Volume 8, No. 5, May-June 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Cloud Computing and Cloud Related Security Issues

Anand
Assistant Professor
Department of Computer Science
Keshav Mahavidyalaya
University of Delhi, India

Abstract:This paper presents a discussion on the basic architecture of the cloud computing and the related threats and vulnerabilities about the security of the cloud computing systems. The discussion is broad based which classifies the various threats and suggests some ways of controlling them in the interest of the cloud service providers (CSP) and the users of the applications which are provided by the CSPs. It is discussed that the underlying infrastructure of the cloud is vulnerable to various kinds of attacks (internal and external) and there is a need for understanding the variety of security issues that are emerging in the current scenario considering that the cloud computing is increasing its reach in the social and business fields.

Keywords:Cloud computing, SaaS, PaaS, IaaS, Security Threats, API.

INTRODUCTION

The *cloud computing* is a distributed architecture that enables a convenient and on-demand access to networked storage space and computer resources. Such a shared pool of computing resources includes networks, servers, applications and services. Cloud computing is definitely a revolution and a paradigm shift in the current computing technologies and framework[1]. The distributed architecture centralizes the resources on a platform which can be released on demand with minimal management effort or service provider interaction [6]. The cloud computing refers to applications which are delivered as services over the internet and it also includes hardware and software delivered through the datacenters. The cloud service providers (CSP) offer cloud platforms which are used by the customers to create various web services, such as email services (for example Gmail)[2].

The advantages of cloud services for the customers include lowering the costs for managing huge resources, as now the companies need not manage the resources which are managed by the CSPs such as Google, Amazon, Microsoft etc. Moreover, the computer resources may be used on demand basis such as on pay- per-use basis by the customers. The cloud computing is an internet based technology and the customers are provided services such as processing power (virtual machine), bandwidth, data storage (virtual space), data transmission & transactions etc. Due to the efficiency of the services provided by the large scale datacenters (which lowers their cost of operation thus making them economically efficient) are making many industries such as banking, insurance, healthcare, education to adopt and use cloud computing services. However, there are many risks which have emerged due to centralized and limited control over the large amount of data. The security threats include data leakage risks, insecurity in interface, risks in sharing of resources and inside and external attacks on stored data. In this paper we will understand the basics, architecture and service models of cloud computing and examine the risks, vulnerabilities and security threats for cloud computing in the recent times.

CLOUD ARCHITECTURE

Although cloud computing is an increasingly discussed area yet itsarchitecture basics are essential to understand the related security concerns. Hence in this section we will discuss the basic building blocks of cloud. The cloud computing is based on decoupling of resources away from the physical location of the infrastructure which delivers them. There is an abstract evolution of this technology from the point of view of the cloud architecture, while it is based on many previous models such as grip computing yet it has evolved encompassing many differences from the previous models. There are many operational, technological and organizational advancements within cloud architecture defining its attributes. The models for describing the cloud architecture below are based on network deployment and service delivery.

A. *Principle Characteristics:* The cloud services are based on five principle characteristics that is;**a**. infrastructural abstractions- the physical resources, computational, network and storage resources through which the data is processed, transmitted and stored is abstract and opaque from the application and service delivery;**b**. resource democratization-through the abstraction of the resources whether information, applications or infrastructure makes the pooled resources available to anyone thus it yields the notion of democratization of resources; **c**. service oriented architecture- provides that the democratized and pooled resources can be accessed and utilized in standard ways thus focusing on the delivery of the services; **d**. elasticity- based on the high speed connectivity, pooled resources, automation and virtualization the capacity to expand and resource allocation can be scaled to as-needed levels; and **e**. utility model for consumption- by governing input parameters the utility, allocation and consumption of resources can be metered thus leading to cost efficacies and management.

B. *Cloud Services Delivery Models [3][4][5]:* The three archetype models are usually referred as SPI model- referring to software, platform, and infrastructure each as a service.

