ISSN: 2454-4248
248 – 250

A Review of Security issues in Cloud Computing

Pradeep Laxkar
Assistant Professor , Computer Sc. & Engineering
ITM Universe
Vadodara, India
pradeep.laxkar@gmail.com

Abstract—Nowadays Cloud computing, as one of the focus point in IT world, it has drawn great attention. Many big IT companies like IBM, Google, Amazon, Microsoft, Yahoo develop cloud computing systems and related products to customers. However, there are still many difficulties for customers to adopt cloud computing, in which manly many security issues exist, because data of a customer is stored and processed in cloud, not in a local machine. This paper I will briefly introduces cloud computing and its key concepts. Specially, we aim to discuss security requirements and security issues in cloud computing. We will discuss security issues in data and virtualization in cloud computing.

Keywords—*Data, security , virtualization, cloud applications;*

*****

I. INTRODUCTION

According to US National Institute of Standards and Technology (NIST) [1] as follows:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models."

It proposes five main features of cloud computing:

• On-demand self-service: a consumer can automatically acquire computing resources such as CPU time, storage or software use, as needed without human interactions with providers of these resources.

• Broad network access: Computing resources are available over the network and accessed by various heterogeneous platforms (such as laptops, tablets and mobile phones).

• Resource pooling: "The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand" . In this sense, the customers do not have control or knowledge over the exact location of these resources.

• Rapid elasticity: For a consumer, computing resources are elastic: they are scaled up to use whenever needed and scaled down to release whenever finished. To the consumer, resources provisioning often appears to be infinite and can be appropriated in any quantity at any time[1].

• Measured Service: cloud system can use appropriate mechanisms to measure the usage of these resources for each individual consumer through its metering capabilities, such as monitoring, controlling, and reporting, which is transparent for both the provider and consumer.

US National Institute of Standards and Technology (NIST) [1] has classified cloud into two models service model and deployment model:

Service Models

There are three key cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These services can be used independently, but also work together.

• Software as a Service (SaaS): in SaaS, the cloud consumers deliveries their applications as a service over the net on a hosting environment, which can be accessed from various user clients. Users rent the software instead of buying it, which brings more choices and economical expense.

• Platform as a Service (PaaS): In PaaS, the consumer can create their cloud services and applications directly on a development environment or platform with tools offered by the platform provider. They then can run and deploy these applications with full control. This model makes companies do not consider about software management on servers.

• Infrastructure as a Service (IaaS): In IaaS, IT infrastructures, such as processing, storage, networks, and other fundamental computing resources, are delivered as a service to the consumer. In this sense,consumer can deploy and run arbitrary applications and operating systems. This model makes consumers only pay for what they use.

Deployment Models

Generally, there exist four cloud deployment models:

• **Private cloud:** The cloud infrastructure is provisioned for exclusive use within a single organization, managed and operated by the organization or a third party regardless whether it exists on or off premise.The owners can control the cloud infrastructure themselves.

• **Community cloud:** the cloud infrastructure is constructed and shared by several organizations based on similar requirements and interests, which may reduce utilization cost of every side.

• **Public cloud:** The cloud infrastructure is provisioned for public use by the general public cloud consumers. It's owned, operated and managed by the public cloud service provider. Public cloud owns weaker security than private cloud because of its open structure.

• **Hybrid cloud:** The cloud infrastructure is a typical combination of public and private clouds that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. In this sense, organizations can optimize their resources by moving peripheral business onto public cloud while controlling core business on private cloud, which enhances their core competencies.

II. CLOUD COMPUTING SECURITY ISSUES

A. Data Security and Privacy Protection Issues

Deyan Chen and Hong Zhao[2] described data security issues as follows:

(i). Confidentiality and integrity of data transmission need to ensure not only between enterprise storage and cloud storage

but also between different cloud storage services. In other words, confidentiality and integrity of the entire transfer process of data should be ensured.

(ii) Due to the multi-tenant feature of cloud computing models, the data being processed by cloud based applications is stored together with the data of other users. Unencrypted data in the process is a serious threat to data security.

Regarding the use of private data, situations are more complicated. The owners of private data need to focus on and ensure whether the use of personal information is consistent with the purposes of information collection and whether personal information is being shared with third parties, for example, cloud service providers.

(iii) Regarding sharing of private data, in addition to authorization of data, sharing granularity (all the data or partial data) and data transformation are also need to be concerned about. The sharing granularity depends on the sharing policy and the division granularity of content. The data transformation refers to[2] isolating sensitive information from the original data.This operation makes the data is not relevant with the data owners.

(iv) In the traditional IT environment, the main threat of the data availability comes from external attacks. In the cloud, however, in addition to external attacks, there are several other areas that will threat the data availability: (1) The availability of cloud computing services; (2) Whether the cloud providers would continue to operate in the future? (3) Whether the cloud storage services provide backup?

(V) When the data is no longer required, whether it has been completely destroyed? Due to the physical characteristics of storage medium, the data deleted may still exist and can be restored. This may result in inadvertently disclose of sensitive information.

B.Security Issues in Virtualization

Shengmei Luo,Zhaoji Lin,Xiaohua and Chen Zhuolin Yang, Jianyong Chen[3] described security vulnerabilities in virtualization, they identified threads in some general threats that are unique to the virtual environment

(i)Attack between VMs or between VMs and VMM

One of the primary benefits that virtualization brings is isolation. This benefit, if not carefully deployed will become a threat to the environment. Poor isolation or inappropriate access control policy will cause the inter-attack between VMs(virtual machine) or between VMs and VMM(virtual machine monitor).

(ii) VM escape

Virtual machine escape(VM escape) is an exploit in which the attacker runs code on a VM that allows an operating system running within it to break out and interact directly with the hypervisor. Such an exploit could give the attacker accessing to the host operating system and all other virtual machines (VMs) running on that host.

Virtual machines are allowed to share the resources of the host machine but still can provide isolation between VMs and between the VMs and the host. New software bugs were already found to compromise isolation. One such example of this kind of attack is VM escape.VM escape is one of the worst case happens if the isolation between the host and between the VMs is compromised. In the case of VM escape, the program running in a virtual machine is able to completely bypass the VMM layer, and get access to the host machine. Since the host machine is the root of security of a virtual system, the program which gain access to the host machine also gains the root privileges basically escapes from the virtual machine privileges.

III. CONCLUSION

Cloud computing causes great revolution in information technology industry. cloud computing has many issues, especially security issues mainly involving data and virtualization technologies. In this paper, I briefly introduced the overview of cloud computing, which included definition, service models and deployment models of it. In this paper I discussed the security issues related to cloud computing, including data security,and security issues in virtualization technologies. Data security is required to protect users' data from leakage, damage or loss.Cloud, virtualization technologies are also having many security threats.

Cloud computing is still in its development phase. As the development of cloud computing, there will be more and more new security issues need to be solved. The security issues of cloud computing will affect its effectiveness and reliability greatly. Thus, a intense study on that is required and a secure and reliable cloud computing platform will appear in the future.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of Cloud Computing,” National Institute of Standards and Technology (NIST),http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 2011.

[2] Chen, D., Zhao, H.: Data security and privacy protection issues in cloud computing. In: International Conference on Computer Science and Electronics Engineering, vol. 1, pp. 647–651. IEEE (2012).

[3] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," In Proceedings of the 2011 International Conference on Cloud and Service Computing. IEEE Computer Society Washington. DC. USA, pp. 174-179, 2011.

[4] G. J. Popek and R. P. Goldberg, “Formal requirements for virtualizable third generation architectures,” Comm. ACM, vol. 17, no. 7, pp. 412– 421,1974