

# Threats and Security Issues in Cloud Computing

**Dr. Gurpreet Singh**

G.T.B Khalsa College of Information Technology, Chhapianwali Malout

[gurpreetkhat0r@gmail.com](mailto:gurpreetkhat0r@gmail.com)

## Abstract

In this paper, we have tried to categorize the key concerns and discuss the related technical implications and research issues, including some advanced security issues specific to cloud. We have also discussed some issues regarding security-related regulatory compliance in cloud. In this paper, we take a holistic view of cloud computing security - spanning across the possible issues and vulnerabilities connected with virtualization infrastructure; software platform; identity management and access control; data integrity; confidentiality and privacy; physical and process security aspects; and legal compliance in cloud. We present our findings from the points of view of a cloud service provider, cloud consumer, and third-party authorities such as Govt.

**Keywords:** Virtualization, SAAS, PAAS, cloud etc.

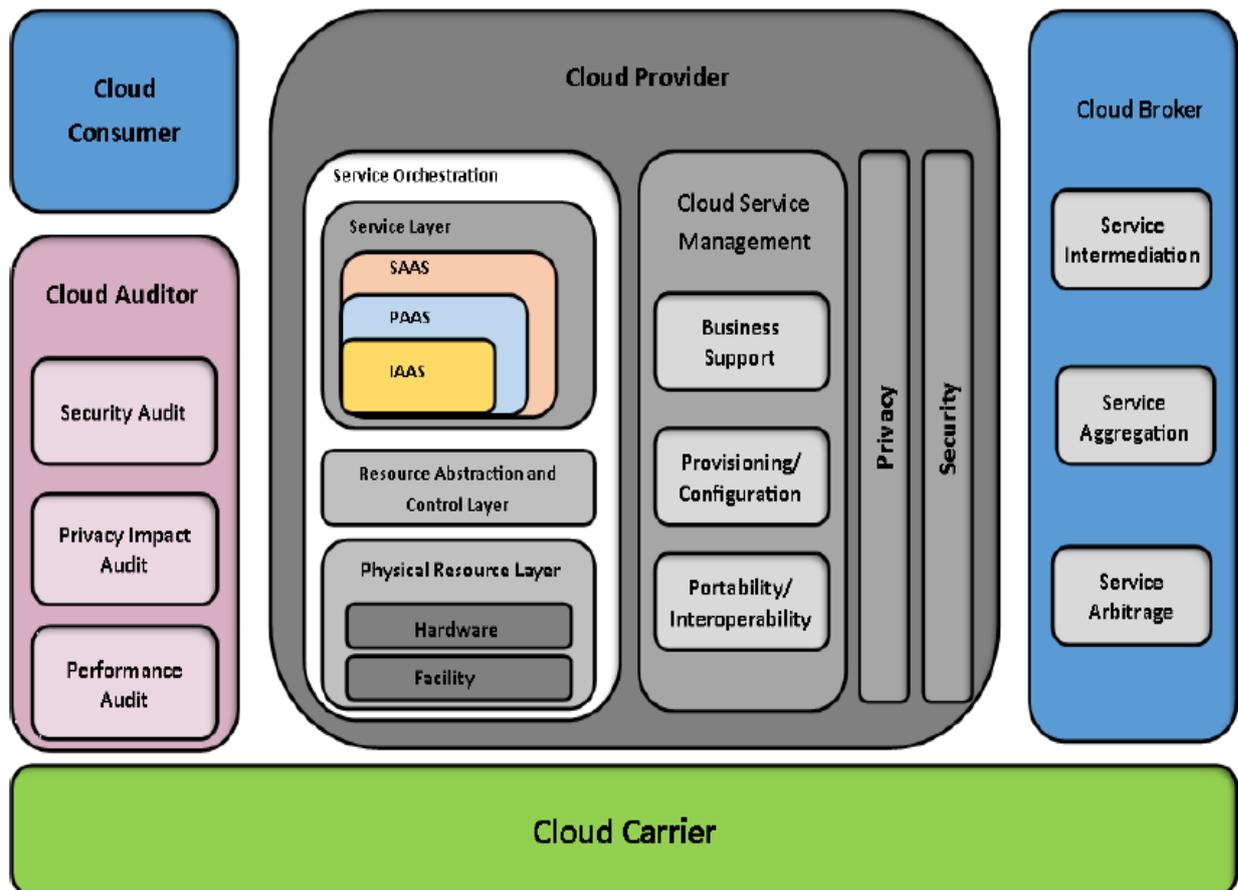
## I. INTRODUCTION

Cloud computing is the latest technology used by different category of users. Cloud computing services such as Software as service, Platform as service and Infrastructure as service are offered to the users using virtualization technology. Virtualization enables sharing resources of one system such as CPU, Memory and Storage to many users as per the requirement. Mainly Infrastructure as service is offered to the users through the

virtual machines. Although there are advantages of using the virtual machines, security is one of the aspect which is taken care to a lesser extent. Virtual machines are exposed to different attacks such as malwares, malicious users. There are threats like denial of service, cross virtual machine attacks, insecure virtual machine migration, attacks on virtual machine image and hypervisor etc., hence virtual machine security has to be looked with high priority. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently.

