International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 717 - 719

FOG COMPUTING:An Approach for avoiding Data Theft by Decoy Information Technology

Bhavesh Pandey
BE.COMPUTER
VOGCOE
Email id:
bhavesh.hpandey@gmail.com

Ankit Pawar
BE.COMPUTER
VOGCOE
Email id:
ankitpawar0033@gmail.com

Jay Mehta
BE.COMPUTER
VOGCOE
Email id: jaymehta794@gmail.com

Satish Mishra
BE.COMPUTER
VOGCE
Email id: satish7962@gmail.com

Sneashesh Patil
BE COMPUTER
VOGCOE
Email id:jonty.patil222@gmail.com

***Abstract*—**Cloud Computing changed the way of computing and data and storage concept nowadays. In Cloud computing we use different type of security concepts to work with it. In present we are working with the encryption mechanism to secure the data. Encryption mechanism is failing and not capable to secure the cloud data as well as internal data theft attacks. For these problems we are proposing different approach to secure the cloud FOG COMPUTING. In this technology we will use decoy information technology to work with and we will monitor the behavior of the user to intercept the user's behavior inside the cloud even though he/she is registered user on the cloud.

***Keywords*—** *Cloud Computing, Decoy, Fog Computing, Security, User Behavioral Profile,Encryption*

*****

1. INTRODUCTION

Cloud has become essential part of our life. We are almost reliable on cloud for data storage, Due to this reliability There are many threats for cloud and the researches which are going on is basically concentrated on the encryption .Encryption is insufficient to prevent the cloud for the data theft attack. Main problem on cloud in insider data theft and the encryption is no capable to prevent the cloud. For this reason we are proposing whole new approach which is decoy information technology in this we check data access in the cloud and observe abnormal information access patterns and when the abnormal patterns are detected we perform series of security questions and flood the intruder's database with decoy information and dummy files and thus can prevent cloud's data. Secured cloud computing with decoy documents extends the Cloud Computing approach to the boundary of the network, thus enabling a new kind of applications and services. Identifying masquerades has become very difficult. Many planned approaches rely on encryption by auditing a variety of sources which are not able. Few years back there was a Twitter incident which is a best example for data theft attack from the cloud service provider. This incident exposed the security problems in cloud computing as it could make the customers of Twitter to lose their sensitive data and documents. [5][2]

2.PROBLEM STATEMENT

Cloud is used to store data remotely any user can access the data by using username and password. The main advantage of using Cloud system is user can access their data form anywhere without any hassles using internet connection. Storage space of user is not being consumed because the data is stored on the cloud .the main thing is that the user don't know where and how data is stored ?and who can see the data ?

The problem of user when he store sensitive information in the cloud the user require security of the cloud computing to assurance nobody can right to use and view his data and business related information that his store in cloud, to avoid this problem used encryption method. But the technique of encryption alone is not enough for providing security to user's sensitive data.[1]

Following are the drawbacks of the Current system:

1. No one can identify whether the attack is occurred or not.
2. It's hard to identify the attacker or intruder.
3. Detection of hacked file is complex.

3. PROPOSED SYSTEM

We propose a completely different approach to securing the cloud using decoy information technology, that we have come to call Fog computing.We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.In this paper we propose a different approach for securing data in the cloud using decoy information technology. The data theft by insider is simply passed with the help of creation of decoy file on demand. We check the cloud and identify suspicious and uneven access patterns. When illegal access is identified then verification is performed using challenging questions,

we perform disinformation attack by returning large amounts of decoy information to the attacker. In the system we develop whenever insider observed to be performing data theft, only then decoy file is created and is passed on to the requesting insider, whenever user trying to upload a file on the cloud user provide security question. The same security question appear when any user want to download or do any operation perform on the particular file form the cloud. We are providing OTP (One Time Password) System to increase the security of the information of the user stored over the cloud.

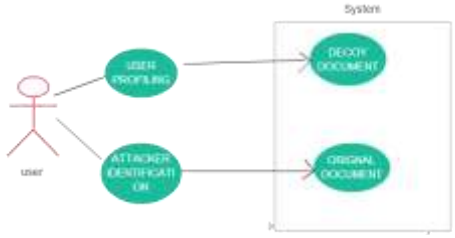

Figure 3.1.Decoy System

Figure 3.2. System Architecture[12]

4.CLOUD SECURING PROCEDURE

We can protect the data on cloud by decreasing its value to the attacker or intruder. We can achieve this by seeding false information in other word using disinformation attack.We imagine that secure cloud services can be implemented given six other security features:

a. Confusing the intruder/masquerader with bogus information.
b. Confuse the intruder by false information
c. Secure the confidential data form web-administrator.
d. Block the masquerader.
e. Enhanced Authentication with OTP.
f. Data security using AES encryption technique

a. Monitoring the undesired behavior of the user:

We envision that the blend of these security elements will give abnormal state of security to the Cloud. at present no other framework can give this level of security .We have utilized these ideas to see unlawful information access to information put away on a neighborhood record framework by impostors, i.e. assailants who duplicate legitimate clients after burglary their recognizable proof .Our trial results in a neighborhood document framework setting demonstrate that joining both procedures can deliver better results, and our outcomes prompt that this methodology may work in a Cloud domain, as the Cloud is proposed to be as clear to the client as a nearby record framework. In the accompanying we investigation quickly a portion of the trial results accomplished by utilizing this way to deal with identify masquerade action in a neighborhood record setting.[11]

b. Confuse the intruder by false information

We recommend the utilization of distraction data innovation. We screen information access in the cloud and sense unpredictable information access designs. We start a disinformation assault by infusing a lot of fake data to the aggressor. This ensures against the abuse of the client's honest to goodness/confirmed information. We utilize this innovation to start disinformation assaults against pernicious insiders, keeping them from recognizing the legitimate mindful client information from false futile.[9][10]

c. Secure the confidential data form web-administrator.