- *Software as a service (SaaS):* It refers to the service provided to the customers to use the applications provided on a cloud infrastructure and it is made available through client interface (such as web browser).It is service on-demand provided to the customer. The benefits to the customers include- no need to invest in servers, computer infrastructure and licenses of the software hence lowering their costs. They also do not need to manage the underlying layer of cloud servers, networks, storage of data, operating systems and applications (except the user specific applications). This reduces the storage of application on their own computer, operating management, reduces load of software maintenance, safeguarding and support. The responsibility of deploying and managing IT infrastructure, processes are managed by SaaS vendors such as Amazon, salesforce and Google.
- *Platform as a Service (PaaS):* It refers to the delivery of a computing platform as a service to the customers and users without any need to install software on own systems. The infrastructure is provided with a high level integration for implementing the various cloud applications. In this, a layer of software is provided as a service over which higher level of services (applications) are built. The users can configure their own applications which can run over the provider's platform. They also have the control over the deployed applications. PaaS providers such as Google App Engine, Force.com and Microsoft Azure can provide a predefined combination of OS and application servers.
- *Infrastructure as a Service (IaaS):* It refers to the sharing of hardware and providing storage and computational capabilities over the network. It allows for making accessible the resources such as servers, networks, storage space for the applications and OS. The basic infrastructure for on-demand services is offered using the Application Programming Interface (API). The API is used for interaction with hosts, switches and routers. The customers are given the capability to rent processing, storage, networks and fundamental computing resources, and they can deploy arbitrary software. The service provider owns the equipment and controls its management and operation while the customer controls the OS, storage and can deploy the applications. Amazon EC2, GoGrid and 3 Tera are some of the examples of IaaS.

C. *Cloud Deployment and Consumption Models:*There are four ways in which the cloud services are deployed, as described below.

- *Private Cloud:* They are owned, leased and managed by an organization and offers a single-tenant operating environment. They offer greater data security and high control. The on-premise private clouds are hosted within own data-center and provides standardized protection and operating processes. However, they may have limited size and scale. The other type can be off-premise or the externally hosted private clouds from external data centers. The user access and the network usage is restricted leading to high security. An example is Eucalyptus systems.
- *Public Cloud:*It refers to a cloud infrastructure that is provided to many customers and it is managed by a third party. At a time, multiple companies can work on the provided infrastructure. The users can therefore provision the resources dynamically. The cloud provider is fully responsible for installation, provisioning, maintenance and overall management of the cloud services. The customers are charged on the basis of pay-for-use. The access restrictions and authorizations techniques are not used in public clouds. The CSPs such as Google and Amazon provide access control to their users.
- *Hybrid Cloud:*It refers to a combination of two or more cloud deployment models. They are linked in such a way that allows the transfer of data between them without affecting any of them. They are provided by the organization but the management of this cloud is shared by the organization and cloud service provider. The company or the organization can define the goals and need of the cloud services. A combination of public or private clouds may make the implementation complicated. The data portability can also be provided if the clouds are linked to proprietary and standard technology. The Amazon Web Services (AWS) are an example of hybrid cloud.
- *Community Cloud:* It refers to the shared infrastructure between several organizations. This may be managed by a third-party service provider or the organizations themselves. These are based on agreements between the similar or related organizations for their common goals. The cloud may be operated locally or remotely. Facebook is an example of community cloud.

CLOUD RELATED SECURITY ISSUES

The security concerns for cloud services are challenging because cloud computing comprises of multiple technologies such as networks, databases, OS, virtualization, load balancing transaction management, resource scheduling concurrency control and memory management. The various security concerns can be, securely mapping the virtual machines to physical; encrypting the data for data sharing and security; securing algorithms for resource allocation and memory management; and using data mining techniques for malware detection [7]. The sections ahead discuss various risks, threats and vulnerabilities which may seem to be interrelated and refer to similar security concerns for cloud but they offer different issues and security problems.

I. *Vulnerabilities:* It refers to the weaknesses of the hardware, software and processes which may allow the attackers to access the resources within the cloud environment. It provides an open door to enter the computer, network by exploiting the weak or absent security measure in the cloud system. The vulnerabilities meeting the following criteria is considered specific to cloud.
   - It is intrinsic to the core technology of cloud computing such as virtualization.
   - Its root cause is an essential cloud characteristic such as resource pooling.
   - When clouds use innovative techniques beyond the

tested security methods.
- It may be existing in the established cloud technology.

II. *Threats:* It refers to any potential danger to the system in which one can identify the vulnerability and sets it to exploit the system and damage the resources. Based on the paper of CSA the threats and their description is provided below.