Some of the key advantages are:

1. Cost of entry for all organizations including small firms
2. Almost immediate access to the resources
3. Reduction in IT barriers to innovation
4. Easy to scale the services
5. Implement and/or offer new class of application and delivery services



**Fig 1: cloud computing**

## II. ISSUES IN CLOUD INTEROPERABILITY

### Intermediary Layer

A number of recent works address the interoperability issue by providing an intermediary layer between the cloud consumers and the cloud-specific resources (e.g. VM).

### Open Standard

Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors.

### Open API

SUN has recently launched the Sun Open Cloud Platform under the Creative Commons license. A major contribution of this platform is the proposed (in-progress) the cloud API. It defines a set of clear and easy-to-understand RESTful Web services interfaces, through which cloud consumers are able to create and manage cloud resources, including compute, storage, and networking components in a unified way.

### SaaS and PaaS Interoperability

While the aforementioned solutions generally tackle with IaaS interoperability problems, SaaS interoperability often involves different application domains

such as ERP, CRM, etc. A group of experts in the field of data mining raises the issue of establishing a data mining standard on the cloud, with a particular focus on “the practical use of statistical algorithms, reliable production deployment of models and the integration of predictive analytics” across different data mining-based SaaS clouds. PaaS interoperability not yet discovered Since PaaS involves the entire software development life-cycle on the cloud, it would be more difficult to reach the uniformity with regards to the way consumers develop and deploy cloud applications.

### III. RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

Several risks and security concerns are associated with cloud computing and its data. However, this study will discuss about the virtualization, storage in public cloud and multitenancy which are related to the data security in cloud computing.

#### Virtualization

Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully. A special function called hypervisor is required to run a guest operating system as a virtual machine in a host operating system. Virtualization is a foundational element of cloud computing which helps in delivering the core values of cloud computing. However, virtualization poses some risks to data in cloud computing. One possible risk is IV. compromising a hypervisor itself. A hypervisor can become a primary target if it is vulnerable. If a hypervisor is

compromised, the whole system can be compromised and hence the data. Another risk with virtualization is associated with allocation and de-allocation of resources. If VM operation data is written to memory and it is not cleared before reallocation of memory to the next VM, then there is a potential for data exposure to the next VM which might be undesirable.

#### Storage in Cloud

Storing data in a public cloud is another security concern in cloud computing. Normally clouds implement centralized storage facilities, which can be an appealing target for hackers. Storage resources are complicated systems that are combination of hardware and software implementations and can cause exposure of data if a slight breach occurs in the public cloud. In order to avoid such risks, it is always recommended to have a private cloud if possible for extremely sensitive data.

#### Multitenancy

Shared access or multitenancy is also considered as one of the major risks to data in cloud computing. Since multiple users are using the same shared computing resources like CPU, Storage and memory etc. it is threat to not only a single user but multiple users. Multitenancy exploits can be exceptionally risky because one fault in the system can allow another user or hacker to access all other data.

### CONCLUSION

This paper discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it

concerning security. This paper is the study of data security techniques used for protecting and securing data in cloud throughout the world. It discusses the potential threats to data in the cloud and their solutions adopted by various service providers to safeguard data.

## REFERENCES

- [1] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," 2010 24th IEEE International Conference on Advanced Information Networking and Applications(AINA), pp. 27-33, DOI= 20-23 April 2010
- [2] M. Q. Zhou, R. Zhang, W. Xie, W. N. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," 2010 Sixth International Conference on Semantics, Knowledge and Grids(SKG), pp.105-112, DOI= 1-3 Nov. 2010
- [3] J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," 2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.
- [4] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "Cloud Computing Research and Development Trend," In Proceedings of the 2010 Second International Conference on Future Networks (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-97. DOI=10.1109/ICFN.2010. 58.
- [5] J. J. Peng, X. J. Zhang, Z. Lei, B. F. Zhang, W. Zhang, and Q. Li, "Comparison of Several Cloud Computing Platforms," 2009 Second International Symposium on Information Science and Engineering (ISISE '09). IEEE Computer Society, Washington, DC, USA, pp. 23-27, DOI=10.1109/ISISE.2009.94.
- [6] S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "The Comparison between Cloud Computing and Grid Computing," 2010 International Conference on Computer Application and System Modeling (ICCASM), pp. V11-72 - V11-75, DOI= 22-24 Oct. 2010.
- [7] M. M. Alabbadi, "Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS)," 2011 14<sup>th</sup> International Conference on Interactive Collaborative Learning (ICL), pp. 589 – 594, DOI=21-23 Sept. 2011.
- [8] P. Kalagiakos "Cloud Computing Learning," 2011 5th International Conference on Application of Information and Communication Technologies (AICT), Baku pp. 1 - 4, DOI=12-14 Oct. 2011.
- [9] P. Mell and T. Grance, "Draft nist working definition of cloud computing - vol. 21, Aug 2 009, 20 09.
- [10] "Sun Microsystems Unveils Open Cloud Platform," [Online]. Available: <http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml>,2009.
- [11] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," 2010 7th International Conference on Informatics and System, pp. 1-8, March 2010.
- [12] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," 2009 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 711-716.