A Survey on Cloud Computing Risks and Remedies

Amit Garg
Assistant Professor
Govt. Women Engineering College, Ajmer, India

Rakesh Rathi, PhD
Assistant Professor
Govt. Engineering College, Ajmer, India

ABSTRACT
Cloud computing is sharing of enormous resource with a billing plan creating ease and providing solution for IT needs to a business of any size. Growth of public cloud has contributed widely in making cloud a household name in the field of software use ,creation, deployment or even management but at the same time securing the cloud is most important responsibility of cloud provider to build trust in the customers. This paper talks about most common threats and the strategies to deal with the risks.

Keywords
Cloud Risk, Cloud Security

1. INTRODUCTION
With the evolution and growth of cloud computing a startup today does not need to buy servers or installation of operating systems and dealing with configurations, they just need to pay and use the computational/storage power of clouds. In cloud accounting is based on computing requirements and the use hence cost is prime factor for the popularity of cloud along with other important advantages like availability, reliability, scalability, elasticity and so on.

Reliability of operations in cloud computing depends on the implementation of security policies that offers technical, legal and administrative challenges at the server, client and network side.

According to Cloud Security Alliance[1] customers are both eager and worried at the prospects of Cloud Computing. They don't have to put efforts for infrastructure management at the same time they are concern about security risks as they feel loss of control over their machine, application or data.

In software as a service (SaaS) the cloud provider is responsible for securing each layer of underlying cloud architecture, such as datacenter, virtualization, operating system, application and Data. In platform as a service (PaaS), the user of cloud service is responsible for securing the applications. In infrastructure as a service (IaaS), the user of cloud service generally has the greatest security responsibility and the cloud service provider is only responsible for securing the datacenter and the virtualization layer.

This paper discuss and survey about the following most common security issues and work towards solution domain.

a) Abuse or Evil Use.

b) Malicious Insiders/weak access control.

c) Data Loss /Leakage.

d) Account or Service Hijacking..

1.1 Abuse or Evil Use:
According to N. V. Juliadotter and K. R. Choo [2], the risk associated with a given attack scenario is composed of the likelihood of a successful attack and the impact of the attack. The likelihood can be determined based on a combination of the five dimensions identified in the first level of the taxonomy that is, source, vector, target, impact, and defense. after identifying the risk they have give it a rating between 1 (low risk) and 9 (high risk) using OWASP risk assessment formula and calculated the average of the likelihood and impact levels. A risk severity of 0–3 is considered low, 3–6 medium, and 6–9 high. To keep pace with the growth and changing face of criminal activity, cloud service providers and users must have a model that they can use to identify, classify, quantify, and prioritize threats and risk that is the aim of their five-dimension mode.

Similarly X. Chen et al. in their research paper "A Cloud Security Assessment System Based on Classifying and Grading,"[3] have determined the protection objects according to the cloud service's delivery mode. Table 1 compares protection objects in cloud and traditional information systems.

Table 1. Protection objects in cloud and traditional information systems.[3]

Delivery Model	Security	Traditional Protection Objects	Cloud Protection Objects
IaaS	Physical	Device, Medium, Environment	Device, Medium, Environment
	Network	Traditional Network Structure and Device	Virtual Network Structure and Device
	Host	OS, Database	OS, Database, VM
	Resource	na	Host, VM, VMM, VM Cluster
PaaS	Platform	na	Middleware Development Framework
SaaS	Application	Business Application System	Business Application System
	Data	Data	Data

1.2 Malicious Insiders/weak access control:

Z. Tari et al. [4] in their paper "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges," states that most cloud systems include basic access control and almost every system has privileged users, such as system administrators who have unrestricted access to user data. Insider threats are particularly need to focus on because such attacks can lead to massive damage. The multi-tenant nature of the cloud makes it difficult to detect and prevent insider attacks. solution is Homomorphic encryption that allows computations to be carried out on encrypted data , thus generating an encrypted result, which, when decrypted, matches the result of the same operations performed on the original data (plaintext). This can be a major advantage for applications that outsource encrypted data to the cloud. Homomorphic encryption is attractive for many applications, but it has a serious limitation: the homomorphic property is typically restricted to one operation.

