FOG COMPUTING: ALLEVIATE INSIDER DATA THEFT ATTACKS

Ranjitha Rao[1], Saritha Shetty[2]
Department of Master of Computer Application, Asst Professor
NMAMIT Nitte
Visvesvaraya Technological University, Belagavi

Abstract

Now a days small or large business entities are depending on the cloud environment. Hence it is necessary to provide proper security to the cloud. The insider data theft is common in the cloud. We propose a completely different approach to securing the cloud using decoy information technology, which we can call Fog computing. We use this technology to launch disinformation attacks against malicious attackers, preventing them from accessing the real sensitive customer data from fake worthless data. In this paper, we propose two ways of using 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 site profiles by individual users.

In decoy technology we confuse attacker by sending bogus information. In recent years Twitter account was hacked by the attackers.

Keywords: Fog computing, cloud computing, insider data theft, cloud attack, cloud security.

1. Introduction

We propose a distinct approach to secure cloud known as Fog Computing. We use decoy information and user behaviour profiling to secure data on Cloud. We launch a disinformation attack against malicious insiders using these two technologies thus preventing them from distinguishing the real sensitive information from the fake data.

II. System Model

There are three different entities as illustrated in Fig. 1, the data owner, the Cloud service provider and the Cloud server.

During the registration procedure the client requests for space on the Cloud. The CSP processes this request and grants access to the client on the Cloud sends an email to the client consisting of a system created password. Once the client is registered, he can upload, download and access his data on the Cloud.

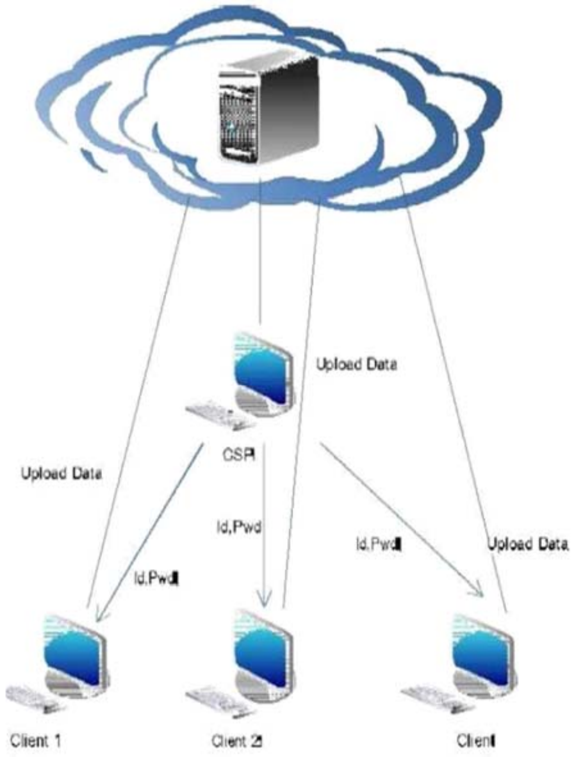

Fig.1.System model.

III. Protecting the cloud with fog

The data in cloud can be accessed anytime, anywhere using the internet. Due to this nature of cloud there arises a security concern. Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls.

Almost all the methods have been demonstrated to fail from time to time for various reasons, including insider attacks, misconfigured services, wrong implementations, erroneous code etc. Various technologies such as encryption, decryption, partitioning does not provide full security to cloud data. These security mechanisms fail now days because attackers are very strong. Attackers in such technologies easily find key for such encrypted cloud data. They can access information easily. Decoy technology is best one to fully secure the cloud data.

The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen information to the attacker. We can achieve this through a "preventive" disinformation attack. We posit that secure Cloud services can be implemented given three additional security features:

3.1UserBehavior Profiling

It is expected that access to a user data in the Cloud will show abnormal 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 showing up. Usually, this kind of method is used in the fraud detection.

It observes the user behavior such as how many times the data is accessed. If there is any deviation in the user behavior profile which is already stored in database then an attack is detected.

User behavior profiling is a reputable technique that is used to determine when and how frequently the user accesses his data on the Cloud. The way of access to a user's information on the Cloud is predictable.

This behavior of the user is checked continuously to detect an abnormal activity. Each user has a distinct profile consisting of the number of times he has accessed his files on the Cloud. These profiles maintain a count of the number of times a file is accessed.

If there is any deviation in the user behavior profile which is already stored in database then an attack is detected.

