International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

# Cloud Computing Issues

Rini Mahajan

Assistant Professor
QIFGOI,Jhanjeri,Mohali
rinimahajan@gmail.com

Dr. Dheerendra Singh
Professor
SUS,Tangori
professordsingh@gmail.com

**Abstract-**Cloud computing is Internet-based computing, whereby shared resources, software and information, are provided to computers and devices on-demand, like the electricity grid. It aims to construct a perfect system with powerful computing capability through a large number of relatively low-cost computing entity, and using the advanced business models like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to distribute the powerful computing capacity to end users' hands. Cloud Computing represents a new computing model that poses many demanding security issues at all levels, e.g., network, host, application, and data levels. The variety of the delivery models presents different security challenges depending on the model and consumers' Quality of Service (QoS) requirements. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. This paper introduces the existing issues in cloud computing such as security, privacy, reliability and so on. This paper surveys the security problems of current cloud computing.

## Introduction

Cloud computing describes both a platform and a type of application. A cloud computing platform dynamically provisions, configures, reconfigures, and deprovisions servers as needed. Cloud applications are applications that are extended to be accessible through the Internet. These cloud applications use large data centers and powerful servers that host Web applications and Web services. Cloud Computing enables innovation. It alleviates the need of innovators to find resources to develop, test, and make their innovations available to the user community. Innovators are free to focus on the innovation rather than the logistics of finding and managing resources that enable the innovation. A cloud is a pool of virtualized computer resources. A cloud can Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications. it Allows workloads to be deployed and scaled-out quickly through the rapid provisioning of virtual machines or physical machines  Support redundant, selfrecovering, highly scalable programming models that allow workloads to recover from many unavoidable hardware/software failures and  Monitor resource use in real time to enable rebalancing of allocations when needed [1].

## Cloud Architecture

Delivery of cloud computing comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple cloud components communicating with each other over application programming interfaces, usually web services. This closely resembles the UNIX philosophy of having multiple programs doing one thing well and working together over universal interfaces. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts.

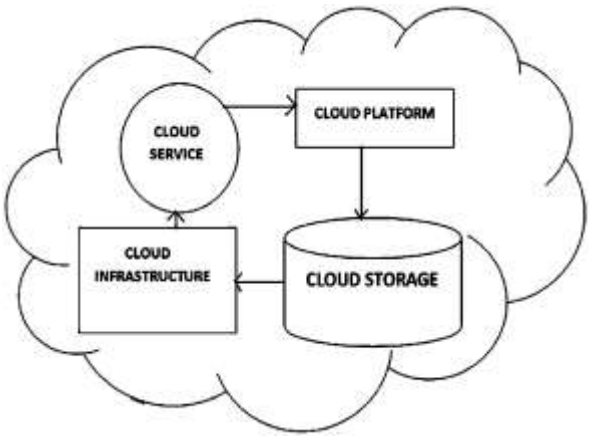



Fig.1: Architecture of Cloud

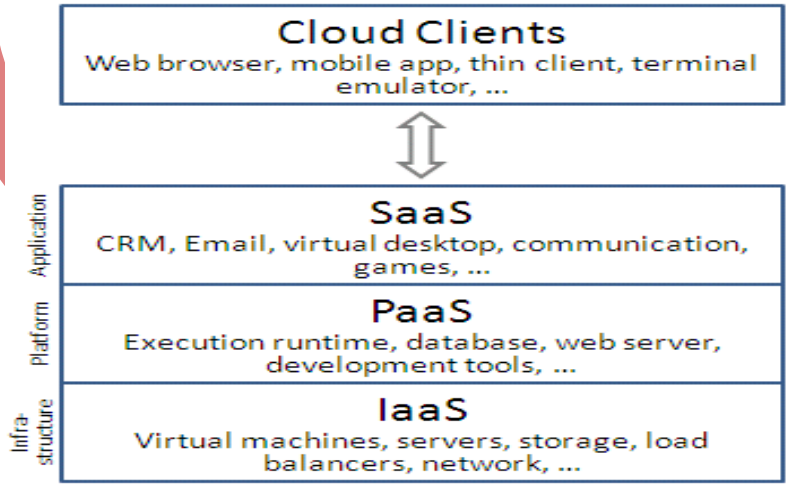
International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Cloud architecture extends to the client, where web browsers and/or software applications access cloud applications. Cloud storage architecture is loosely coupled, where metadata operations are centralized enabling the data nodes to scale into the hundreds, each independently delivering data to applications or users. Security is the challenge seen related to Cloud Computing according to our architecture. The main security concerns include performance, reliability compliance, privacy in interoperability and visibility under virtualization.

