ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Preclusion of Insider Data Theft Attacks in the Cloud

Ameya Bhorkar[1], Tejas Bagade[2], Pratik Patil[3], Sumit Somani[4]

Computer Science Department, P.V.G.'S C.O.E.T, Parvati, Pune, India[1,2,3,4]

Abstract: Cloud Computing is the fastest growing technology in the software market. We are using clouds from Google Drive to social networking everyday. It is result of evolution and adoption of existing technologies. With these new computing and communications paradigms arise new data security challenges. Various protection mechanism techniques like Encryption have failed in preventing attacks carried out by Cloud service provider employees i.e. insider attack. To solve such issues, we proposed a new approach for securing data in the cloud using Decoy files. We observe data access patterns for user of cloud, based on these observations, we are deciding to send original or decoys file to user. 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. This protects against the misuse of the user's real data

Keywords*:* Decoy files**,** Cryptographic keys, OTP, DSA.

1. INTRODUCTION

There is, to date, no universally agreed industry definition of cloud computing and it is usual to find conflicting descriptions in any nascent industry. Cloud computing is a term used to describe a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure.

Most of Businesses are opting for data outsourcing and computation to the cloud. This increases the efficiency but risk factors of data theft attacks also increases. Although cloud computing is portrayed as a generally valuable consideration for enterprise IT integration, adoption of cloud computing models carry a number of risks. It is difficult to detect data theft attack when it is launched by the insider. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance.If an insider is having customer's password then he can access user account without any difficulty.

Current research going in cloud computing security has shown that sophisticated access control and encryption techniques have failed against insider attacks. Hence there was urgent need to deal with such attacks.

2. PREVIOUS SYSTEM

In present era we have shifted from clients and centralized provision to cloud computing. It is also strongly founded that due to lack of direct resource control there is data privacy violations and leakage of sensitive information by service providers. The Fully Holomorphic Encryption (FHE) tool is one of the promising tool to ensure data security, but cryptography algorithm alone cannot fulfil the privacy demanded by common cloud computing services by defining a hierarchy of natural classes of private cloud applications.

It is proposed that a malicious insider can steal any confidential data of the cloud user in spite of provider taking precaution steps like. 1) Not to allow physical access. 2) Zero tolerance policy for insiders that access the data storage. 3) Logging all accesses to the services and later use for internal audits to find the malicious insider. It proposes to show four attacks that a malicious insider could do to: - (I) Compromise passwords. (ii) Cryptographic keys and (iii) Files and other confidential data like, clear text passwords in memory snapshots, obtaining private keys using memory snapshots, extracting confidential data from the hard disk and Virtual machine relocation.

3. PROPOSED SYSTEM

Providing security of confidential information, is the main problem which remains a core security problem that, to date, has not provided the levels of assurance most people desire. Many proposals have been made to secure remote data in the Cloud based on encryption. It is not wrong to say that all of the standard approaches have been demonstrated to fail for a variety of reasons, including insider attacks. Construction of trustworthy cloud system alone is not important because accidents continue to happen, and when they do, and information gets lost and there is backup mechanism.

Our basic ideology is that we can minimize the damage of stolen data if we subside the value of stolen information to the attacker. This can be achieve through 'preventive' wrong information attack. Our proposed cloud system has two security features:

1) User Behaviour Profiling:

We expect that cloud user will access his account on cloud in normal way. User profiling is a famous technique that can be used to monitor user behaviour. This can be used to decide user type.

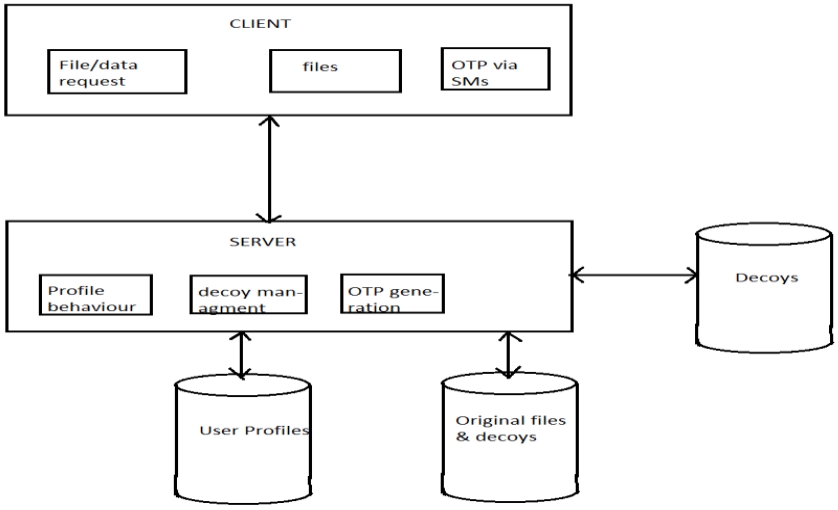
This method of behaviour-based security is commonly used in fraud detection applications. Such profiles would include timing information, type of documents read and its frequency, access pattern. These simple features can be used to detect user behaviour.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

2) Decoys:
Decoy information is nothing but bogus information which can be generated on demand and serve as a mean sof detecting unauthorized access to information. It can be used to 'poison' the thief's ex-filtrated information. Serving decoys will muddle and confuse an adversary into believing they have ex-filtrated useful information. This technology can be combined with user behaviour profiling technology to secure a user's information in the Cloud. Whenever illegal user is detected cloud will send back decoy files. The true user, who is the owner of the information, can easily know decoy information is being returned by the Cloud, and hence could alter the Cloud's responses through one time password facility provided by us, to inform the Cloud security system that it has wrongly detected an unauthorized access. In the case if access is detected as illegal, Cloud security system would deliver unbounded amounts of bogus information to the adversary, thus shielding user's true data from unauthorized disclosure. The decoys serve two purposes: (1) validating whether data access is authorized when abnormal information access is detected, and(2) confusing the attacker with bogus information.

4. SYSTEM ARCHITECTURE



The overall system is a typical client server model with some significant and powerful modifications. The server will respond differently to different users, based on output of the profile matching algorithm.
The client (genuine or malicious) can make file or data request to the server. This request can either for searching, uploading, downloading, deleting a particular file.
If system has incorrectly detected a true user to be illegal, then it will provide facility of OTP to the user which is sent to user on his registered mobile using a third party mobile gateway. This OTP can be used for validation. This will help in case the access behaviour diverts from normal behaviour for a genuine user.
ANN algorithm will be used to check the user profiling based on user characteristics.
This algorithm is based on neuron network present in human brain. It is used to recognize the user behaviour based on its characteristics as in this case access pattern.
It will decide whether user is legal or malicious.
The server will have different modules for carrying out different tasks such as user access behaviour profiling decoy management and OTP generation & validation. The database will contain a sufficient stock of decoy file of many different formats. Also the user profile and original files of the user will part of the same database. For all the decoys files in database DSA will be calculated using SHA-1 i.e. secure hashing algorithm. It provides 20 byte unique digital signature which can be used further for validation. In order to recognize user behaviour accurately, we need to have user multiple access initially. Another requirement is that database should large enough to apply ANN for finding actual user.

5. CONCLUSION

In this paper, we present a new tactic to securing personal and business data in the Cloud. We propose supervising data access patterns by profiling user behaviour to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we flood 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 unparalleled levels of security in the Cloud and in social networks.

REFERENCES

[1] Salvatore J. Stolon, Malik Ben Salem, Angelo's Keromytis Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud IEEE Computer society 2012

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

[2] 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

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

[4] 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].