Here the legitimate user of the pc is familiar with the locations of the file, directory and database structures in the system. So, if it happens to be searching for a file, immediately targeted. It may be difficult to find in the case of masquerade. Based on this key factor we record user search behavior and developed user model with one class modeling technique, namely one class support vector machines. It builds a classifier without sharing the user details and their data. Hence, the confidentiality of the data is preserved. In this way we can clearly identify any abnormal behavior.

3.2 Decoy Technology

Basically here there will be heap of wasteful information kept to confuse the attacker. Whenever he tries to gain the access to data, incorrect data will be displayed and the same will be accessed by the attacker.

The file system is packed together traps, these traps are uploaded on the system by the cloud service provider. These traps can contain very important data such as bank statements, tax returns, credit card details. These documents are placed in highly egregious places.

A masquerade who is not acquainted with the system and who has an ill intent may is likely to click on these false documents. They may believe that he has accessed important information, when they have not. When a decoy document is downloaded an alert can be generated. Thereby the system can be notified of masquerade activity. This technology is incorporated along with User behavior profiling. When illegal access is suspected and later verified through various means, such as security question, a disinformation attack may be launched. In this attack, the attacker is provided with false information and made to believe that the information that he has received is true. This secures the users actual data.

The decoy documents carry a keyed-Hash Message Authentication Code (HMAC), which is hidden in the header section of the document. The HMAC is computed over the file"s contents using a unique key to each user. When a this decoy document is loaded into the memory, we verify whether the document is a decoy document by computing a HMAC based on all the contents of that document. We compare it with HMAC embedded within the document. If the two HMACs match, the document is deemed a decoy and an alert is issued.

3.3 Hybrid Technique

The correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance.

Therefore to improve a detector's accuracy. We hypothesize that detecting abnormal search operations performed prior to an unsuspecting user opening a decoy file will corroborate the suspicion that the user is indeed impersonating another victim user. 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.

In other words, detecting abnormal search and decoy traps together may make a very effective masquerade detection system. Combining the two techniques improves detection accuracy.

1.Previously we were storing real data and decoy data in the cloud.

2. So there is wastage of time and overhead to store the decoy data along with original data.

3. Hence when unauthorized user is detected that time it gets bogus data which is stored along with original data.

4. This process is complex and overhead of retrieving database.

5. In modification of above technology we just upload the original data in the cloud database.

6. In this, unauthorized user is detected then the decoy information is generated automatically and it will be given to unauthorized person.

7. The automatically generated information is not known to user as well as the admin.

8. Every time the new decoy information is generated for the same.

9. Hence the real data is secured from attacker and also the privacy is maintained.

10. This mechanism provides very strong security to cloud data.

We use decoys for validating the alerts issued by the sensor monitoring the user's file search and access behavior. Here, we did not generate the decoys on demand at the time of detection when the alert was issued.

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. With this approach, we were able to improve the accuracy of our detector. Crafting the decoys on demand improves the accuracy of the detector even further. Combining the two techniques, and having the decoy documents act as an oracle for our detector when abnormal user behavior is detected may lower the overall false positive rate of detector.

IV. Advantages

I. Information stored in cloud is highly secure.

II. This provide privacy.

III. The insider attack can be detected

IV. Attacker doesn't get any key access to stored data.

V. Attacker is satisfied with this decoy information.

VI. Attacker is tracked easily.

V. Future Scope

We can apply decoy technology for every type of data file such as images, multimedia files etc. Data can also be split up and stored on multiple Clouds for providing additional security.

Here in this paper, we present an approach to protect the data from the intruders by using other than common ways such as user behavior profiling and decoy technique on the cloud. Exfiltrating wasteful information to the attacker leads to think that he has actually accessed the real data, where he has not.

Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology, could provide unprecedented levels of security in the Cloud and in social networks.

References

[1] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud Position Paper By Salvatore J. Stolfo- Computer Science Department Columbia University ,New York, NY, USA ,Malek Ben Salem -Cyber Security Laboratory,Accenture Technology Lab Reston, VA, USA and Angelos D. Keromytis Allure Security Technologies New York, NY,USA.

[2] International Journal of Advance Foundation and Research in Computer(IJAFRC)Volume 2, Special Issue (NCRTIT2015), January 2015. ISSN 2348 – 4853 Prof. S .V. Phulari, Gawali Mahesh, Chorghe Vaibhav, Khavale Akshay PDEA's College of Engg.Manjari(Bk).Pune .

[3]Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March2010.