



## Issues in Realization of Cloud Computing Framework

Rituraj Jain

Department of Computer Science & Engineering  
Vyas Institute of Engineering and Technology  
Jodhpur, India  
[jainrituraj@yahoo.com](mailto:jainrituraj@yahoo.com)

**Abstract:** Ongoing researches from past many years in the field of information technology introduced a new terminology known as “Cloud Computing” which works as a solution to reduce costs for organizations. Cloud computing is the way by which resources, software and information are shared and provided to smart devices including computers over the Internet. Revolution in the technology in the form of cloud computing set up the smart ways to do business with effective cost and ease but also introduces new challenges and risk factors into the critical applications and sensitive private data and information stored in the cloud servers. This paper aims to identify the issues related to securities and privacy challenges in cloud computing environment.

**Keywords:** Cloud Computing, Community Cloud, Hardware as a Service, Hybrid Cloud, Platform as a Service, Security, Private Cloud, Public Cloud, Software as a Service.

### I. INTRODUCTION

So many statements from the experts are defined in favor as well as in against for cloud computing. Some of which are: “We’ve redefined Cloud Computing to include everything that we already do... I don’t understand what we would do differently in the light of Cloud Computing other than change the wording of some of our ads.” quoted by Larry Ellison, founder of Oracle in Wall Street Journal, 26 September 2008. Richard Stallman, founder of GNU in Guardian, quoted that “It’s stupidity. It’s worse than stupidity: it’s a marketing hype campaign” on September 29, 2008. “A lot of people are jumping on the [cloud] bandwagon, but I have not heard two people say the same thing about it.” quoted by Andy Isherwood, vice president and general manager of HP’s worldwide Software in ZDnet News, December 11, 2008 [1].

So first point comes into the mind is whether cloud computing is favorable or not. But before answering this question it is required to understand the cloud computing technology as well as the issues related to security involved in it.

Cloud computing terminology is the outcome of continuous research in the field of networking, web solutions, distributed computing etc. from many decades. The term became “popular” sometime in October 2007 when IBM and Google announced collaboration in that domain. This was followed by IBM’s announcement of the “Blue Cloud” effort. Since then, everyone is talking about “Cloud Computing” [2]. By maintaining the data and applications at central remote servers using the internet it allows consumers and businesses to use applications and availability of computing data from anywhere without installation those applications. A Google spokesperson added, “This means people can access the information that they need from any device with an Internet connection—including mobile and handheld phones—rather than being chained to the desktop. It also means lower costs, since there is no need to install software or hardware” [3].

Yahoo email and Gmail or any mail services can be consider as an example to understand brief picture of cloud computing. No one requires special software or a server to use them except an internet connection. It was found in the study conducted by VersionOne in June, 2009 that many senior IT professionals and two-thirds of senior finance professionals are either don’t know about the new term cloud computing or confused by the concept. According to an Aberdeen Group study conducted in Sep 2009 it was found that there is reduction about 18% on an average IT budget and 16% reduction in data center power costs at discipline IT organizations [4]. Both of these studies suggest that savings can be made by organization by adopting cloud computing in practice. But only considering savings always not fulfill the objectives of the new technology. Protection and control of the organizational as well as individual data must also be considered as critical factor of this service. So many issues related to risk ownership, contract and audit ownership must be address before actually make use of cloud computing services [5].

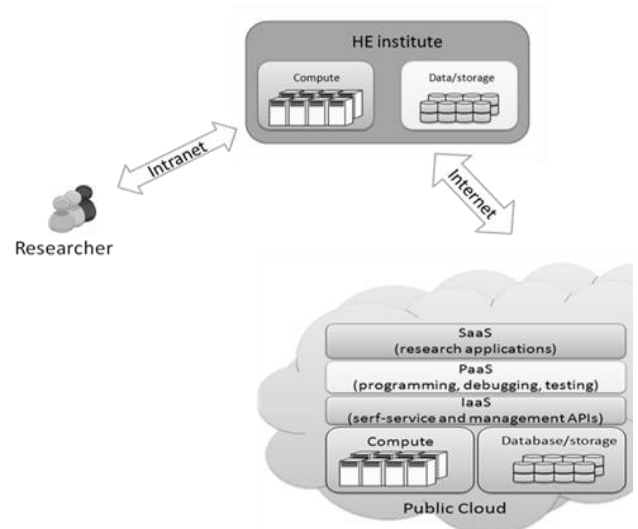


Figure. 1 Public Cloud

## II. REALIZATION OF CLOUD COMPUTING

Cloud computing is Internet based system development in which large scalable computing resources are provided “as a service” over the Internet to users. Based on the requirements of customer business cloud service provider provide either model as Public cloud, private cloud, community cloud, and hybrid cloud. Differentiation between all these models are listed in the below given Table1 [6].

