Alleviation of data attacks in cloud computing using offensive decoy technology

G.Ramesh Kumar, Assistant Professor, Dept. of CA, Vasavi College of Engineering, Hyderabad.
Balaji Tedla, Assistant Professor, Dept of CSE, Vasavi College of Engineering, Hyderabad.

Abstract - *Cloud computing is the new era which facilitates as per the user requirements. To provide the services to the user the major problem is the security. 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*.

Keywords – cloud computing, security.

1. INTRODUCTION

The cloud provider has to ensure that the customer does not face any problem such as loss of data or data theft. There is a chance that attacker can mitigate as a legitimate user, there by effecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. The following are the security issues

i. Data Issues

Whenever data is on a cloud, anyone can access common, private and sensitive data in a cloud from anywhere any time. So that the customer, the cloud provider can modify data. Data stealing and data loss are the serious issues in a cloud computing environment. These are occurred due to cloud service provider depends on the others server, shutdown of his service due to legal problem etc.

ii. Privacy Issues

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintain the server so that it enable the provider to protect the customer's personal information.

iii. Infected application

Any malicious user is uploading any infected application onto the cloud which will affect the customer and cloud computing service.

iv. Security Issues

Security must be provided on two levels. One is on provider level and another is on user level. The user should make sure that there should not any loss of data or stealing or tampering of data for the other users who are using the same cloud due to its action.

v. Trust issues

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

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.

2. EXISTING SYSTEM

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. 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.

3. PROPOSED SYSTEM

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.

MODULE DESCRIPTION:

1. Cloud Computing.
2. User Behavior Profiling:
3. Decoy documents.

1. cloud computing

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 divide into three type.

1.Application as a service.
2.Infrastructure as a service.
3.Platform as a service.

Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.
2. Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation. The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.
3. Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.
4. Multi tenancy enables sharing of resources and costs across a large pool of users.
5. Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
6.Utilization and efficiency improvements for systems that are often only 10–20% utilized.
7.Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
8.Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
9.Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible.

Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
10. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

2. User Behavior Profiling:

We monitor data access in the cloud and detect abnormal data access patterns 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. We monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy.

3.Decoy documents.

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. 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. 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.

4. 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. 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. Such preventive attacks that rely on disinformation technology, could provide unprecedented levels of security in the Cloud and in social networks model.

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,"July2009.[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: Stealingconfidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers

and Virtual ComputingEnvironments, 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]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934

[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].