© 2017 IJSRST | Volume 3 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
16th February 2017
In association with
International Journal of Scientific Research in Science and Technology

Fog Computing : Providing Data Security to the Cloud

Prof. Abhijit Pande, Akshay Kawale, Avinash Padoliya, Mrunal Chaple, Pranay Gakare, Rohit Wankar

Department of Computer Technology, Rajiv Gandhi College of Engineering & Research, Nagpur, Maharashtra, India

ABSTRACT

Cloud computing is to significantly change the way we use computers and access and store our personal and business information. Nowadays, security and privacy both are main concern that needed to be considered. In an existing system the data protection mechanism such as encryption was failed in securing the data from the attacker it does not verify weather is the user was authorized or not so We propose a different approach for securing data in the cloud using user behavioral and decoy technology This protects against the misuse of the user's real data that we have come to call fog computing.

Keywords :- Advance User Behavioral, Hybrid Decoy Technology.

I. INTRODUCTION

In today's world small as well as big organization are using cloud computing technique to protect their data. Data theft attacks are amplified if the attacker is a malicious insider. The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to technological website and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed. The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents. Fog computing to prevent attacks such as the Twitter attack, by deploying decoy information within the Cloud by the Cloud service customer and within personal online social networking profiles by individual users. 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.

II. METHODS AND MATERIAL

A. Advance 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. We monitor for abnormal search behaviors that exhibit deviations from the user baseline. According to our assumption, such deviations signal a potential masquerade attack. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. These simple user-specific features can serve to detect abnormal Cloud access based partially upon the scale and scope of data transferred.

B. Hybrid Decoys

Decoy information, such as decoy documents, honeyfiles , honeypots, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's exfiltrated information.

Serving decoys will confound and confuse an adversary into believing they have ex-filtrated useful information, when they have not. A masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files, if he or she is in search for sensitive information, such as the bait information embedded in these decoy files This technology may be integrated with user behavior profiling technology to secure a user's information in the Cloud. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely legitimate and normal.

C. Literature Riview

Claycomb, W. R. (2012) has characterized a hierarchy of administrators within cloud service providers and also gave examples of attacks from real insider threat cases. They discussed how cloud architecture let attackers to breach the security. They have also presented two additional cloud related insider risks: the insider who exploits a cloud related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource. They mentioned the key challenges faced by cloud providers and clients for securing their highly confidential data.

Salvatore J. Stoflio et al. Proposed a new technique and named it as Fog computing. They implemented security by using decoy information technology. They discussed two methods, namely User behavior profiling and Decoy. In User behavior profiling they checked how, when and how much amount of information a user is accessing. They monitored their user's activity to check for any abnormality in the data access behavior of the user. 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.

Park, Y. Et al. (2012) developed a technique that was a software decoy for securing cloud data using software. They proposed a software based decoy system that aims to deceive insiders, to detect the exfiltration of proprietary source code. The system builds a Java code which appears as valuable information to the attacker. Further static obfuscation technique is used to generate and transform original software. Bogus programs are synthesized by software that is automatically transformed from original source code, but designed to be dissimilar to the original. This deception technique confuses the insider and also obfuscation helps the secure data by hiding it and making bogus information for insider. Beacons are also injected into the bogus software to detect the exfiltration and to make an alert if the decoy software is touched, compiled or executed.

Kaufman L. et al. (2009) has examined some security issues and the associated regulatory and legal concerns that have arisen as cloud computing. Interestingly, a major concern included in the Security Content Automation Protocol is the lack of interoperability between system level tools. By combining industry best practices with the oversight National Institute of Standards and Technology US and other entities are developing, we can effectively address cloud computing's future security needs. They also emphasize on providing data confidentiality which can impact the incident reporting.

Madsen and Albeanu.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 multitier 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.

III. RESULTS AND DISCUSSION

COMPARISION TABLE

Paper title	Advantages	Techniques
Software decoys for insider threat	Discussed a technique that confuses the insider and a is used for obfuscation which helps to secure data by hiding it and making it bogus information for inside	Developed a technique that was a software decoy for securing cloud data using software
Reliability in the Utility Computing Era: Towards Reliable Fog Computing	Provides the concept of Fog computing and its feasibility for real life projects	Three tier architecture for FogComputing is discussed
Improving Websites Performance using Edge Servers in Fog Computing Architecture	Concept of Fog Computing Architecture is used in such a way that various methods are combined with unique knowledge to improve the performance of rendering a web page	Minimizing HTTP requests,reducing the size of web objects and reorganizing the web page.
Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud	Monitor data and provides data security from malicious intruders and also helps in confusing the attacker about the real information	1-User Behavior Profiling 2-Decoy Information technology

IV. 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 behavior of the user and providing security to the user data. Other techniques discussed in this paper use Fog computing for optimizing the website performance. We hope that by continuing this work using Fog Computing platforms can lead to improved defensive techniques and would contribute in increasing the level of security if user data on the cloud.

V. REFERENCES

[1]. Claycomb, W. R. (2012) "Connected vehicles, the internet of things, and fog computing," in The Eighth ACM International Workshop on Vehicular Inter- Networking (VANET), Las Vegas, USA, 2011.

[2]. Salvatore J. Stoflio, "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.

[3]. Kaufman L. et al. (2009), "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr 2010.Σ Park, Y. Et al. (2012), "On optimally reducing power loss in micro-grids with power storage devices," IEEE Journal of Selected Areas in Communications, 2014 to appear.

[4]. Madsen.H and Albeanu, "The internet of things: A survey," Comput. Netw, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.