International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 230-232
e-ISSN:2278-621X

FOG COMPUTING MITIGATING INSIDER DATA THEFT ATTACKS IN THE CLOUD

Nithesh[1] & Sahana Y S[2]

Abstract- Cloud computing significantly alters the way we use computers and guarantees access and storage of our personal and business information. These new computing and communication models face new data security challenges. Existing data conservation procedures such as encryption fail to prevent data from the attacks of theft, especially in the cloud provider. So to overcome these problems we are proposing a new technology called Fog Computing.We propose a different approach in Fog computing to obtain data in the cloud using aggressive decoy technology and user behavior profiling. The users using the Cloud are trapped and their access patterns are recorded. Every User has a unique profile which is monitored and updated. We monitor data access in the cloud by the users and detect abnormal data entry patterns. When unauthorized access is suspected and challenged by challenge questions, we begin the wrong attack by returning the bulk of the information to the attacker. This protects users' real data from being misused. Experiments in a local file setting give evidence that this approach can provide an unprecedented level of user security in the cloud environment.
Keywords –: Fog computing, Point Clouds, Decoy Technology, and Cloud computing.

1. INTRODUCTION

Fog computing, or "fogging", is a distributed infrastructure in which certain application processes or services are maintained at the edge of the network by smart devices, but others are still maintained in the cloud. Now a days in a business world cloud is used to store the more confidential data. Security is an important issue in the cloud. Most recently used technologies fail to provide security for cloud data. Insider Data Theft Attacks have often occurred in the cloud, so most business areas are aware of security problems. So we are using fog computing for solving the issues in the cloud by using two technology. We can use decoy technology to give security for cloud. In decoy technology we confuse attackers by Sending fake information's. Recently Tweeter account was hacked by the attackers. We propose a unique method to secure cloud, called as Fog Computing. We use decoy information and user behaviour profiling to protect data in the Cloud. We start offensive attacks against malicious Insiders using these two technologies thus preventing the attackers from distinguish the real sensitive information from the fake data.

2. SYSTEM MODEL

There are three different components as described in Fig. 1: the data owner, the Cloud user and the Cloud server. At the time of registration procedure the Cloud user requests for space in the Cloud. The Cloud Service Provider processes this request and grant the permission on Cloud and sends an email to users who have access to the cloud with a password created by the system.After the registration, user can upload, download, and access their data in the cloud.

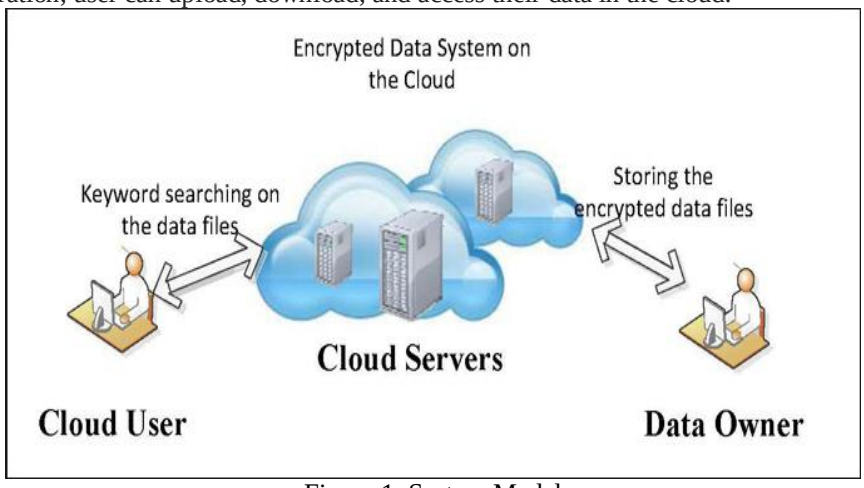

Figure 1: System Model

[1] Department of MCA, AIMIT, Mangaluru, Karnataka, India
[2] Department of MCA, AIMIT, Mangaluru, Karnataka, India

3. EXISTING SYSTEM:

The current system provides only the single user authentication which is not much safer and can be easily hacked by an attacker. The system does not provide any additional security such as security queries for extra security. The attacker can easily get into the cloud and search for the files or data that are available in the cloud. The current system do not investigate whether user is authorized or not. The current system gives security by encryption technology but it fails to secure the cloud data.