To deal with Insider Attack from Tenant Domain a tenant Specific Attack Detection[5] component can be added in the cloud architecture, to detect insider attacks. This component can be used to log the activity of the users on their systems. The logs can help to extract the behavior of user, identify security policies that need to be enforced and also to analyze the attacks if the malicious insider is successful in exploiting the vulnerabilities in the tenant virtual machines. However monitoring user activity may not be effective against newly added malicious insiders who do not have much history. Hence tenant Specific Attack Detection component detects the attacks by monitoring the user activity and system state for suspicious behavior. To handle Insider Attacks from Cloud Service Provider a simple role based access control model for system administrators of the cloud providers may be used. These system administrators will need different levels of access to the resources in the cloud to perform their tasks. However the privileged domains in the current VMMs do not support fine granular access control for the cloud administrators. An important principle in the design of secure systems is the notion of least privilege that means system administrators will need to have only those privileges that are needed for the tasks at hand.

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, cloud providers may utilized and combined three cryptographic techniques: KP-ABE, PRE and lazy re-encryption[6].

It is a simple concept not allowing data to last in volatile memory if not in use to improve security hence arise need for evolution from generalizes time-based file assured deletion into a more fine-grained approach called policy-based file assured deletion, in which data files are assuredly deleted when the associated file access policies are revoked and become obsolete. The idea[7] is to decouple the management of encrypted data and cryptographic keys, such that encrypted data remains on third-party cloud storage providers, while cryptographic keys are independently maintained and operated by a quorum of key managers that altogether form a reliable union.

Sharing cloud data among dynamic user groups at a fine grained level a scheme is proposed[8] by defining and enforcing access policies based on the attributes of the data, permitting key generation center (KGC) to efficiently update user credentials for dynamic user groups and allowing some expensive computation tasks to be performed by untrusted CSPs without requiring any delegation key.

1.3 Data Loss /Leakage:

J. Aikat et al. [9] mentions in their research paper titled "Rethinking Security in the Era of Cloud Computing," that sharing hardware resources can cause the unintentional leakage of secret information across tenant boundaries in cloud contexts called side channels This condition arise due to tenants' shared use of micro architectural components on shared architecture. side channels should not be left unchecked otherwise sensitive information like encryption data might leak causing serious damage.

Defenses against side channels in cloud contexts, ranging from specialized defenses against side channels in processor caches to more holistic defenses for wide ranges of side-channel attacks arising from co-residency. An example of a cache-specific defense is hypervisor scheduler modifications to ensure that one virtual machine (VM) can't preempt another with very fine granularity.

From a tenant point of view, the cloud security model does not yet hold against threat models developed for the traditional model where the hosts are operated and used by the same organization. However, there is a steady progress towards strengthening the IaaS security model[10].

Despite all of the preventive measures put in place by a company, a data breach can still occur. A manufacturing company must be able to promptly detect a data breach to prevent malicious insiders and competitors from further exploiting the vulnerability to obtain company documents and secrets. The breach identification module should monitor the data exchanged and stored within clouds when a given manufacturing process is performed, checking the correct flow of data within the overall infrastructure. Breach identification remains an open research issue, and lacks a substantial body of literature. One possible solution is to use digital watermarking and other steganography based approaches on the data held by the cloud manufacturing solution[11]. The principle is to include data that can be used to detect possible unauthorized modifications or access resulting from a data breach.

In cloud environment specially in public cloud Multiple VMs can be created in the same physical machine with different configurations. Each VM will have its own virtualized RAM, swap space, disk, etc. The way such resources are allocated and deallocated in the cloud is not clear. Upon initialization and during runtime, user VMs are allocated memory and storage from a shared pool of memory pages and physical hard disks. After termination, VM resources are re-allocated to the shared pool. This may lead to leaking private and sensitive contents from one user VM to a different user VM. Besides this situation of leakage, data may also be leaked during dynamic resource allocation. In cloud, the total VMs memory allocation might exceed the physical host memory. Careless management of the aftermath of VM memory to disk spill-over might leave traces of VM memory content when the storage is later allocated to another VM.

