Fog Computing:Detecting Malicious Attacks in a cloud

[1]Madhusri.K, [2]Navneet.Y, [3] Harish.CH,[4]Sandeep.A,[5]Dr.T.V.Rao
[1,2,3,4] B.Tech Students Dept of C.S.E
[5]Professor Dept of C.S.E,
K L University, Vaddeswaram,
Guntur, India

Abstract

Cloud computing is a new paradigm which enables ubiquitious,on demand network access to a shared pool of configurable resources with minimal management effort.it provides many services like pay per use model and elasticity of resources.There is a need to provide better security in order to get rid of malicious insider attacks.Existing cryptographic data security mechanism such as Encryption has failed in preventing insider data attacks.

We propose a different approach in order to avoid insider attacks using decoy information technology.We monitor the user search modeling in the cloud.When unauthorized access is suspected verification is done by providing some security questions and then we launch a false information attack by providing decoy documents.This protects against misuse of real data.This technique prevents malicious attacks and provide high security in cloud environment.

INTRODUCTION

Cloud computing has become an important paradigm which provides better operational efficiency,so business people started opting cloud.This obviously provide better efficiency but comes with a most serious risky issue like data theft attack.Cloud cannot prevent data theft attacks if they are insider attacks.These attacks have become a serious threat to cloud.Cloud computing customers are well aware of this threat but they are only left with the choice i.e., trusting the service providers.Lack of transperancy is one of the reasons for this threat.

A completely new approach is proposed,decoy information technology which comes under Fog Computing.Fog computing is an extension of cloud computing.It is a unifying platform at the edge of the network that supports a wide range of emerging applications and services requiring low latency,orchestration of large scale controlled systems,mobility support etc.We propose two ways using fog computing.

Detecting malicious attacks

Masqueraders can steal a legitimate users credentials by sniffing passwords,installing keylogger etc.Detecting masquerades has become very difficult.Many proposed approaches rely on encryption by auditing a variety of sources which are not efficient.It is fair to say that all of the standard approaches that have been demonstrated to fail from time to time.Building a trustworthy cloud is not enough,avoiding data theft attacks is more important.once the data is lost we couldnot get it back.Then a basic idea is proposed which can secure data to some extent i.e disinformation attack.
This could be implemented using two techniques:

1.User search modeling
2.Decoys

A.User search modeling:

Generally the access to a users information in the cloud will exhibit normal means of access.This technique usually observes the users search behaviour.So it can easily differentiate between normal user and unauthorized user.This method is generally used in fraud detection applications.Whenever it gets suspicious it provides a security question and then gets an indication that it is a abnormal access.

B.Decoys:

Decoy information such as decoy documents provide bogus information on unauthorized access.After the user search modeling if it gets suspicious it releases false information in order to mislead the attacker.Through this we could keep important data safely.The true user, who is the owner of the information would readily identify when decoy information is being returned by the Cloud and hence could alter the Cloud's responses through a variety of means, such as challenge questions, to inform the Cloud security system that it has inaccurately detected an unauthorized access.It protects the true data from masquerades.
Decoy serves two purposes:
1.Validating whether the data is authorized and
2.Misleading the user with false or bogus information

Combining User Search modeling and Decoy technology for Masquerade detection

The two techniques complement each other.As soon as the user search modeling indicates unauthorized access the decoy technology provide bogus information.Only the authorized users could identify this decoy whereas the attackers get confused.They get lots of false information.Both the techniques provide very good security for the true confidential data.Through this the cloud becomes more trustworthy.After many experiments we could easily say that these two techniques are good at preventing masquerade attacks.

CONCLUSION

Masquerade attacks have become a serious threat to cloudcomputing.In this paper we have presented an integrated approach to prevent such attacks.Decoy documents which are stored in the cloud alongside the user's real data serve as sensors to detect illegitimate access.Once the unauthorized access is suspected,we inundate malicious insider with bogus information.These techniques which rely on decoy information technology provide high level of security in the cloud.

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 TechCrunch 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].

[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

1.Madhusri.K is pursuing B.Tech in Computer Science and Engineering from KL University,Vaddeswaram,Guntur,India.
Madhusri1708@hotmail.com
2.Navneet.Y is pursuing B.Tech in Computer Science and Engineering from KL University,Vaddeswaram,Guntur,India.
navneetyerra@gmail.com
3.Harish.CH is pursuing B.Tech in Computer Science and Engineering from KL University,Vaddeswaram,Guntur,India

4.Sandeep.A is pursuing B.Tech in Computer Science and Engineering from KL University,Vaddeswaram,Guntur,India

5.Dr.T.V.Rao is currently working as Professor Dept. of Computer Science and Engineering KL University,India.
Drtvrao@kluniversity.in