Analysis of Security Issues in Cloud Computing

Kandarpa Kalita,
Department of IT, Assam Down Town University
Nilim Jyoti Gogoi
Department of CS and Elec., USTM

Abstract

Cloud computing is new edge computing based on internet. In cloud computing shared servers provides software, infrastructure, and platform using their different deployment model such as *PaaS, IaaS and SaaS* to the target customers on pay-per-use basis. The advantages of cloud computing include scalability, flexibility, resilience, efficiency and outsourcing of non-core activities. Despite the potential gains achieved from the cloud computing, the organizations are reluctant to invest in cloud services mainly due to security issues and challenges associated with it. This paper presents various security issues and challenges affecting in cloud deployment.

Keywords: Cloud computing, Deployment model, security issue, scalability, virtual machine, cloud API.

Introduction

Cloud Computing is a service through which one can avail shared computing resources (e.g., infrastructures, applications, and services) with minimal management effort and service provider interaction. Cloud computing is a way to increase the capacity or capabilities of an organization without investing in new infrastructure, training of the operational personals, or licensing to the new software's [1]. Therefore many organization is found to be adapting to the cloud computing. Even though migrating to the cloud remains a likable trend from a financial perspective, there are many other aspects that must be taken into account by organizations before they decide to do so. One of the most important aspects refers is the security. Security is found to be one of the most important key considerations for the cloud computing scenario [2]. This viewpoint is shared by many distinct groups, including researchers [3], business decision makers [4] and government bodies [5 - 6].

Cloud Deployment (Spi) Models

The services from the cloud can be provided using three services models [7-8]:

Software-as-a-Service (*SaaS*): It is a software distribution model in which applications are hosted by a cloud provider or any third party vendor and made available to target customers over the Internet. By the use of any thin client interfaces (e.g. Web browsers) the application can be accessed using various computing devices.

Platform-as-a-Services (*PaaS*): *PaaS* is a model for providing platform layer resources such as operating systems, software developing frameworks and other associated services over the Internet to the end users for their use without downloads or installation.

Infrastructure-as-a-Service (*IaaS*): Using this paradigm the consumer are provide with different operational hardware such as processing components,

storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software.

Before analyzing security issues in Cloud Computing, we have to understand the relationships and dependencies between all these cloud deployment models [9]. Before analyzing security issues in Cloud Computing, we have to understand the relationships and dependencies between all these three cloud deployment models. *SaaS* as well as the *PaaS* Model are hosted on the top of the *IaaS* model. Any issue in *IaaS* will impact on the security of *PaaS* or *SaaS* or Both the services, true on the other way also. As *PaaS* provides the platform to build and deploy *SaaS* applications, it increases the security dependency between them. As a result of these dependencies, any attack to any cloud service model can affect the upper layers. These dependencies between the cloud deployment models may also be the source of security risks. In a wide scenario a *SaaS* provider may lease a development framework from a *PaaS* provider, which may also lease an infrastructure from an *IaaS* provider. Each provider is equally responsible for securing their own services, which may result in inconsistency in security models. It also creates perplexity over which service provider is responsible if an attack happens.

1. Software-As-A-Service Security Issues:

Among all the three fundamental delivery model providers has the least control over security for *SaaS*. As common application can be accessed by many users simultaneously it is the responsibility of the cloud provider to ensure security so that no user can see each other private data. Some of the common security challenges in *SaaS* layer are as follows:

1.1. Application security: On demand applications in cloud environment are typically delivered through the Internet using Web browser. Attackers have been using the web to access user computers and perform malicious activities such as stealing of sensitive data. *SaaS* attacks are somehow similar with the traditional web attack but traditional solutions are not effective in securing the *SaaS* from attackers [10].

1.2. Data security: Data security is one of the major concern in web based services. In *SaaS* as data is processed and stored in the cloud services provider's data center, it is the responsibilities of the cloud provider to provide security from the data being stolen when it is processed or stored. On the other hand data backup is also equally important for the recovery of the data in case of disaster [10].

1.3. Multi-tenancy: *SaaS* applications can be grouped into maturity models for the deployment, the most common one is the multi-tenancy [13]. Using this model one single instance can be served to many users. With this approach the resources efficiency is increased but scalability is limited. This approach enables more efficient use of the resources but scalability is limited. Since data from multiple tenants is stored in a shared database, it increases the risk of data leakage between these tenants. It is the responsibilities of the cloud provider to set security policies to ensure that data from one user are kept separate from other [14].

2. Platform-As-A-Service (*Paas*) Security Issues:

As compared with *SaaS* and *IaaS*, *PaaS* depends on secure and reliable network connections also a secured web browser. *PaaS* application security comprises of two software layers: security of the *PaaS* platform (i.e., runtime engine), and Security of customer applications deployed on a *PaaS* platform

[15]. *PaaS* providers are responsible for securing the runtime engine that runs the customer applications. Following are some of major security concern in *PaaS* layer.

2.1. Third-party relationships: PaaS provide traditional programming language, Programming framework also third party web components such as mushup. Mashup merge up more than one source components into one single integrated unit. Therefore, *PaaS* model inherit security issues related to mashup [16].Thus, the *PaaS* users have to depend on both the security issue of web development tools and third-party services.

2.2. Development life cycle: From the perception of the application development, developers are facing the complexity of building applications that can be hosted securely from the cloud. The pace at which applications are change in the cloud will affect the System Development Life Cycle (SDLC) as well as the security [17]. Developers also have to understand that any changes in PaaS components can negotiate the security of their applications. Apart from secure development techniques, developers should have known about legal issues regarding data. So that data is not to be stored in inappropriate locations. If so it can compromise privacy and security.

