International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-8, August 2015

Identifying data theft attack using fog computing

Kiran G.Dhapodkar, Prof. Kahkashan Siddavatam

***Abstract*— Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new data security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider.**

We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a Cloud environment.

***Index Terms*— Data storage, privacy-preserving, public auditability, cryptographic protocols, cloud computing.**

I. INTRODUCTION

Cloud computing is achieving popularity and gaining attention in business organizations. It Offers a variety of services to the users. It is an ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [1]. Due this ease, software companies and other agencies are shifting more towards cloud computing environment. To achieve better operational efficiency in many organizations and small or medium agencies is using Cloud environment for managing their data. Cloud Computing is a combination of a number of computing strategies and concepts such as Service Oriented Architecture (SOA), virtualization and other which rely on the Internet.It is considered as a delivery platform in which resources are provided as a service to the client through the Internet. Although, Cloud Computing provides an easy way for accessing, managing and computation of user data, but it also has some severe security risks. There are some traditional security mechanism such as identity, authorization and authentication, but now these are not sufficient [2]. Very common risks now days are data theft attacks. Data theft is considered one of the top threats to cloud computing by the Cloud Security Alliance [3]. Moreover, if the attacker is an Insider than the chances of data theft increase as the insider may already have some personal information. The common notion of a cloud insider as a rogue administrator of a service provider is discussed, but we also present two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource[11].

To deal with such cases and malicious intruders there are some techniques which are used to secure user data. A new technology called Fog computing is gaining attention of the cloud users nowadays. Salvatore J. Stolfo et al. used it for making disinformation attacks against the malicious intruder or attacker Fog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, compute, storage, and application services to end-users. The difference is Fog provides proximity to its end users through dense Geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network.

II. PROPOSED SYSTEM

The proposed system has the objective to validate the access is authorized or not and if abnormal access is detected than providing the hacker with encrypted or unreadable information. Fog Computing deals with two technologies User Behavior Profiling and Decoy Information Technology.

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. The decoys, then, serve two purposes: (1) validating whether data access is authorized when abnormal information access is detected, and (2) confusing the attacker with bogus information.

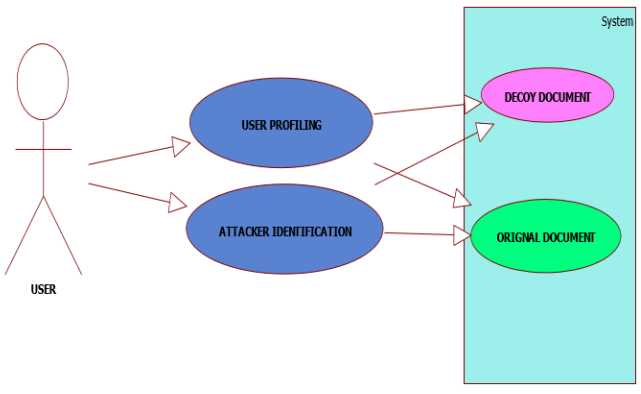

Fig. 1: Decoy System

Decoy data, such as decoy documents, honeypots and other bogus information can be generated on demand and used for detecting unauthorized access to information and to „poison" the thief"s ex-filtrated information. Serving decoys will confuse an attacker into believing they have ex-filtrated useful information, when they have not. This technology may be

Kiran G.Dhapodkar, Department of Computer Engineering, Lokmanya Tilak College Of Engineering, Navi Mumbai, India
Prof. Kahkashan Siddavatam, Department of Computer Engineering, Lokmanya Tilak College Of Engineering, Navi Mumbai, India

integrated with user behavior profiling technology to secure a users data in the Cloud. .

Whenever abnormal and unauthorized access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way that it appear completely normal and legitimate. Fig 1 shows that the legitimate 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 incorrectly detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Cloud security system would deliver unbounded amounts of bogus information to the attacker, thus securing the user's true data from can be implemented by given two additional security features: (1) validating whether data access is authorized when abnormal information access is detected, and (2) confusing the attacker with bogus information that is by providing decoy documents.

