International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Security Issues and Risks in Cloud Computing

Garima Singh[1], Apoorv Vikram Singh[2]

[1]Gautam Buddha University, Department of Computer Science and Engineering, Greater Noida, Uttar Pradesh

[2]Department of Computer Science and Engineering Motilal Nehru National Institute of Technology, Allahabad, Uttar Pradesh

Abstract: ***Cloud computing is a way of arranging a pool of resources to increase efficiency and reduce the infrastructural as well as maintenance costs to provide faster access to the users of that pool. Due to this reason it is today's most promising and commonly used technology. According to recent surveys the top reasons for moving to a cloud is basically because three main factors: security, performance, reduced costs. Thus organisations are looking for factors that add "security" to their business at the same time reducing the cost of its implementation along with making resources available whenever required.***

Keywords: Cloud Computing IAAS, PAAS, SAAS, VM, Vulnerabilities

1. Introduction

Since the concept of cloud computing originated, it has been the most promising technology as well as the rapidly growing technology in the IT industry. Now even the companies hit by the recession have realised that by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. Cloud computing is concerned with activities such as the use of social networking sites and other forms of interpersonal computing; accessing online software applications, data storage and processing power. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. This is mainly because of the security issues faced by people by investing in cloud computing. In this paper we are going to talk about such security risks and issues.

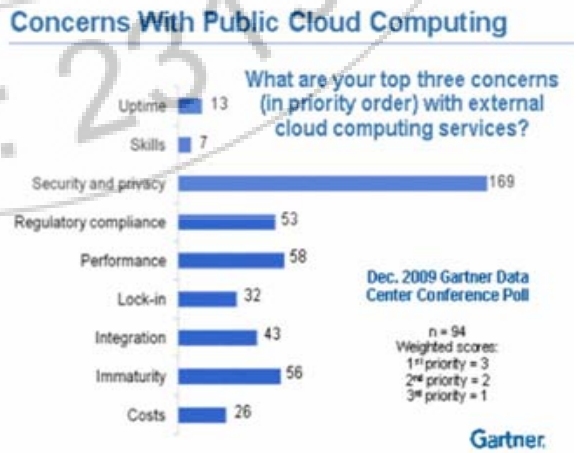
Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while their software and data are stored on the servers [1]. In some respects, Cloud Computing represents the maturing of these technologies and is a marketing term to represent that maturity and the services they provide [2].

Cloud Computing model provides three types of services namely-

1) **SaaS:** Software-as-a-Service provides complete applications to a cloud's end user. It is mainly accessed through a web portal and service oriented architectures based on web service technologies. Credit card or bank account details must be provided to enable the fees for the use of the services to be billed.
2) **PaaS:** Performance-as-a-Service comprises the environment for developing and provisioning cloud applications. The principal users of this layer are developers seeking to develop and run a cloud application for a particular platform. They are supported by the platform operators with an open or proprietary language, a set of essential basic services to facilitate communication, monitoring, or service billing, and various other components.
3) **IaaS:** The services on the infrastructure layer are used to access essential IT resources that are combined under the heading Infrastructure-as-a-Service. These essential IT resources include services linked to computing resources, data storage resources, and the communications channel. They enable existing applications to be provisioned on cloud resources and new services implemented on the higher layers.

Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters [3]. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [4]. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing [5].

1.1 Main Concerns related with Cloud Computing



Source: Dec'09 Gartner Data Center Conference Poll

From the above figure, it is clear that the main goal of any cloud service provider is to secure its cloud network. However, data security has also improved due to data centralisation but the main focus it to protect the most sensitive data present in the cloud such that customers do not face any trouble.

2. Main Security Issues

• Cloud computing definitely makes sense if your own security is weak, missing features, or below average.

- Ultimately, if
  - o the cloud provider's security people are "better" than yours the web-services interfaces don't introduce too many new vulnerabilities, and
  - o the cloud provider aims at least as high as you do, at security goals, then cloud computing has better security.[6]

2.1 Factors

2.1.1 Loss of control

- here the provider is the administrator of resources and data
- cloud handles the user identity
- rules and services are enforced by the cloud provider

2.1.2 Lack of trust

- Risk is taken as a third party is getting involved.

2.1.3 Multi ownership

- Multi ownership means multi tenancy. Multiple tenants share the pool of resources with different and conflicting rules.
- Conflict of interest

2.2 Cloud computing models

Cloud Computing can be deployed by agencies depending on various factors such as where the cloud services are hosted, the security requirements, sharing of cloud resources and the ability to manage some or all the services. Therefore 4 deployment models are distinguished by the National Institute of Standards and Technology.

2.2.1 Private Cloud

This type of cloud model is operated for a single organisation. This allows private clouds to enforce their own security and controls. The cloud's capacity is paid by the agency itself. No unaffiliated agencies can use the resources of cloud. An agency will typically host a private cloud on-premise, connect to it through private network links, and only share its resources within the agency.

2.2.2 Public Cloud

A third party cloud service provider owns this and the cloud is available to the general public. In a public cloud, an agency dynamically provisions computing resources over the Internet from a CSP who shares its resources with other organizations.

This can be the most cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability.