Table1: Comparison of Cloud model based on setup and accessibility

| Cloud Model     | Setup as                          | Accessible to                                 |
|-----------------|-----------------------------------|---|
| Public Cloud    | external to the organization      | public over the internet                      |
| Private Cloud   | within organization's data center | operated exclusively for an organization      |
| Community Cloud | Sharing between many organization | group of organizations that jointly construct |
| Hybrid Cloud    | composition of two or more clouds | Public as well as private                     |

Structure of the all the clouds Public, Private, Hybrid and Community is shown in figure 1, 2, 3, and 4 respectively [7].

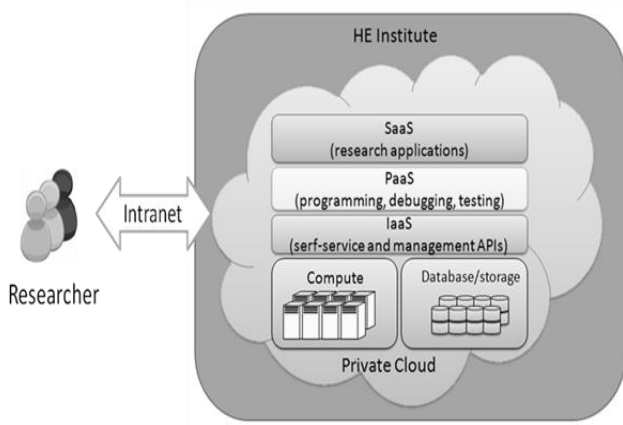


Figure. 2 Private Cloud

The concept of cloud computing incorporates web infrastructure as a Service (IaaS), Software as a Service (SaaS), Hardware as a Service (HaaS), Web 2.0, Platform as a Service (PaaS) and other emerging technologies, and has attracted more and more attention from industry and research community.

Infrastructure as a Service (IaaS) is concerned with providing infrastructure facilities like data center, hardware and software resources, servers, operating systems, disk storage, database, and/or messaging resources. Some of the examples are Amazon's Elastic Compute Cloud (AWS), IBM, VMware, HP etc. IT vendors are also offering services.

SaaS is one of the methodologies of Cloud Computing by which an enterprise organization will build a web based software application and host it and operate it over the internet for use by its customers. This web application will be shared by multiple clients. So it can be characterized as "Software deployed as a hosted service and accessed over the Internet." Issues related to access to the application, security, availability, and performance will be taken care by

the service provider itself. From the customer point of view no hardware or software has to buy, install, maintain, or update. Only an internet connection required to access applications.

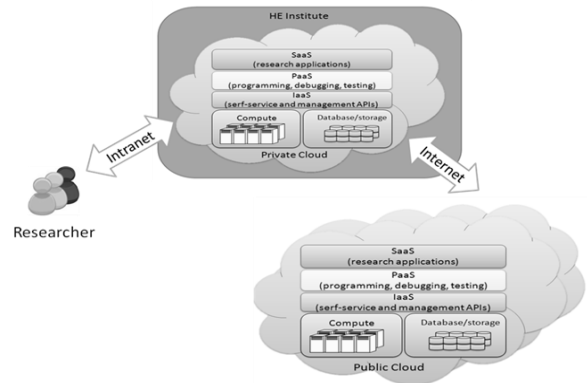


Figure. 3 Hybrid Cloud

Platform as a Service (PaaS) provides infrastructure over the internet which are actually required to build an application and services. By using these services new applications or existing application with some extended form can be developed by software developers. Salesforce.com's Force.com, Google's App Engine, and Microsoft's Azure are examples of PaaS. These Platform features enable companies to create custom applications, but also allow Independent Software Vendors and other third parties to create solutions for vertical niches.

## III. ISSUES INVOLVE IN CLOUD COMPUTING

When we talk about the benefits like cost and ease of use of the cloud computing, we also need to think about the issues that put their impacts on the success of this new technology. Because of the integration of many technologies like networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management in cloud computing, there are numerous security issues associated with it [8].

As different models of the cloud computing will share critical applications and sensitive data to publicly or within multiple organizations, some security issues must be discussed before deployment of cloud services.

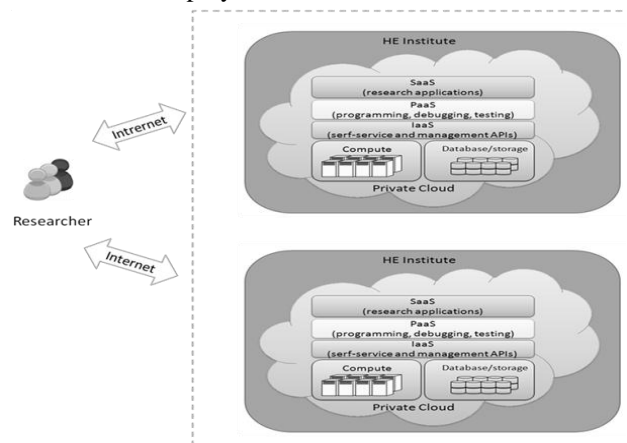


Figure. 4 Community Cloud

It must require providing similar or more commanding security than the security level they have without the use of

cloud services. Issues which must be discussed are: location and accessibility of the data, regulatory requirements concerns to the organization location like certification or accreditation, auditing issues like who is responsible for auditing the security provided by the cloud, training requirements, organization of the data i.e. how individual organization data is separated from other organizations, aging and experience of the service provider, and recovery plan.

