HINDERING DATA THEFT ATTACK THROUGH FOG COMPUTING

Arbat Rashmi Vinod[1], Bhalke Sumit Sunildatta[2], Kumari Uma Rani[3], Pillai Preethy Sasidharan[4]

[1]*Computer, AISSMS COE, Maharashtra, India*
[2]*Computer, AISSMS COE, Maharashtra, India*
[3]*Computer, AISSMS COE, Maharashtra, India*
[4]*Computer, AISSMS COE, Maharashtra, India*

Abstract

Fog computing is a paradigm that extends cloud computing which has become a reality that paved the way for new model of computing. Also fog provides application services to end terminal in the age of network. The inner data stealing attacks in which a user of a system illegitimately poses as the identity of another legitimate user which is an arising new challenge to the service provider where cloud service provider may not be able to protect the data. So to secure the real user's sensitive information form the attacker in the cloud. We are proposing a completely distinct approach with the help of offensive decoy information technology, which is used for validating whether the data access is authorized where abnormal information is detected and thereby confusing the attacker with the bogus information.

Keywords: *Fog computing, Decoy information, User behavior profiling.*

----------***----------

1. INTRODUCTION

Cloud computing is nothing but computing power which is virtualized and through platform-agnostics delivery of storage infrastructures of abstracted hardware and internet software. The shared, on-demand IT resources, are created and disposed of effectively, are dynamically scalable through a variety of programmatic interfaces and cloud computing is a general term for anything that involves delivery hosted services over `the internet. Cloud is being used in various deployment models and service models. Out of these 3 service models, the bottom layer is infrastructure as a service (IaaS) provides virtual machines and other resources like block and file storage, network security, load balancing, virtual local area networks (VLANs) etc.

The second layer form the bottom is Platform as a service here, cloud service provider deliver a computing platform like operating system, execution environment (programming language), database and web servers. Some PaaS service providers like Windows Azure, Google AppEngine enable the computers and storage resources vary automatically to match application demand so that the cloud user dos not have to allocate resources manually.

The last service model is a Software as a Service (SaaS),user are provided access to application software and databases. SaaS is something also called as "on demand service of software and is usually available on a pay-per-use basis.

With this new computing and communication paradigms arise a new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing the data theft attack, especially those perpetrated by an insider to cloud provider.

We propose a completely different approach to securing the cloud using the decoy information technology that we have come to call Fog computing. Such as Twitter attack, by deploying decoy information within a Cloud by the Cloud service customer and within personal online social networking profiles by individual users. We use this technology to launch disinformation attacks against malicious Associates, preventing them from distinguishing the real sensitive customer data from fake worthless data.

2. DATA THEFT

A very high and workable servicing is given to the business organizations, which for their secured data trust the providers of the cloud services. But this work is not as simpler to do in case of private services of cloud, as simpler it sounds. One of the major attacks in cloud is data theft. For Example, a series of cyber-attacks striking major banks as believed by U.S. officials, were the work of Iranian government to escalate cyber security standoff between the two nations. By infecting data centers at clouds instead of computers, the hackers obtained the computing power to mount enormous denial of service attacks. Thus, to limit the attacks of this kind we can reduce the value of the data which is being stored on the cloud.

3. SECURING CLOUD THROUGH FOG

For securing data of cloud, none out of all the proposed methods is full proof due to various reasons. Let it be standard access or the encryption mechanism being used for securing cloud, they have failed because a cloud's reliable environment only, is not enough for the customer. Nowadays, the customer requires security which is healthy for its applications and data. So such incidences must also be dealt with. If we decrease the value of stolen data by providing decoy documents then we can limit the harm of the system.

Following features of extra security are proposed:

3.1 Profiled Behavior of User

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 a user. It is absolutely necessary that there should be a way so that we can automatically process the behaviour of the user to avoid the Insider Misuse Problem. Currently even in case of malicious insider the data is accessed normally from the cloud as the insider is having the identity of the victim.

