ISSN 2395-1621

FOG COMPUTING :USING DECOY TECHNIQUE

[#1]Rupesh R Bhairat, [#2]Ajit N Ghagare, [#3]Yogesh K Nath

[1]rupeshbhairat@gmail.com
[2]ajitnghagare919@gmail.com
[3]nathyogesh03@gmail.com

[#123]Department of Computer Engineering

G H Raisoni College of Engineering And Management,
Wagholi, Pune.

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.

ARTICLE INFO

Article History

Received: 27th November 2016

Received in revised form :

27th November 2016

Accepted: 1st December 2016

Published online :

2nd December 2016

Keywords: Cloud Computing, User Behavior Profiling, Decoy documents

I. INTRODUCTION

Cloud storage is a model of networked enterprise storage where data is stored in virtualised pools of storage. Outsourcing data and storing in on Cloud has become an extremely convenient option for the business sector. In spite of an excellent operational efficiency, storing data on cloud has its own set of drawbacks which cannot be ignored. Masqueraders mimic legitimate users after stealing their credentials when they access of Cloud. When the masqueraders logs in with the stolen credentials, he acts as the legitimate user with the same access rights as the real users. This type of attack is an insider attack. The data theft attacks carried out by an insider is one of the top threats to Cloud security. Given the headlines over the past couple of years, there remains a concern about outages, loss of control over security policies, exposing data to attack or privacy breaches. One of the latest examples being the credit card data breach at Marriot, Sheraton and other hotels. The company said information subject to potential theft by cyber criminals included names and numbers on consumers' debit or credit cards, security codes and card expiration dates. Fog computing provides- Low latency and location awareness, it has Wide-spread geographical distribution, supports Mobility, is compromised due to the huge number of nodes. The main task of fog is to deliver data and place it closer to the user who is positioned at a location which at the edge of the network. Here the term edge refers to different nodes to which the end user is connected and it is also called edge computing. If we look according to architecture fog is situated below the cloud at the ground level. The term fog computing is given by CISCO as a new technology in which mobile devices interact with one another and support the data communication within the Internet of Things. But here we consider Fog Computing as a paradigm through which we can provide local access to the user and with the help of decoy technology, we provide security for user data and prevent insider theft attacks.

II. LITERATURE SURVEY

Kaufman L. et al. (2009) [7] has examined some security issues and the associated regulatory and legal concerns that

have arisen as cloud computing. Interestingly, a major concern included in the Security Content Automation Protocol is the lack of interoperability between system-level tools. By combining industry best practices with the oversight National Institute of Standards and Technology US and other entities are developing, we can effectively address cloud computing's future security needs. They also emphasize on the of providing data confidentiality which can impact the incident reporting.

Grobauer B. Et al. (2012), [8] provided an overview of vulnerabilities in security of cloud. They explained the meaning of the term vulnerability that it it's the probability that an asset is unable to defend itself against a threat.they said vulnerabilities should always be defined in terms of resistance to attacks or threat.Control challenges typically highlight situations in which otherwise successful security controls are ineffective in a cloud setting. They have discussed about the core cloud computing technologies such as web applications and services which use SaaS and PaaS platforms, virtualization and said that there are many such security requirements which are solvable only with the help of cryptographic techniques. Thus, these challenges are of special interest for further cloud computing security research.

Sabahi, F. (2011) [9] mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. In this paper he has summarized reliability and availability related issues of cloud resources provided by the trusted third party. He discussed about the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology offering the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown [9].He said that security is the most argued concern in cloud computing because user's entire data is stored at a remote location and that location needs to be secure enough that it could deal with data thefts and malicious intruders.

Claycomb, W. R. (2012) [10] has characterized a hierarchy of administrators within cloud service providers and also gave examples of attacks from real insider threat cases. They discussed how cloud architecture let attackers to breach the security. They have also presented 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. They mentioned the key challenges faced by cloud providers and clients for securing their highly confidential data.

III. 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 Behaviour Profiling:**
3. **Decoy documents.**

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 thus allowing for

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.

User Behaviour 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.

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.

IV. CONCLUSION

With the increase of data theft attacks the security of user data security is becoming a serious issue for cloud service providers for which Fog Computing is a paradigm which helps in monitoring the behavior of the user and providing security to the user data. Other techniques discussed in this paper use Fog computing for optimizing the website performance. We hope that by continuing this work using Fog Computing platforms can lead to improved defensive techniques and would contribute in increasing the level of security if user data on the cloud.

REFERENCES

[1] Hashizume K., Rosado D. G.,Fernandez- Medina E. and Fernandez E. B. "An analysis of security issues for cloud computing". Journal of Internet Services and Applications, 2013, 4(1), pp. 1-13.

[2] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472- 484.

[3] Archer, Jerry, et al. "Top threats to cloud computing v1. 0." Cloud Security Alliance (2010).

[4] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[5] Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.

[6] Zhu, Jiang, et al. "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture." Service Oriented System Engineering (SOSE), 2013 IEEE.

[7] Kaufman, L. M. "Data security in the world of cloud computing". Security & Privacy, IEEE, 2009, 7 (4), 61-64.

[8] Grobauer, B., Walloschek, T., & Stocker, E. "Understanding cloud computing vulnerabilities". Security & Privacy, IEEE, 2011, pp. 50-57.

[9] Sabahi, F. "Cloud computing security threats and responses", In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (2011, May),(pp. 245-249).

[10] Claycomb, W. R., & Nicoll, A. "Insider Threats to Cloud Computing: Directions for New Research Challenges", In Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual, 2012, July, pp. 387-394.

