International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 8, August - 2013

Security Behind Each Layer Of Cloud Computing

Somayeh Sobatimoghadam

HakinSabzevari University, Sabzevar, Iran.

ABSTRACT

Cloud computing is a recent technology which has been replaced traditional IT systems. It has a waste rang of advantages so that it attracts significant attention during these decades. It offers a flexible, save cost and on demand computing. In addition to large number of benefits, the security aspects is steal a challenge. In this paper a new definition of cloud security in depth of each layer, is presented which separate the concept of security specifically in each layer and try to introduce a comprehensive solutions.

KEYWORDS:cloud computing, cloud security, privacy, availability, integrity.

1. Introduction

Nowadays cloud computing is a neo-aspect of Information Technology which attracts significant attention within the IT managers. Beside this absorbency of cloud among enterprises the security is an unresolved problem. At the moment, the leakage of worldwide accepted specification for security aspect is a big difficulty. In addition to a large number of benefits like scalability, flexibility, cost efficiency the security aspects like confidentiality, integrity and availability play an important role in attraction and reliance of cloud customers. Security is an important service which should be provided and guaranteed with
provider. A secure cloud is a reliable source for information. The most important task of a provider is protecting the cloud. It could be achieve in many different ways like availability, delivering high performance, using the IDSs to monitor the malicious activities, recovering in disasters, securing the authentication. The cloud providers must make sure their customers and clients that they never face such problems. Implementing a good encryption mechanism is unavoidable [1]. One of the most important aspect of cloud benefits is availability. The customer must be able to access their information regularly. The integrity of information is another privacy. It's not comfortable for customer to store their critical data in outside data center. In each services, cloud computing encounters with different security problem. In this direction there are some researches and disputes. There are numerous blog and white paper which attempt to talk about security concerns. Some of most important are: Cloud Security Alliance (CSA), InfoSec, Knights. They are trying to bring forward a standard way to define the security and discover the solution. Firstly, we define the cloud services: software as a service, Platform as a Service and Infrastructure as a Service. Then the cloud type will introduce. Finally, we represent a new methodology to define the cloud security.

2. Cloud Services

There are three cloud services models often referred to as "SPI model" which refers to Software, Platform and Infrastructure (as a service) respectively.

2.1 Software as a Service (SaaS)

A platform which is designed to provide rent out the software to the customer. It is usuallyprovided simply through only a web browser. This capabilityis provided ona cloud infrastructure by providers. For instance, a web based email client is a SaaS that user don't face with the problems like Storage, mail transfer, filtering because they are offer by provider.

2.2 Platform as a Service (PaaS)

The NIST describes PaaS as: "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. "The consumer wants to use a platform provided as a service to develop own software without concerning about underlying details [2].

2.3 Infrastructure as a Service (IaaS)

The customer buy the infrastructure and own the software and purchases virtual power to execute as needed. Infrastructure as a service provide the capability for consumer to manage processing, storage, networks and any computing resources. The consumer will be able to run and deploy their applications and software. The consumer could manage and control over his resources but he has no control on underlying Infrastructure. The provider allows the customer to control the system from the choice of operating system to any kind of applications, which is similar to create a virtual machine on physical resources.

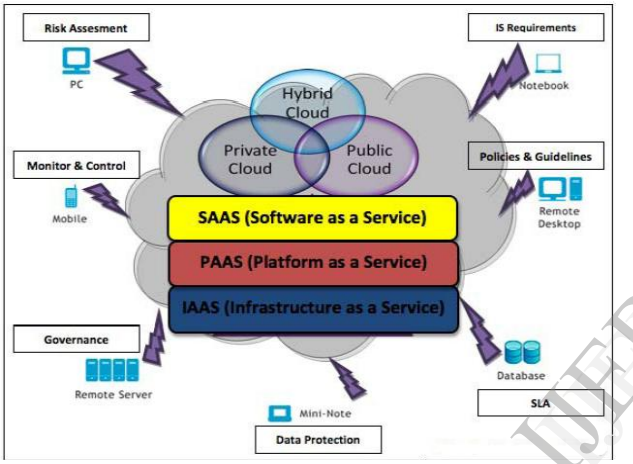

Figure 2. Cloud deployment model [1]

3. Cloud Types

The cloud computing model has four main deployment models: private, community, public, and hybrid [3].

3.1 Private cloud

This kind of cloud emulate cloud computing on privet networks. These clouds are internal to an organization and access from the outside is impossible. Unlike public clouds all resources are available and manage by the organization, like Intranet. For example, many organization have their own compute clouds to keep their sensitive data within the organization. The privet cloud seems to be more secure rather than the public cloud because it could be accessed internal [4].

3.2 Community

This kind of clouds are similar to private clouds but several organization use the cloud instead of a single organization. The joint together to manage their resources, which provide more compute power in Infrastructure.

3.3 Public

Clouds are those that are available in the public for anyone or any-organization. The consumer use the resources on the basis of pay-per-use or pay-per-usage model [5].The user of public cloud assured about all the resources which needs without any wastage. But the security of public clouds is steal a challenge [6].

3.4 Hybrid

Hybrid clouds are clouds that make use of a combination of othercloud types. The provider own its private cloud connect it with a public cloud. By outsourcing the resources which is an advantage of public clouds, the cost strongly reduced and the control over data highly maintained[7].

4. Security in depth of clouds

In traditional system where all resources were provided in own individual or corporative model, the security was handled by the IT engineers. In such systems, an attack could be identify easily and the insecure or offensive software could be diminished easily. In the cloud model, this problem is a bit more sophisticated. The security leakage could take place in each three layers (Iaas, PaaS and SaaS). The different layers in cloud cause different security concern which could make thisdifficult to define and trace in general way. Defining the security concept within each service, distinguish and classify the security issue thus providing the solution would be more efficient.