User profiling (the well-known technique) should be used for detecting the illegitimate access. Here for legitimate users the admin will be easily able to set working baseline going to record log record of all users. To detect about user behaviour's abnormal access the admin can keep a constant eye on 'Normal user' behaviour. Basically for applications of fraud detection this security method based on behaviour can be commonly used. Volumetric information such as the number of documents, their frequency of being read would naturally be used. We analyse for such type search behaviour which is dissimilar with that of actual user that exhibits deviation from the users threshold limit that has standby anomaly detect.

3.2. Decoy

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 access.

4. MERGING USER BEHAVIOUR AND DECOY

The current logged in user access behavior is compared with the past behavior of the user. If it is exceeding the threshold value or a limit, then the remote user is suspected to be anomaly. If the current user behavior is as the past behavior, the user is allowed to operate on the original data. The correlation of search behavior anomaly detection with trap based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy. This scenario covers the threat model of illegitimate access to Cloud data. Furthermore, an accidental opening of a decoy file by a legitimate user might be recognized as an accident if the search behavior is not deemed abnormal. Combining the two techniques improves detection accuracy. Instead, we made sure that the decoys were conspicuous enough for the attacker to access them if they were indeed trying to steal information by placing them in highly conspicuous directories and by giving them enticing names.

5. CONCLUSION

In this paper, by combining user search behaviour and decoy information we presented an integrated detection approach through anomaly detection with a baiting approach based on the deployment of decoy documents to secure personal and business data in the cloud. In our future work, this security system as we have explained is applicable only for single cloud ownership system. If the cloud owner has a more than one clouds to operate then our security system will not be applicable for providing security, therefore in the future enhancement we can enhance our existing application to manage a cloud environment which has more than one cloud architecture. Cloud computing is the future for organizations.

REFERENCES

[1]. M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Sympo- sium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

[2]. B. M. Bowen and S. Hershkop, "Decoy Document Distributor: ht t p ://sneaker s .cs.columbia.ed u/ids/fog/,"2009. [Online]. Ava ilable: http : / /sneakers.cs.columbia.ed u /ids/FOG/

[3]. M. A. Maloof and G. D. Stephens, "elicit: A system for detecting insiders who violate need-to-know," in RAID, 2007, pp. 146–166. [4]. R. Baeza-Yates, C. Hurtado, M. Mendoza, and G. Dupret, "Modeling user search behavior," in LA-WEB '05: Proceedings of the Third Latin American Web Congress. IEEE Computer Society, 2005, pp. 242–251.

[5]. J. Attenberg, S. Pandey, and T. Suel, "Modeling and predicting user behavior in sponsored search," in KDD '09: Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. New York, NY, USA: ACM, 2009, pp. 1067–1076.

[6]. B. M. Bowen, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, "Baiting inside attackers using decoy documents," in SecureComm'09: Proceedings of the 5th International ICST Conference on Security and Privacy in Communication Networks, 2009.

[7]. Fog Computing: Mitigating Insider Data Theft Attacks in the / Cloud. [Online].Available:http://ids.cs.columbia.edu/sites/default/files/Fog_Computing_Position_Paper_WRIT_2012.pdf

[8]. Lucky Nkosi, Paul Tarwireyi and Matthew O Adigun "Insider Threat Detection Model for the Cloud", 978-1-4799-0808-0/13/$31.00 ©2013 IEEE.

BIOGRAPHIES

Arbat Rashmi Vinod is pursuing Bachelor's degree in Computer Engineering from Savitribai Phule Pune University from A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Bhalke Sumit Sunildatta is pursuing Bachelor's degree in Computer Engineering from Savitribai Phule Pune University from A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Kumari Uma Rani is pursuing Bachelor's degree in Computer Engineering from Savitribai Phule Pune University from A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Pillai Preethy Sasidharan is pursuing Bachelor's degree in Computer Engineering from Savitribai Phule Pune University from A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.