4. PROPOSED SYSTEM (PROTECTING CLOUD WITH FOG):

Several proposals of cloud-based services describe ways to store documents, files, and media in a remote service that can be accessed anywhere whenever user connected to the Internet. A particularly raging problem before such services are accepted everywhere provides guarantees for safeguard the user's data in a sequence where that guarantees only for the user and nobody can gain access to that data. The problem of giving security of confidential data remains a basic security problem that, till date, has not provided the levels of assurance, according to the people wishes.

Several approaches have been made to protect the remote data in the Cloud, using encryption and standard access controls. It is well enough to say all of the standard proposals have been exhibited to fail from time to time for a various reasons, including insider attacks, miss-configured services, bug fixes, error code, and innovative formation of effective and sophisticated attacks not conceived by the implementers of security procedures .Creating a trustful cloud computing environment is not enough, because attacks continue to happen, and when it happens, and data gets lost, there is no way to take it back. One needs to prepare for such attacks.

Various technologies such as encryption, decryption, partitioning do not provide complete security to cloud data. These security procedures fail now days because attackers are too strong. Attackers in such technologies can easily find key for such encrypted cloud data. They can get the information easily. Fog computing by using Decoy technology is best way to completely secure cloud data. It uses two types of mechanisms:

4.1 User Behaviour Profiling:

User behavior profiling is a popular technology in fog computing which is used to determine when and how frequently the user access his data in the cloud. The way to access Cloud's user information is predictable. This behavior of the user is constantly checked for abnormal activity. Each user has a unique profile consisting of the number of times he has accessed his files on Cloud. These profiles maintain the count of numbers that the file has accessed. If there is any deviation in the user behavior profile already stored in the database, then the attack will be detected.

4.2 Decoy Technology:

The file system is mounted with traps which are uploaded on the system by the Cloud service provider. These traps include documents such as credit card details, tax returns, bank statements.These documents are placed in very egregious places. The attacker who is not influenced with the system and who has bad intent may likely to click on these false documents. They may believe that he has Ex-Investigated important information, although they have not. When a decoy document is downloaded an alert will be generated. Through this the system can be notified of an illegal activity.

This technology is integrated with user behavior profiling. When an illegal access is determined and later verified by various methods, such as security question, a disinformation attack may be started. In this attack, the attacker will be given false information and the information they received was believed to be true. This will secure the actual data for the user.

5. FUTURE SCOPE

We can apply decoy technology for every type of data file, such as images, multimedia files, etc. Data can be split up and stored in different clouds to provide additional security. By using the User Behavior Profiling technology the illegal access to the cloud will be determined. So that the user may store any amount of his data on to the cloud without worrying of attacks and all. These two technology (decoy and user behavior profiling) provides more security to the users in order to store the data on the cloud.

By using the decoy and User behavior profiling technology for the fog computing the attacker will not be able to access the stored data on the cloud. If and only if attack is happened, the attacker will be satisfied with the decoy information's (i.e. attacker will be sent wrong information's).Due to this the attackers will be tracked easily.

6. CONCLUSION

Thus in this paper we propose a Fog computing by using unique technology to safeguard the cloud by securing the personal and important data of the business firms. We provide monitoring of access to the account by examining the behaviour of the users. We provide access not only by login details but also by challenge queries which would be only known to the clouds user. If access is found to be unauthorized, the user's actual data may be saved by providing duplicate data. This technology adds a level to secure data on the cloud.

7. REFERENCES

[1] Prof. S .V. Phulari, Gawali Mahesh, Chorghe Vaibhav, Khavale Akshay," Fog Computing: Mitigating Insider Data Theft Attack in the Cloud",PDEA's College of Engg.Manjari(Bk).Pune,2015.

[2] Viraj G. Mandlekar, VireshKumar Mahale, Sanket S.Sancheti, Maaz S. Rais," Survey on Fog Computing Mitigating Data Theft Attacks in Cloud", International Journal of Innovative Research in Computer Science & Technology (IJIRCST), 2014.

[3] Ben-Salem M., and Stolfo, Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud," IEEE symposium on security and privacy workshop (SPW) 2012.

[4] Bowen, B. M., Hershkop, S., Keromytis, A. D., and Stolfo, S. J., "Baiting inside attackers using decoy documents." in Department of Computer Science Columbia Universit, 2009.

[5] Ben-Salem, M., and Stolfo, S. J., "Modelling user search-behaviour for masquerade detection," In Columbia University Computer Science Department, Technical Report # cucs-033-10 (2010).

[6] Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, "Fog Computing Mitigating Inside Data Theft Attacks In The cloud",IEEE Base Paper, 2013

[7] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centres and Virtual Computing Environments, Hong Kong, ser. DCDV '11, June 2011.