Prevention Of Malicious Insider In The Cloud Using Decoy Documents

S. Muqtyar Ahmed[1], P. Namratha[2], C. Nagesh[3]

[1]M.Tech, Department of CSE, Intell Engineering College, Anantapur, AP, INDIA.
[2]Assistant Professor in Department of CSE, Intell Engineering College, Anantapur, AP, INDIA.
[3]Associate Professor in Department of CSE, Intell Engineering College, Anantapur, AP, INDIA.

ABSTRACT

Cloud[1] computing is the use of computing resources (hardware and software) that are delivered as a service over a network. Cloud computing entrusts remote services with a user's data, software and computation. 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. The data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those illegal actions by a malicious insider[2] to the cloud. Much research in cloud computing security has focused on ways of preventing malicious insider and illegitimate access to data. A different approach to secure the cloud using decoy information technology, which we have come to call Fog computing[3]. Decoys[4] are used to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data. Alert message is issued to authenticated user.

Keywords: *Cloud[1], Malicious Insider[2], Fog Computing[3], Decoys[4]*

Introduction

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It provides three services they are as

Software as a Service (SaaS): Offers renting application functionality from a service provider rather than buying, installing and running software yourself. Examples include Salesforce.com and Gmail.

Platform as a Service (PaaS): Provides a platform in the cloud, upon which applications can be developed and executed. Examples include Salesforce.com, through Force.com, and Microsoft (Azure).

Infrastructure as a Service (IaaS): Vendors offer computing power and storage space on demand. Examples include, Rackspace and Amazon S3.

The following figure shows the structure of the cloud computing,

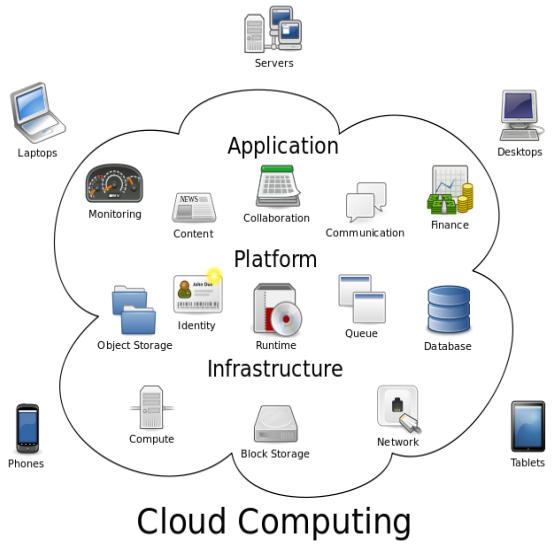

Fig 1: Structure of cloud computing

Cloud Computing Threats: As we already mentioned, there are several significant threats that should be considered before adopting the paradigm of cloud computing, these threats are

1. *Abuse and Nefarious Use of Cloud*
2. *Malicious Insider*
3. *Data Loss or Leakage*
4. *Account or Service Hijacking*
5. *Unknown Risk Profile*

Much research in Cloud computing security has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise. Van Dijk and Juels have shown that fully homomorphic encryption, often acclaimed as the solution to such threats, is not a sufficient data protection mechanism when used alone [1].

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.

Malicious Insider

Insider attacks can be performed by malicious employees at the provider's or user's site. Malicious insider can steal the confidential data of cloud users. This threat can break the trust of cloud users on provider. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may involve various types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has increased due to lack of transparency in cloud provider's processes and procedures [2]. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed. Additionally, users have little visibility about the hiring practices of their provider that could open the door for an adversary, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection. Malicious insider attacks can damage the financial value as well as brand reputation of an organization.

User Behavior Profiling

It is expected that access to a user's information in the Cloud will exhibit a normal means of access. User profiling is a well known technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such

'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. These simple user specific features can serve to detect abnormal Cloud access based partially upon the scale and scope of data transferred [3].

Legitimate users of a computer system are familiar with the files on that system and where they are located. Any search for specific files is likely to be targeted and limited. A masquerader, however, who gets access to the victim's system illegitimately, is unlikely to be familiar with the structure and contents of the file system. Their search is likely to be widespread and untargeted. Based on this key assumption, we profiled user search behavior and developed user models trained with a one class modeling technique, namely one-class support vector machines. The importance of using one-class modeling stems from the ability of building a classifier without having to share data from different users. The privacy of the user and their data is therefore preserved. We monitor for abnormal search behaviors that exhibit deviations from the user baseline. According to our assumption, such deviations signal a potential malicious insider.

Decoys

Decoy information, such as decoy documents, honeyfiles, honeypots, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's ex-filtrated information. Serving decoys will confound and confuse an adversary into believing they have ex-filtrated useful information, when they have not. This technology may be integrated with user behavior profiling technology to secure a user's information in the Cloud. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely legitimate and normal. 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. 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 adversary, thus securing the user's true data from unauthorized disclosure.

Decoy Technology

We placed traps within the file system. The traps are decoy files downloaded from a Fog computing site, an automated service that offers several types of decoy documents such as tax return forms, medical records, credit card statements, e-bay receipts, etc. [4]. The decoy files are downloaded by the legitimate user and placed in highly-conspicuous locations that are not likely to cause any interference with the normal user activities on the system. A masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files, if he or she is in search for sensitive information, such as the bait information embedded in these decoy files. Therefore, monitoring access to the decoy files should signal masquerade activity on the system. The decoy documents carry a keyed-Hash Message Authentication Code (HMAC), which is hidden in the header

section of the document. The HMAC is computed over the file's contents using a key unique to each user. When a decoy document is loaded into memory, we verify whether the document is a decoy document by computing a HMAC based on all the contents of that document. We compare it with HMAC embedded within the document. If the two HMACs match, the document is deemed a decoy and an alert is issued. The advantages of placing decoys in a file system are threefold:

(1) The detection of masquerade activity

(2) The confusion of the attacker and the additional costs incurred to distinguish real from bogus information, and

(3) The deterrence effect which, although hard to measure, plays a significant role in preventing malicious insider.

Whenever the decoy document is downloaded an alert message which consists of data that attacker acquired is issued to the authenticated user.

Conclusion

We present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behavior 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. An alert message is issued about the attacker to the real user. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data.

References

[1] 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

[2] E., Mathisen, "Security challenges and solutions in cloud computing," in Digital Ecosystems and Technologies Conference (DEST), 2011 *Proceedings of the 5th IEEE International Conference on*, 2011, pp. 208-212.

[3] 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.

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