2.3. Underlying infrastructure security: SaaS provide user with the application, PaaS provides the development environment and the tools. In PaaS usually the developers have only a little access or have no access to the underlying infrastructure, so providers are responsible for securing it as well as the applications. The user of the PaaS (developers) does not have the full assurance over the tools provided by the cloud provider that it is secured. Therefore for both SaaS and PaaS security is the responsibility of the provider.

3. Infrastructure-As-A-Service (*Iaas*) Security Issues:

Using IaaS a large set of computing devices as well as networking devices are provided to the end user. Users are allowed to run any software with full control the resources allocated to them [18]. Unlike the other two model IaaS user has better control over security. The user controls the software of their own running in their virtual machines, and they can set their own security policies correctly. Still, this is the responsibilities of the provider to control the underlying infrastructure. IaaS providers must undertake a significant effort to secure the resources from security threat. Some of the security issues associated to IaaS is as follows:

3.1. Virtual Machine Security: Virtualization is the backbone of a cloud. A virtual machine (VM) is an independent software instance that represents a full copy of an operating system or application software. Each instance can be shared the hosting server's computing resources. For fault tolerance, load balancing or maintenance virtual machines can be migrated between physical servers hence dramatically increases the physical server hardware usage. Any instance can be cloned and faultlessly moved between physical servers. This dynamic nature of VMs increases the measures for security. When it moved from one machine to another flaws such as vulnerabilities or configuration errors may pass from one to another. It is also difficult to keep auditable record of the security state of a virtual machine at any given point in time.

The Virtual Machine Monitor (VMM) or hypervisor is low-level software that is responsible for virtual machines isolation; any compromisation with the VMM regarding security leads to the compromised with the VMs. If the VMMs are not root secure or complex it increases the risk of security vulnerabilities, as it is more tedious to find and fix any vulnerability [18].

3.2. Issue regarding shared resource: VMs are located on the same server can share CPU, memory, I/O, and other hardware. Sharing of resources between VMs may decrease the security of each VM. A malicious VM can attack and infer some information about other VMs through shared memory without the need of compromising the VMM. Two VMs can communicate bypassing all the rules defined by the security module of the VMM using covert channels. Thus the attacker can infer information about other virtual machines.

3.3 Insecure API: Application programming Interface (in short API) defines how a third party connects to a service. Problem with the cloud APIs are that they are frequently updated. Therefore fixing a bug can introduce another security issue in the API. Also improper authentication posses threat to the cloud server, which lead to the interception of the attacker in the data exchanges between two parties (client and server).

Conclusion And Future Scope

Cloud computing is a new edge computing based on internet. Computing tools such as infrastructure, platform and software can be deployed to the end user with a minimal fee for rent on pay-per-use basis. Like any other internet based services cloud services is also suffered from security threat. In this paper some of the major security challenges are discussed. In future it can be used for studying new security threat as well as building framework for securing the cloud.

References

1. Kuyoro, S. O., Ibikunle, F., & Awodele, O., (2011). Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), vol.3, no. 5, pp. 247-255.

2. Gens, F., (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, [online] Available: <http:// blogs.idc. com/ie/? p =730> [Feb. 18, 2010].

3. Rimal, B.P., Choi, E., Lumb, I., (2009). A Taxonomy and, Survey of Cloud Computing Systems. Fifth International Joint Conference on INC, IMS and IDC, NCM '09, CPS., pp. 44–51

4. Shankland, S., (2009). HP's Hurd dings cloud computing, IBM. CNET News

5. Catteddu, D., & Hogben, G., (2009). Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, enisa.europa.eu /act/rm/files/ deliverables/ cloud-computing-risk-assessment

6. CSA (2009) Security Guidance for Critical Areas of Focus in Cloud Computing. Tech. rep., Cloud Security Alliance

7. Subashini, S., & Kavitha, V., (2011). A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl4(1), pp. 1–11

8. [Online] Available : http://searchcloudcomputing.techtarget.com/definition/SPI-model

9. Rosado, D.G., Gómez, R., Mellado, D., & Fernández-Medina, E., (2012). Security analysis in the migration to cloud environments. Future Internet, vol. 4, no.2, pp. 469–487

10. Grobauer, B., Walloschek, T., & Stocker, E., (2011). Understanding Cloud Computing vulnerabilities. IEEE Security Privacy, vol. 9, no. 2, pp.50–57

11. Ju, J., Wang, Y., Fu, J., Wu, J., & Lin, Z., (2010). Research on Key Technology in SaaS. In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp. 384–387.

12. Bezemer , C. P., & Zaidman, A., (2010). Multi-tenant SaaS applications: maintenance dream or nightmare? In: Proceedings of the Joint ERCIM

13. Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium.ACM New York,NY, USA, pp 88–92

14. Mather, T., Kumaraswamy, S., & Latif, S., (2009). Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA

15. Xu, K., Zhang, X., Song, M., & Song, J., (2009). Mobile Mashup: Architecture, Challenges and Suggestions. In: International Conference on Management and Service Science. MASS'09. IEEE Computer Society, Washington, DC, USA, pp. 1–4

16. Morsy, M. A., Grundy, J., & Müller, I., (2010). An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC Cloud Workshop. APSEC,Sydney, Australia

17. Dahbur, K., Mohammad, B., & Tarakji, A.B., (2011). A survey of risks, threats and vulnerabilities in Cloud Computing. In: Proceedings of the International conference on intelligent semantic Web-services and applications. Amman, Jordan, pp 1–6

18. Ranjith, P., Chandran,P., S. Kaleeswaran, On covert channels between virtual machines. Journal in Computer Virology Springer vol. 8, 2012, pp. 85–97