Based on the issues listed above a checklist must be drawn as given below [5]:

- a. Who is questionable about the risk?
- b. Who can access data in what amount and in which from?
- c. Who is responsible of information security?
- d. Who has an authority to validate the security provided to the data in cloud environment?
- e. What to do when cloud service provider itself is a part of forensic investigations?
- f. Is the cloud service requester can able to audit the service provider?
- g. How to assure that your data is separated from others and not accessible to unauthorized entity.
- h. What about data encryption?
- i. What about data when service provider is shuts down or bankrupt?
- j. Which jurisdiction rules must be applied on disputes?
- k. What happened in the case of Denial of Service attack?
- l. How do we know and verify that the computations do by cloud provider is correct?
- m. How do we ensure that our data is stored without tampering?

In a broad way issues like trust and privacy, interoperability, and the reliability of the services will be consider during the discussion before the deployment. Many cloud networks are configured as closed systems so multiple networks cannot integrated together which lead to a negative impact because organization cannot realize productivity gain and cost saving. Reliability comes into the picture when services provided to users on demand. Users required it to access in any network. One of the examples identified for unreliability is Apple's MobileMe cloud service, which stores and synchronizes data across multiple devices. This service started with a problem that many users were not able to access mail and synchronize data correctly. To avoid such problems, providers are turning to technologies such as Google Gears, Adobe AIR, and Curl, which allow cloud based applications to run locally, some even allow them to run in the absence of a network connection [6].

#### IV. SOLUTIONS TO IDENTIFIED ISSUES

The non-profit Cloud Security Alliance (CSA) working towards gathering the number of groups seeking to introduce solutions as a standards and security for cloud computing. Similarly information about cloud standards under development are shared by the Cloud Standards web site, list of vulnerabilities to cloud-based or Software as a Service deployment models maintain by the Open Web Application Security Project (OWASP), while the security and infrastructural specification documents are published by the Open Grid Forum. Issues concerning web application security can be resolved by defining a development

framework which shows and provides training regarding the security. For issues related to accessibility can be handling by identifying the count of filtering a packet-sniffer output to specific services. One general solution to accessibility vulnerabilities is just shut down unused services, keep patches updated, and reduce permissions and access rights of applications and users. Issues like authentication can be controlled by avoiding IP spoofing by using encrypted protocols wherever possible as well as ARP poisoning can be avoided by requiring root access to change ARP tables; using static, rather than dynamic ARP tables.

Issues related to data security can be making less effective by isolation of the resources e.g. isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache. There is still no way to indentify whether the user data is deleted or not. Issues related to privacy and control solutions can not completely dissolvable from their implemented image. But these issues merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private. Physical access solutions will be provided by using in-house private cloud [9].

#### V. CONCLUSION

In the current scenario of competitive market definitely cloud computing introduce an edge of benefits to the companies. So many organizations are now trying to touch this technology as soon as possible. But the real question or the constraint that they have to think about is the security in all levels and in different aspects of this new emerging technology. It is required to closely go through the security issues of any cloud-based services and imply the protections to the information of the different cloud consumers.

#### VI. REFERENCES

- [1]. <http://sardes.inrialpes.fr/~malvault/introCC.pdf>
- [2]. Mladen A. Vouk, (2008) "Cloud Computing – Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246 doi:10.2498/cit.1001391
- [3]. <http://www.freeonlinepaperresearch.com/cloud-computing-research-paper>
- [4]. [http://www.wikinvest.com/concept/Cloud\\_Computing](http://www.wikinvest.com/concept/Cloud_Computing)
- [5]. Henry B. "Cloud Computing: The Emperor's New Clothes of IT". Proceedings of Informing Science & IT Education Conference (InSITE) 2011
- [6]. Sarfraz Nawaz Brohi et al. "Challenges and Benefits for Adopting the Paradigm of Cloud Computing", International Journal Of Advanced Engineering Sciences And Technologies Vol No. 8, Issue No. 2, 286 – 290
- [7]. Xiaoyu Chen et al. "Using Cloud For Research: A Technical Review", TeciRes Project Report, [http://tecires.ecs.soton.ac.uk/use\\_case\\_scenarios.php](http://tecires.ecs.soton.ac.uk/use_case_scenarios.php) (accessed on: 30<sup>th</sup> Sep, 2011)
- [8]. Kevin Hamlen, et al. "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 39, DOI: 10.4018/jisp.2010040103
- [9]. <http://wolfhalton.info/2010/06/25/security-issues-and-solutions-in-cloud-computing/>