III. DESIGN GOALS

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee: 1) Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users; 2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact; 3) Privacy-preserving: to ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process; 4) Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously; 5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

IV. THE PROPOSED SCHEME

Fog Computing system is trying to work against the attacker specially malicious insider. Here malicious insider means Insider attacks can be performed by malicious employees at the providers or users site. Malicious insider can access the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files. The threat of malicious attacks has increased due to lack of transparency in cloud providers processes and procedures. It means that a provider may not know how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed.

The actual working of the fog computing .In two ways login is done in system that are admin login and user login .When admin login to the system there are again two steps to follow:
step1:Enter username

step2:Enter the password.

After successful login of admin he can perform all admin related tasks, but while downloading any file from fog he have to answer the security Question if he answer it correctly then only original file can be download. In other case ,when admin or user answer incorrectly to the security question then decoy document (fake document) is provided to the fake user . Decoy technology work in the given manner if you have any word ,suppose "MADAM" in the document then some alphabets are replaced as M->A then the given word become "AADAA" which have no meaning. In some Case ,if attacker getting to know that „M‟ is replaced by „A‟ in the given document and by applying reverse engineering he get result as "MMDMM". In any case he can‟t judge content of document.

V. EVALUATION

Let us consider that we have database 'D' and 'n' number of attribute such as user name, user id etc.

D = {A|A ε Information of user}

Here D is the set of all A such that A is information of user which is to be store on server

Consider following function

STORE (D, SERVER): Here admin enter the user information into database at server.

Let us consider that the receiver provide us with value "X" for every input it obtain from the every time login account of the particular user .so we can further assume to have a set 's to have value 'n' number of detect value at particular instance.

Let us denote the current situation in the following manner

S = {X| ✂ X ε D ∃ ID for attacker}R · e(σγ,g) = e((sc Y i=s1H(Wi)vi)γ · uμ,v). (1)

Suppose that our extractor can rewind a cloud server in the execution of the protocol to the point just before the challenge h(R) is given. Now the extractor sets h(R) to be γ* _= γ. The cloud server outputs {σ, μ*,R} such that the following equation holds.

Here S is the set all X such that for all X there exits Id for user.

Now, for some X value that match with some value inside the database when admin check user account update.

1. GET(D,X,SERVER): Admin get all information about the user account from server.

2. PUT(X,ATK,SERVER): Here admin will upload attacker's information on server.

3. PUTP(X,REPORT,SERVER) : Here admin upload daily report on server.

VI. CONCLUSION

In this paper we propose a distinct technology to make the cloud safer by securing the personal and the important data of the business firms. We provide monitoring of the access to the account by checking the behavior of the user. We provide access not only by login credentials but also by challenge questions which would be only known to the user. If the access found to be unauthorized thus providing with the fake data so that the real data of the user can be saved. This technology would add up a level in securing the data on the cloud.

ACKNOWLEDGMENT

This work was supported in part by the US National Science Foundation under grant CNS-0831963, CNS-0626601, CNS0716306, and CNS-0831628.

REFERENCES

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

[2] 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.

[3] 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,pp. 1–8, 2010.

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

[5] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010.S. Wilson, "Appengine outage," Online at http://www. cio-weblog.com/50226711/appengine outage.php, June 2008.

[6] M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

[8] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www. cloudsecurityalliance.org.

[9] Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC, 2009, pp. 109–127.

[10] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. of CCS'09, 2009.

[11] P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010.

[12] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010.

[13] M. Arrington, "In our inbox: Hundreds of confidential twitter documents," July 2009.

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

[15] B. M. Bowen and S. Hershkop, "Decoy Document Distributor".

[16] Ali Ahmad Milad, Hjh Zaiton Muda, Zul Azri Bin Muhamad Noh, Mustafa Almahdi Algaet," Comparative Study of Performance in Cryptography Algorithms" Journal of Computer Science 8 (7): 1191-1197, 2012 ISSN 1549-3636, Malaysia, 2012.