Memory over-commitment needs to be managed only when all allocated memory is used. In the situation where one VM needs all the allocated memory, then the hypervisor will use an over-commitment management technique to identify the idle memory in the VMs and dynamically reallocate that memory to the other VMs that need it.Popular memory over-commitment techniques are Transparent Page Sharing, Ballooning and Hypervisor Swapping[12].

1.4 Account or Service Hijacking:

Account or service hijacking is a kind of identity theft aimed at deceiving end users. to deal with it along with the authentication practices, organizations should try to get as minimal information as possible, to uniquely identify and authenticate their users. Most publicly available information on social media should not play a key role in the user authentication process. It can be concluded that an Incident Response Plan is of top importance irrespective of nature of the incident[13].

2. CONCLUSION

Threats discussed in this paper as summarized in Table 2 is commonly seen subset of all possible threats that may affect the cloud and every careless enhancement of the technology is adding to the vulnerabilities in cloud computing. Also the solution is not confined to a particular technology. Combination of techniques mentioned in this paper along with other models like privacy preservation, SLA based security, security overlay network etc is also suggested.

Table 2. Risk and Remedies in Cloud Computing.

Threat/Risk	Remedies
Abuse or Evil Use	Risk assessment based on Classification and grading.
Malicious Insiders/weak access control	Encryption, Role based access control, log user activity, policy based file deletion
Data Loss /Leakage	VM preemption policy, check correct data flow, digital watermarking, memory over-commitment management
Account or Service Hijacking	Minimal user information for authentication, incident response plan

3. REFERENCES

[1] Cloud Security Alliance, "Top threats to Cloud Computing" version 1 (2010), http://www.cloudsecurityalliance.org/topthreats, Mar 2010.

[2] N. V. Juliadotter and K. R. Choo, "Cloud Attack and Risk Assessment Taxonomy," in IEEE Cloud Computing, vol. 2, no. 1, pp. 14-20, Jan.-Feb. 2015.

[3] X. Chen, C. Chen, Y. Tao and J. Hu, "A Cloud Security Assessment System Based on Classifying and Grading," in IEEE Cloud Computing, vol. 2, no. 2, pp. 58-67, Mar.-Apr. 2015.

[4] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok and I.Khalil, "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges," in IEEE Cloud Computing, vol. 2, no. 2, pp. 30-38, Mar.-Apr. 2015.

[5] V. Varadharajan and U. Tupakula, "Security as a Service Model for Cloud Environment," in IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 60-75, March 2014.

[6] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9.

[7] Y. Tang, P. P. C. Lee, J. C. S. Lui and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 903-916, Nov.-Dec. 2012.

[8] S. Xu, G. Yang, Y. Mu and R. H. Deng, "Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2101-2113, Aug. 2018.

[9] J. Aikat et al., "Rethinking Security in the Era of Cloud Computing," in IEEE Security & Privacy, vol. 15, no. 3, pp. 60-69, 2017.

[10] N. Paladi, C. Gehrmann and A. Michalas, "Providing User Security Guarantees in Public Infrastructure Clouds," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 405-419, 1 July-Sept. 2017.

[11] C. Esposito, A. Castiglione, B. Martini and K. R. Choo, "Cloud Manufacturing: Security, Privacy, and Forensic Concerns," in IEEE Cloud Computing, vol. 3, no. 4, pp. 16-22, July-Aug. 2016.

[12] B. Albelooshi, K. Salah, T. Martin and E. Damiani, "Experimental Proof: Data Remanence in Cloud VMs," 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, 2015, pp. 1017-1020.

[13] Tirumala, S. S., Sathu, H., & Naidu, V. (2015, December). Analysis and prevention of account hijacking based incidents in cloud environment. In 2015 international Conference on Information Technology (ICIT) (pp. 124-129). IEEE.