Alleviating Malicious Insider in Cloud Through Offensive Decoy Technology

Ms.B.Ankayarkanni

Department of Computer Science, *Sathyabama UniversityChennai-600 119, Tamilnadu, India.*

Abstract—

The eternal way for using computer in the way of cloud computing used to store our personal and private organization information. In this new technology for communication computing there exist many challenges for securing data. There are many data protection techniques existing which uses encryption technique that prevents data attacks from the insider in provider of cloud. To secure data from an offensive decoy attack that access data from cloud storage. To monitor data access which suspects and verify attacks send large amounts of decoy information. They also can misuse real user data which evidences the level of data security provided in cloud security. In this model we propose approach for securing data using fog computing. This technique used for launching disinformation attacks against malicious insiders which prevents them from differentiating the sensitive data provided from the fake useless data. This process alleviates the malicious insider from the cloud storage area who uses offensive technique for attacking.

Keywords—Cloud Computing, decoy technology, disinformation attack, data protection.

I. INTRODUCTION

In a cloud computational medium for data outsourcing they have efficient operational source to overcome greater risks for serious stealing of data attacks. They are simply defined as malicious insider considering top threats in cloud secured computing technology [1]. Almost all the customers have knowledge about this kind of attack threat and left with trusting of the service provider where they can protect data. They have control over transparent authentication for authorizing the controls for controlling the threat for attacks.

In such attacks over data incorporates the personal accounts of important persons even like American president. The attacker administer the password to gain access over the corporate documents of others personal account [2]. This posting of important documents in general browsing media produces significant loss for both that account provider and their customers. When an attack launched by outsider who steals administrator passwords and helps out the attacks will be inflicted by malicious insider [3]. The password from the cloud provider will be easily stolen by the malicious insider that demonstrates the theft of private keys. These type of theft stoles the confidential data which is extracted from its hard disk drive directly [4]. After when a customer password and private key is stolen then the malicious insider get access to all the customer data. When the customer has no way for detecting the data with unauthorized access the cloud computing security will focus the ways for preventing illegitimate and unauthenticated access to data developing the access control over encryption mechanism. This kind of mechanism could not able to prevent the compromising attack for preventing it. Thus this encryption technique for solutions to such threats is not sufficient for protecting the data and such mechanism is used to prevent it alone.

Our approach completely secure the cloud for decoy information technology which is known as fog computing. This technique launches attacks against the insiders prevents the sensitive customer data and differentiates it with the helpless fake data [5]. Just by deploying the decoy information for the cloud service the profiles of online personal sources by the individual users.

From different cloud services based on proposals for storing documents and fie medias accessed by the remote server used to connect with the internet. For problem such as services accesses for accepting the secure user data having problem will provide security to information which is very confidential. This remains in a core part for problem of security in which the date will not provide any assurance levels for most of the desired people [6]. They secured data from remote services in a cloud services have standard for encryption controls the access. The demonstrated approach varying from time to time for different reasons includes the insider attacks for

services configured with fault implementations creates constructive coding.

The effective bug code attacks not spy by any procedure implementing the security providers. This leads to trustworthy cloud computing environment which is not limited because of continued lost of information [7]. If there is no need to be prepared before for such lost then we have to limit the damage occurred by the stolen data. The better idea decreases the stolen data damage value and the information got by the attacker. This can be done by preventing the disinformation attacks.

The cloud security for implementing additional features for security expected for profiling the behavior of users. When the cloud exhibits the user information the technique for profiling the user applied to this model is helpful in accessing the information provided by the cloud. The behavior for normal user checks the determination of abnormal access of normal user [8]. This user information secured by the method for behavior based on fault detection application technologies. These profiles naturally increase the volume of information with the number of documents which read typically and read often. The specified features for simple user who could detect the abnormality for cloud access where the data transfer includes the scope for data.

II. DECOY INFORMATION TECHNOLOGY

There are many documents for generating the decoy information which has many honey pot files for demanding the detection of unauthorized access. This information to be accessed have extracted information serves the decoy for confusing and rebating adverse effect which is not involved in it. Integration of such technology helps in profiling behavior of the user information in the cloud service. Cloud service when deployed with abnormal access towards the noticed information returned and delivered in complete appearance of normal user which has legitimate information.

The authenticate user having complete information of owner identifying the decoy information for returning into the cloud [9]. When the cloud responds to alternate means for variety of challenges to inform the cloud system of security have inaccurate accessing of unauthorized system. When the access deliver to amount of unbounded adverse information secures the true data of the user.

The disclosure of decoy is unauthorized to help two needs for validating the access of data where the authorized information has abnormal access to information access detected for controlling the attacker information. When the combination of security features providing level for security of cloud with current mechanisms for cloud security they provide different levels. They apply such concepts for detection of illegitimate data access to store data from local file system by the attackers for storing data in the local file system. The legitimate users have impersonation of credentials stolen by them. The consideration for insider attacker with malicious attacks has settings for local files that combine most of the techniques provide better results in detecting the attackers. This approach is mostly suggested for cloud computing service.