If genuine user is not interested in giving its confidential data to the web administrator he can do so by using the concept of FOG COMPUTING. In current system, web-administrator can directly access all the data without the permission form the normal or corporate user which is stored on to the cloud. There is no any situation for security of information which is stored on to the cloud. So in our system, all the data which is stored on the cloud is confined, it is totally depend on the user to assign access agreement to its data. In case, if web-administrator wants to access the information which is stored on the cloud, it has to gain the private key of that particular user to decrypt the information.

d. Block the masquerader.

On the off chance that we will found any awful client from his client profile conduct we can straightforwardly obstruct that client or we can solicit an arrangement from security questions. This exercises of the all clients will put away in the client log exercises, so when framework distinguishes any suspicious exercises, it obstruct that client on the off chance that, if any permitted client attempt to look whatever other broadly put away documents then as indicated by our circumstance our framework hinders that customer, yet in the wake of blocking we fire some arrangement security address in order to guarantee verified/authentic client.[11]

e. Increasing the security level using OTP

In the cloud when two genuine users tries to communicate with each other then they will send a text message which shall encrypted using AES (Advanced Encryption Standard).this will generate a key which shall be used for decryption purpose also .This key will sent to the user as a OTP on the email id provided by the user during the time of registration.

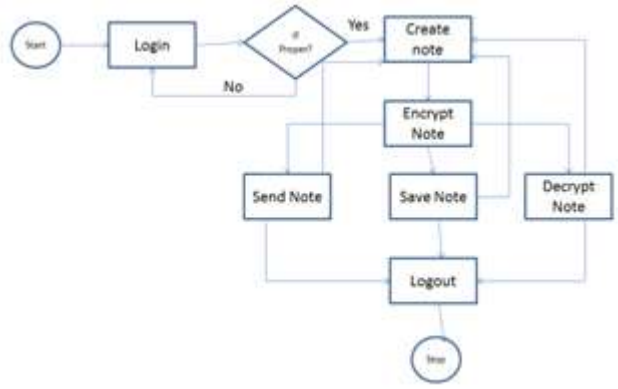

Figure 4.e.1Control Flow Diagram

f. Data security using AES encryption technique

The Advanced Encryption Standard (AES) is a symmetric-key encryption standard approved by NSA fortop secret information and is adopted by the U.S.government. AES is based on a design principle known as a substitution permutation network. The standard comprises three block ciphers: AES-128, AES-192 and AES-256. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively

Key Length	Number of Rounds
128	10
192	12
256	14

Figure 4.f.1.AES key information

CONCLUSION

In this paper we are proposing the entire new way to deal with secure the information on the cloud by utilizing imitation data innovation and the client behavioral profiling. IN current situation, Encryption is utilized to secure the information of the client which alone is not adequate to give security of the clients data on the cloud. By utilizing fake data procedure we can debase the nature of the information so that the assailant won't be capable concentrate any secret data, which can posture damage to the client. By utilizing different security elements of the FOG COMPUTING we build the administration of the client profile and utilize more fake data from different areas in order to acculturating accurate positives of the mist processing.

ACKNOWLEDGEMENT

We would like to thank Prof.AnupMauryaand our friends which help us throughout our process without their guidance and support we would never complete our paper in time.

REFERENCES

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010.[Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidential-twitter-documents/

[3] D. Takahashi, "French hacker who leaked Twitter documents to Tech Crunch is busted," March 2010. [Online].Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked-twitter-documents-to-techcrunch-is-busted/

[4] D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online]. Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwitters- admin-panel/3292

[5] P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010. [Online]. Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html

[6] 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 Centers and Virtual Computing Environments, Hong Kong*, ser. DCDV '11, June 2011.

[7] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in *Proceedings of the 5th USENIX conference on Hot topics in security*, ser. HotSec'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934

[8] J. Pepitone, "Dropbox's password nightmare highlights cloud risks,"June 2011.

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

[10] B. M. Bowen and S. Hershkop, "Decoy Document Distributor:http://sneakers.cs.columbia.edu/ids/fog/," 2009. [Online]. Available: http://sneakers.cs.columbia.edu/ids/FOG/

[11] M. Ben-Salem and S. J. Stolfo, "Combining a baiting and a user search profiling techniques for masquerade detection," in *Columbia University Computer Science Department, Technical Report # cucs-018-11*, 2011.[Online]. Available: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1468

[12] D.C.Saste "fog computing: comprehensive approach for avoiding data theft attack using decoy technology"Int.J.Computer Technology & Applications (IJCTA), 2014.