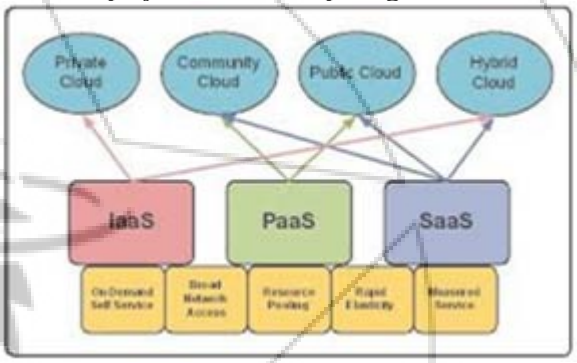
2.2.3 Community Cloud

Multiple organisations share the cloud infrastructure with the same cloud rules and services. The cost is thus reduced compared to private cloud. The organisations sharing the cloud usually have the same requirements.

2.2.4 Hybrid Cloud

It is a combination of two or more clouds (public or private or community). Agencies will likely not limit themselves to one cloud deployment but will rather incorporate different and overlapping cloud services to meet their unique requirements. Hybrid deployment models are complex and require careful planning to execute and manage especially when communication between two different cloud deployments is necessary.

Cloud Deployment and Computing Models



Source: http://blog.thehigheredcio.com/2011/02/22/cloud-
A third party cloud service provider owns this and the cloud is available to the deployment-models/

2.3 Vulnerabilities and Threats in cloud computing

In order to protect the users of cloud and help them adopt the correct cloud, the threats and vulnerabilities in cloud computing must be described. Thus there should be several significant threats considered before adopting the paradigm of cloud computing, these threats are:

2.3.1 Resource allocation

Unlimited resources are allocated.

2.3.2 Vulnerabilities related to data

a) Data can be merged with the data of unknown owners (can be competitors, or intruders).
b) Data may be located in different places which have different laws
c) Data can't be completely deleted and third party creates the backup.
d) Data is often stored, processed, and transferred in clear plain text

2.3.3 Vulnerabilities in Virtual Machines

a) Allocation and Deallocation of resources with VMs are unrestricted.
b) VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware

maintenance

c) Data leakage as VMs can be copied in order to provide flexibility.
d) Attackers can map where the target VM is located within the cloud by knowing the IP addresses.

2.3.4 Hijacking of Account

By account theft or social engineering an account theft can be performed. An attacker can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction.

2.3.5 Leakage of data

Occurs when the data gets into the wrong hands while it is being transferred, stored, Audited or processes. [8, 10]

2.3.6 Denial of Service

System cannot satisfy any request from other legitimate users due to resources being unavailable. This case may arise when malicious user has taken over all the resources.

2.3.7 Malicious VM Creation

An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository.[7]

2.3.8 Insecure VM Migration

Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions [9]:

a) Access data illegally during migration
b) Transfer a VM to an untrusted host
c) Create and migrate several VM causing disruptions or DoS

2.3.9 Data Scavenging

Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data

2.3.10 Virtual Machine Monitor Vulnerabilities

Flexible configuration of VMs or hypervisors (virtual machine monitors) to meet organization needs can be exploited

2.3.11 Sniffing VM

A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [11].

2.3.12 VM Hopping

It happens when a VM is able to gain access to another VM (i.e. by exploting some hypervisor vulnerability) [12]

2.3.13 Vulnerabilities in Virtual Networks

Sharing of virtual bridges by several virtual machines [13]

Conclusion

The concept of cloud computing is new and is the rapidly growing technology. It has many benefits along with some security risks. There are still some comments made on its possible implementations for large size organisation. In this paper we have discussed about various security issues (IAAS, PAAS and SAAS) and risks on cloud models. Not just cloud computing but also various virtualisation technologies are the target by hackers and various other threats for disfunctioning of the system. By taking proper counter measures and risk management techniques we can combat the issue and threats related with cloud computing.

References

[1] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin.
[2] Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf
[3] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/ whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291
[4] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469-487
[5] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. Sebastopol, CA: O'Reilly Media, Inc..
[6] From John McDermott, ACSAC 09.
[7] An analysis of security issues for cloud computing by Keiko Hashizume1*, David G Rosado2, Eduardo Fernández-Medina2 and Eduardo B Fernandez1, Hashizume et al. Journal of Internet Services and Applications 2013.
[8] Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA.ACM New York, NY,USA, pp 199-212.
[9] Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer 8:85–97
[10] Zhang Y, Juels A, Reiter MK, Ristenpart T (2012) Cross-VM side channels and their use to extract private keys. In: Proceedings of the 2012 ACM Conference on Computer and communications security, New York, NY, USA. ACM New York, NY, USA, 305–316
[11] Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007
[12] Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35-41
[13] Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing. In:

5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, pp 18–21

Author Profile

Garima Singh is presently enrolled in the 4th yearof her Integrated M.Tech programme (2011-2016) in Computer Science Engineering from Gautam Buddha University. She has already written papers in 3rd year but this one is her first to be published. She has interests in web development and has developed a website for her college fest. Besides this she loves to read novels, painting and listening to music.

Apoorv Vikram Singh is currently enrolled in 4th year of his B.Tech programme (2011-2015) from Motilal Nehru National Institute of Technology (MNNIT). He is an ace programmer and has developed many android applications. In 2013, he received the title of "Mr. Avishkar" in the Technical Festival organised by his college. Besides programming, he has interests in playing football and listening to music.