The intended transparency of user in the local system containing files follows the results achieved by approaching the detecting the activity for local files. From the combination of profiling the behaviors of user and technology for decoy detection the legitimate users might familiar with files for system wherever they are located. The target of attack is limited to search for specified files in masquerade the access for victim who illegitimately familiar with structures containing the contents for filing system.

The widespread search for targeted results attack based on key assuming the profiles that searches the user behavior by developing the models for user training the modeling technique will support the vector machines. The importance for modeling ability to the classifier building the data without the need for sharing has different kinds of variety of users. The private users have to share data for preserved data. To monitor the abnormal search for behaviors that exhibit deviations for the attack will be potential enough to intrude in cloud. Validating the assumptions and demonstrating the reliable detection for simulating the attacks using approach with low late of false positive.

In deployment of decoy technology the traps are placed in the file system for those systems downloaded from fog computing. It has automated service for different types of decoy documents like records and receipts [10].

Those files are easily downloaded by the legitimate users and they hide it in highly private locations which could cause interference for normal user activities on the system. The familiar file system has contents for accessing the decoy files for searching the sensitive information with the knowledge of placing the bait in appropriate time.

Embedding the decoy files by monitoring the access for signaling the activity of attacks on system can carry message for authentication code which is hidden in the header of documents. The computation over contents of file use the unique key for each user with decoy document loaded in memory for verifying the decoy document [11]. Based on the contents of document the comparison for deemed alert for decoy technique will be done.

The placements for decoy file system have advantage over system of three fold detection of attacking activity. This process confuses the attacker which includes additional costs for incurring the distinguished information. The effect of hard measures for playing any significant role can help in preventing the activity for reversing the attackers. By combining different techniques of correlation which searches the behavior for anomaly detection of trap based decoy family.

To provide stronger evidence for correlating the behavior for searching the anomaly detection with trap based on protection of strong evidence for improving the accuracy. By detecting the abnormal search operations for accurate detection of unsuspecting user for decoy file system collaborating the suspicious user. The intended victim for impersonation of search operations prior to file has collaboration of the threat model for such scenarios.

For opening the accidental decoy file having the authenticate user for recognizing the accident with the search behavior for abnormal detection of abnormality. The decoy trap like effective attacks together makes the combination for techniques improving the detection accuracy. To decoy the validation for issuing alerts with monitoring of sensor nodes have user files for searching the behavior of access.

To generate decoy technology detecting the time and demand for behavior for issuing the alert to users for searching the file system while improving the accuracy detection. In case of using sensor monitoring system the access towards the behavior for searching the time demand for alert creation in simulation based analysis. The apparent attack of decoy offensive method the attacker could access.

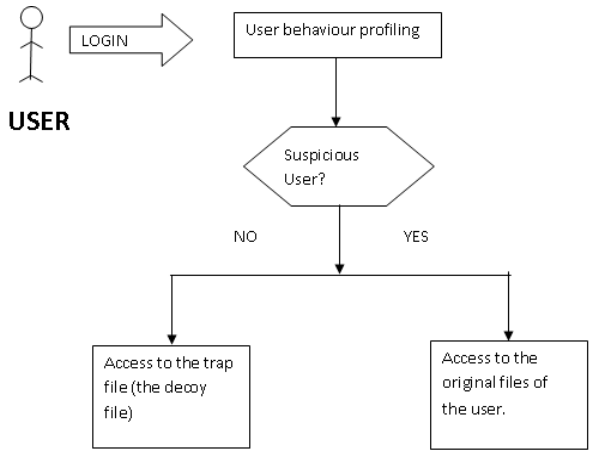

Fig.1. Security Mechanism using decoy technology.

The information is stole from obviously clear directories. They instead of making it placed in a highly secret place made them in the apparently open directories have common names for them. Thus by this method they can ensure the cause of vulnerability and the increasing chance for finding the attack detector.

While deploying the decoy technology the accuracy can be improved by further combination of some of the existing techniques. They have documents for decoy which acts as a helper for detecting the behavior of users when it is abnormal. The detection rate may be lower compares to other techniques as the false positive rate decreased to highly noted manner. From the results caused from simulation there are many classifiers used for computing the data of some of the user data collected over a period of time. The trained classifiers used for searching the behavior and detecting the anomaly with trained set of user data.

In other approach for detection they too train some of classifiers in the same basis which combines the behavior for profiling the access to monitor the decoy files based on local file system. For describing the above classifier for placing the local file system for profiling the monitoring access for decoy files. The file system for describing the access for monitoring files using the classifiers simulating the masquerade data. Displaying

the score the detection approach for user model for the results modeling uses the combination for detection approach. For equal and better resulting the profile approaches. The resulting experiments for suggesting the user profiles for detecting the unauthorized access to cloud. When accessing the unauthorized detection for responding to the present decoy technology for documents validating the access indeed of using the local file setting.

