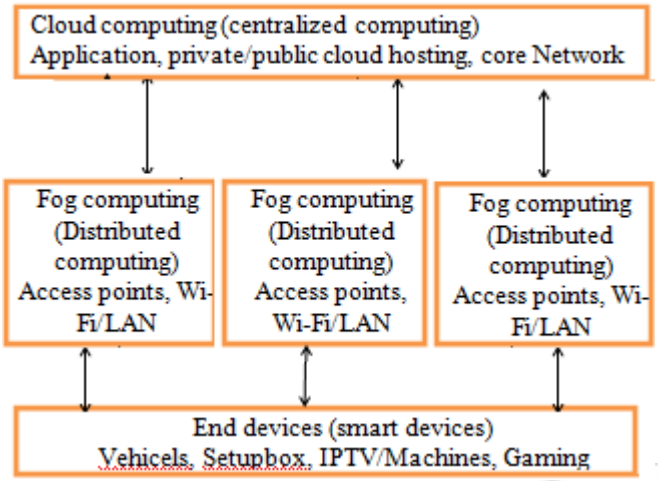

Figure 2: Reference Architecture

5. Securing Cloud Computing Using Fog Computing

Fog computing implement security by using Decoy information technology which discusses two methods, namely User Behaviour profiling and Decoy.

1. User Behaviour Profiling

It would be very hard if appropriately defined to impersonate the behaviour of any user. But the problem is its turning out really hard to define the behaviour of an user. There should be a way that we can automatically process the behaviour of the user to avoid the Insider Misuse Problems. User profiling should be used for detecting the illegitimate access. The current logged in user access behaviour is compared with the past behaviour of the user. If the user behaviour is exceeding the threshold value or a limit then the remote user is suspected to be anomaly. If the current user behaviour is as the past behaviour the user is allowed to operate on the original data. If the current user behaviour seems anomalous then the user is asked random secret questions. If the user fails to provide correct answers for a certain limits or threshold the user is provided with decoy files. If the user provided correct answers for a limit the user is treated as normal user.

2. Decoy System

Decoy means the relative disinformation, bogus information about the related data documents. If it gets suspicious then to mislead the attacker false information is being released after the user search modelling. For making sure that the attacker fails to differentiate between the decoy files and the actual files the same database is used for both decoy as well as original file. There is direct linking to fog computing sites in case the attack on user's data is continued by the attacker. Through this the safety of the important data is increased. The actual user will now identify if the bogus data is being sent by the cloud as he is the owner of the data. Thus through a large number of means the response by the cloud can be altered , such as challenge questions to inform the cloud security system about its unauthorized and incorrect.

Fog Computing system is trying to work against the attacker especially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files. The threat of malicious attacks has increased due to lack of transparency in cloud providers processes and procedures. It means that a provider may not know how employees are granted access and how this access is monitored or how reports as well as policy compliances are analysed.

6. Conclusion

With the increase of data theft attacks the security of user data security is becoming a serious issue for cloud service providers for which Fog Computing is a paradigm which helps in monitoring the behaviour of the user and providing security to the user data. Fog Computing presents a new approach for solving the problem of insider data theft attacks in a cloud using dynamically generated decoy files and also saving storage required for maintaining decoy files in the cloud. So by using decoy technique in Fog can minimize insider attacks in cloud.

References

[1] Cloud Computing for Dummies.
[2] Salvatore J. Stolfo, Malek Ben, Angelos D. Keromytis,"Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud,‖,'IEEE'.
[3] Mohamed Firdhous, Osman Ghazali and SuhaidiHassan,"Fog Computing: Will it be the Future of Cloud Computing?",'Third International
[4] Hashizume K., Rosado D. G.,Fernandez- Medina E. and Fernandez E. B. "An analysis of security issues for cloud computing". Journal of Internet Services and Applications, 2013, 4(1), pp. 1-13.
[5] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472-484.
[6] Archer, Jerry, et al. "Top threats to cloud computing v1. 0." Cloud Security Alliance (2010).
[7] G. Peng, "CDN: Content Distribution Network," arXiv preprint cs/0411069, 2004.