Table1: A tabular depiction of the threats in cloud computing

Threats	**Description**	**Examples**	**Control Suggestions**
Abuse and frauds	The spammers, malicious coders, and other fraud developers may abuse the anonymity and opaqueness of the services provided by the clouds. IaaS and PaaS suffer these attacks. Precisely because the cloud providers offer illusion of unlimited network and storage. Includes password key cracking, Distributed DoS, CPATCHA solving farm, Rainbow table making, Botnet command and control.	Zeus botnet and Infostealertrojan and Spams	Making the registration and validation strict. Monitoring public blacklists. Introspecting customer traffic network.
Insecure API and Interface	Provisioning, management, orchestration and monitoring are managed by using the APIs and interfaces, which are used by the customers to interact with cloud. Security of the cloud services can be attacked by malicious attempts to damage these APIs/ interfaces.	Reusable tokens, password, improper authorization and access, clear-text authentication, unknown service or API dependency.	Ensuring strong authentication and access control. Encrypted transmission of data. Securing the dependency chain of APIs. Strengthening the security model of cloud provider.
Malicious Insider attacks	IT services and customers of a single management are prone to high risk if there are any malicious insiders.	Disclosed examples are unknown.	Ensuring security in overall security of information management. Examining the security breach if any.
Issues of Shared Technology	The cloud services are provided by sharing the infrastructures. The hypervisors mediate the access between guest OS and the physical underlying infrastructure through virtualization. This may create flaws, such as the guest OS may obtain unauthorized controls and may influence the underlying cloud compute resources. Thus the threat of putting data at risk for multiple-tenants.	Joanna Rutkowska's Blue and Red Pill exploit.	Ensuring strong authentication and access control. Vulnerability scanning should be performed. Performing configuration audit. Enforce SLAs and patching and vulnerability remediation.
Data Leakage and Data Loss	Compromising the integrity and confidentiality of data. Such as deletion of data, theft of data, alterations in original data, unlinking the records of data thus making the recovery difficult in future.	Insufficient authorization, authentication and access control (AAA). Operation failures	Data encryption in transmission. Strong control for API access. Using strong keys for storage and management Design and runtime data protection. Better provider level backup.

Hijacking of Service/ Account	Hijackers access the confidential information such as passwords, and other credentials such as biometrics. They can use it for eavesdrop on the activities and transactions of the customers and end users. They can manipulate the data, return wrong information, misuse the obtained information such as bank frauds, redirection to other websites.	Bank frauds using the credentials of the users.	Prohibit the sharing od credential and confidential information such as passwords between the users and service providers. Monitoring the unauthorized activities.

III. *Risks Areas:*Based on the above discussed vulnerabilities and threats in cloud computing environment (equipment and software) we can say that there are six major'risk' areas which need security attention. These are- **a**. security of data (at rest); **b**. data in transit; **c**. authentication for users, applications and processes; **d**. need for robust separation of data (which belong to different customers); **e**. legal and regulation issues related to cloud computing; **f**. incident response to cloud.

CONCLUSION

In this paper we first discussed the cloud computing and its basic architecture, then we presented a discussion on the vulnerabilities and threats to the security of cloud based services. It is considerable that the cloud services have adopted limited standardization and proprietary uses are limited to the individual service providers. Hence the security concerns are multilayered and multiple. It is important for the CSPs to assure that tight security provisions are in place for ensuring and safeguarding the client's interests. Maximum focus is needed for protecting the cloud services from various internal and external attacks which compromise the data security of the users who have no or minimum access to the underlying infrastructure and cloud compute resources. The users should have strictly controlled access and authorization for the illusion of the unlimited services [1] may bring opaqueness that is exploited by the attackers. Correct configuration of VMs and Hypervisors is needed along with defined access parameters and strong identity and access configurations in the cloud systems. The traditional security threats, threats on data availability of the service providers, customer IT services and the third party control are the various levels at which the security concerns can be implemented, designed and managed in the cloud computing services.

REFERENCES

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinsky, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. 2009. Above the Clouds: A Berkley View of Cloud Computing. Technical Report No. UCB/ EECS-2009-28. Department of Electrical Engineering and Computer Sciences, UC at Berkley. Accessed from: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
2. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. 2011. Draft Cloud Computing Synopsis and recommendations. NIST. Special Publication 800-146. US Department of Commerce. May 2011. Accessed from http://csrc.nist.gov/publications/drafts/800-146/drafts-NIST-SP800-146.pdf (Accessed on 12 May 2017)
3. Jianfeng, Y. and Zhibin, C. 2009. Cloud computing Research and Security Issues. Professional Communication conference. IECC. IEEE International.
4. Kresimir, P. and Zeljko, H. May 24-28 2010. Cloud Computing security issues and Challenges. MIPRO 2010 Proceedings of 33 International Convention, IEEE, Croatia.
5. Meiko, J.J., Nils, G., and Luigi, L.I. 2009. On technical security Issues in Cloud Computing. IEEE Conference on Cloud Computing.
6. Mell, P. and Grance, T. 2011. The NIST definition of cloud computing. NIST special publication 800-145. Computer security division. NIST. Doi: http://dx.doi.org/10.6028/NIST.SP.800-145
7. Sen, J. and Sengupta, I. 2005. Autonomous Agent-Based Distributed Fault-Tolerant Intrusion Detection System. In Proceedings of the 2nd International Conference on Distributed Computing and Internet Technology, pp. 125-131, December, 2005, Bhubaneswar, India. Springer, LNCS, Vol. 3186.