The anomaly detector used for accessing the decoy for validating the local file setting for personal and business data within the cloud for proposing the monitoring access for patterns by profiling the behavior for users. For illegitimate access of making the data from unauthorized data by detection of data exposed to the suspected real data information. Documents used for decoy technology storing information served as challenging the instance for malicious insider for the system. This kind of prevention from attacks can suspect the access for information which makes the user data easier. For social network in information technology for cloud security have distinguished levels of technology.

III. Malicious Insider Detection Using Fog Computing

The malicious insider is considered to be an attacker inside the cloud service provider for compromising data inside the cloud. The easy control for accessing the protection for data often finds solution for threats. The decoy information technology finds help for prevention mechanism using fog computing. By implementing this technique the secure user data in cloud service provider have good behavior for fog computing in decoy information technology. This technique used for providing the data security in cloud computing.

There are many offensive decoy technologies for providing the decoy information with unauthorized user access by the attacker. Relative disinformation for sending information related documents for storing in cloud is known as decoy. While monitoring the data access from the cloud detects the abnormal data access patterns. They generate useless data files for demanding the system for attacking against them.

This original information will often change with unexpected format of extracting the documents from information which is not much impossible for them to return from disinformation attacks. They can easily identify the malicious insider for preventing them from unauthorized access.

Usually the cloud user data provides storage for clouds for users from different parts where once the user can log information from their account with given user name and password. This is their private information which they can use for uploading, downloading, deleting or do any kind of operation in their personal area within their area of online cloud storage. When a malicious insider trying to attack any others personal area by masquerade their account with adverse operations for trusting the computing based on trusted adverse effects.

In case of adverse reactions there are no operations inside the trusted based computing for basic trust for operations. In case of sensitive data there is no protection for them inside the cloud storage area. There exist many encryption and decryption techniques used for transmitting the data securely over the network. As they could not stop the data access when their username and password they are stolen from the user.

Monitor the data access for cloud detection of abnormal data for accessing patterns from the wide storage area. When an unauthorized access suspecting will be questioned by the verification method for launching the disinformation attacks must return the information. Retaining such technology for large amounts for decoy information to the attacker will provide protection against the real user data. This repeated event for downloading time from cloud helps in launching the disinformation attacks.

A decoy document used for decoy information provides the information for unauthorized access with user search modeling the suspicious release for false information to mislead the attacker. This profusely confuses the attacker by providing the safety for data content. The legitimate user will get the information about the authenticate owner of any social network account providing the response over variety of means for challenges faced by data protection techniques. To inform and equip the cloud security over system for

inaccurate detection of data accessed in unauthorized manner.

The protection of real user data from the masquerade attacks returns the cloud information along with offensive decoy method having different responses over inaccurate detection of data access. There are two purposes for serving the decoy information technology which can validate the data for authorized information whether they are authorized or not. Also they help in misleading the attacker with false user information that detects the attacks in cloud security.

IV. PERFORMANCE EVALUATION

The results of the experiment with the previous models suggest that there is a larger chances of finding the suspicious users who login to the cloud system with a negative intensions.

Graph highlighting the number of suspicious users found between the methods.

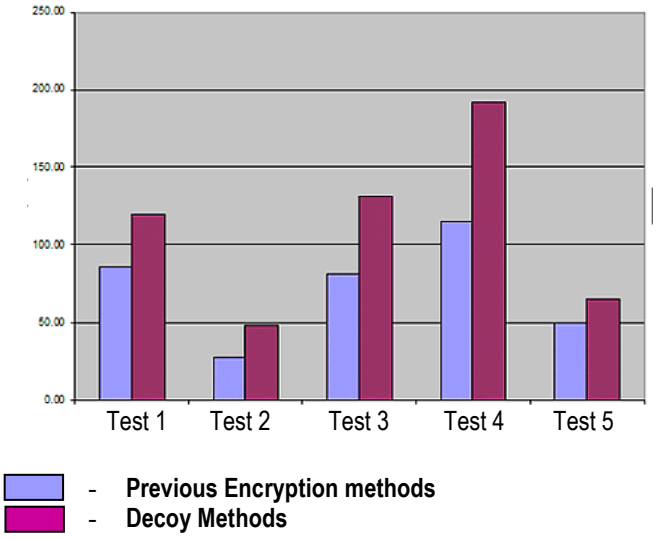

Fig 2. Performance comparisons of decoy method with the encryption model.

The results are compared with the previous methods to verify the performance of the decoy methodology. And the Fig. 2 gives the performances of the previous methodologies and the decoy method, and proves that decoy method has more chances in finding the malicious insider than the other methodologies.

V. CONCLUSION

In our proposed paper we have a tendency to deploy decoy documents keep in cloud together with real user knowledge served as detector for detective work the illegitimate access. once AN unauthorized user accessing and exposing the suspected verification can have any instance of malicious corporate executive of real user knowledge for data at intervals the limit. Hindrance of such attacks depends on misinformation technology that provides completely different levels of security at intervals the social networks. They supply fog computing for overcoming the matter for decoy computing technology. This helps in protective user data from the attacks of cloud security.

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

[7] Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV '11, June 2011.

[8] 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

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

[10] 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.

[11] 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/

[12] 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.