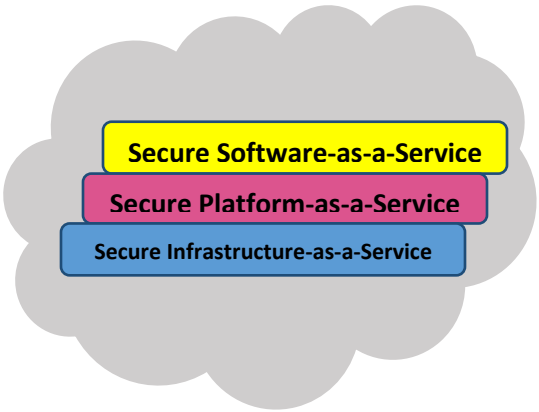

Figure 2. The security of cloud in depth of each layer

4.1 Secure Software-as-a-Service

In S-a-a-S it's customer who is responsible for his software security. Beside the security measures in Platform, the other security mechanisms should be intransitive. The provider is undertaking for infrastructure security, and it would be scant for comprehensive security. The use should use the encrypting to ensure the exhaustive security, especially for sensitive data. Using such secure mechanisms guarantee protection of your data versus internal and external threats. Internal threats like accessing by provider employee whose could discover provider's key generation routine or the key itself. Using own secure routine to use the public cloud storages, is a safe and provide a secure and assured manner. Despite the providers generally provide backup it is recommended that users make their own personal backups.

4.2 Secure Platform-as-a-Service

The shared nature of platform presents some particular challenges. There are two major aspects that influence the P-a-a-S security: The security of platform and security of the applications that users deployed[8]. The providers should provide the platform security which run the customer applications. Another most important side is availability. It could be provided by reliable software. Integrity and confidentiality could be provided by encryption. For instance, SSLencryption is one of the most common communication protocols which provide a safe encrypted communication on the internet. The customers have to keep in mind that anychanges in PaaS could adapt with security of the applications. The juridical aspect is latent aspect. The location of data storage brings legal challenges which could affected on data security. An international agreement about the cloud legal issues could be defined to untie the juridical problems.

4.3 Secure Infrastructure-as-a-Service

Generally, when the cloud security is proposed, all the attention are paid to the Infrastructure security, which is true. It's the provider who insure the customer about the security essentials. The provider decides when and how the data should be stored. The disclaimer of cloud provider is to provide the trust mechanisms to authenticate the intruder and unauthorized activities. Discovery in disasters is an important assumption. Cloud providers generally should provide surplus backups. Providing an automated failover system to relocate the data to another data center in disaster is a strong point for a provider. The availability could be achievable by customer, thus defense proceedings unto attacks should be forecasted and the protection measures are unavoidable.

There should be similar separations at the SaaS and IaaS levels. It is in the purview of the SaaS provider to decide how the data should be stored. For example, it is the decision of Gmail to store your emails on their servers as an encrypted byte stream or in plain text. This prevents unauthorized people from accessing the emails, but since the key used for encryption is in their possession, anyone with sufficient access can view the message. The customer of a SaaS provider is somewhat limited in security terms, but their obligations include using a secure web browser, a secure operating system, and ensuring the connection is done using SSL.On the otherend, an IaaS provider must ensure that their network and physical machine are secure while the customer is responsible for operating system, runtime, and application security. It then becomes the responsibility of the cloud customer to install an operating system (typically the IaaS provider also has some default options), configure the services and interactions, and secure anything the customer deems necessary.

5. Conclusion

Cloud computing is a new trend in organization because it offer a large number of benefits. In order to keep the cloud secure, it is important to have a clear definition of cloud security. In traditional look there is no separation in cloud security issues in it discusses in a general way whichcause the ambiguity for customers. Today, security is often listed as the number one concern forclients consideringcloudadoption. In this paper a new definition ofcloud security based on separated layer was presented which could help the IT managers to classify the cloud security concerns and provide the solutions.

References

[1] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." *Platform Computing*, 2010,pp. 6.

[2] "NIST Cloud Computing Reference Architecture", *Special Publication 500-292*, September, 2011,pp. 15—17.

[3] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing",*Special Publication 800-145*, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 2011,pp. 2-3.

[4]S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy.",*KM World,*2009,pp. 14-22.

[5]Salesforce, "*What is CRM?" Salesforce.com Winter'12 Release*, 2011.

[6] Wald, Hannah, "Cloud Computing for the Federal Community.", *IAnewsletter*, 13 (2), 2010,pp.10-15.

[7] EuropeanCommunities European Commission,"The future of cloud computing",*European Commission Information Society and Media*,2010.

[8]Mather T, Kumaraswamy S, Latif S ,"Cloud Security and Privacy", O'Reilly Media, Inc., 2009.

[9] "Cloud Security Alliance," retrieved November 14, 2011,

[10] Bernard Golden, "Cloud CIO: The Two Biggest Lies About Cloud Security" ,*CIO CXO Media*, 2011.

[11] Steve McDonald, "Legal and Quasi-Legal Issues in Cloud Computing Contracts," *EDUCAUSE and NACUBO Workshop on Cloud Computing and Shared Services*, 2010.

[12] Thomas Ristenpart, EranTromer, HovavShacham, and Stefan Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Part Compute Clouds," *ACM Conference on Computer and Communications Security,* 2009.