Cloud computing technologies can provide organizations competitive advantage in the market, cost reductions, higher margins, simplified maintenance and management of applications across the enterprise, greatly extended scalability, agility, high availability, automation, large data storages and reliable backup mechanisms. By using Cloud Computing environments, organizations can focus on their core business as opposed to concerning themselves about infrastructure scalability. Organizations may explore use of cloud computing initially for better performance through peak demand periods but eventually adoption could spread to other areas.[2]

## Service Models

Cloud computing is an innovation of traditional computing model. there is no standard, every enterprise is using different architecture. At the bottom of the upper service layer, Infrastructure as a Service (IaaS) supplies computing resources and storage resource for users. In the case of a particular service constrains, IaaS provides an intermediate platform to run arbitrary operating systems and software. Platform as a Service (PaaS) is in the middle part of the cloud service layer, it can give users better performance, a more personalized hardware and software services, and a lot of infrastructure module, such as remote call module, distributed data module, the user registration module, billing module, etc. These modules can be used by the Software as a Service (SaaS). The top of cloud service layer is the SaaS, it provides application, which is closest to the user's service, and allows deploying the software in a network environment, so that the software can be run under a multi-user platform. [3,4].




## Deployment model

Public Cloud- A public cloud is one in which the infrastructure and other computational resources that it comprises are made available to the general public over the Internet. It is owned by a cloud provider selling cloud services and, by definition, is external to an organization. Private Cloud- A private cloud is one in which the computing environment is operated exclusively for an organization. It may be managed either by the organization or a third party, and may be hosted within the organization's data center or outside of it. A private cloud gives the organization greater control over the infrastructure and computational resources than does a public cloud. community clouds-A community cloud is somewhat similar to a private cloud, but the infrastructure and computational resources are shared by several organizations that have common privacy, security, and regulatory considerations, rather than for the exclusive use of a single organization. Hybrid

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Cloud- A hybrid cloud is a composition of two or more clouds (private, ommunity, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables interoperability[5].

## Cloud computing characteristics

Cloud computing exhibits the following key characteristics:

- Agility improves with users' ability to re-provision technological infrastructure resources.
- Application Programming Interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.
- Cost is claimed to be reduced and in a public cloud delivery model.This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks
- Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using. As infrastructure is off-site and accessed via the Internet, users can connect from anywhere.
- Multi-tenancy enables sharing of resources and costs across a large pool of users thus allowing for:
- Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer. They are easier to support and to improve, as the changes reach the clients instantly.
- Scalability via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.

## Issues in Cloud Computing

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model differ widely from those of traditional architecture [6]. as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

- **Privacy** Different from the traditional computing model, cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data center rather than stay in the same physical location, even across the national borders, at this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users [9]. The cloud model has been criticized by privacy advocates for the greater ease in which the companies hosting the cloud services control, and, thus, can monitor at will, lawfully or unlawfully, the communication and data stored between the user and the host company. The relative security of cloud computing services is a contentious issue that may be delaying its adoption. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solution to various cloud security issues vary through cryptography, particularly public key infrastructure (PKI), use of multiple cloud providers, standardization of APIs, improving virtual machine support and legal support[6, 7, 8]

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

**Abuse** As with privately purchased hardware, crackers posing as legitimate customers can purchase the services of cloud computing for nefarious purposes. This includes password cracking and as a means of launching attacks.

- **Security** Where is your data more secure, on your local hard driver or on high security servers in the cloud? Some argue that customer data is more secure when managed internally, while others argue that cloud providers have a strong incentive to maintain trust and as such employ a higher level of security.However, in the cloud, your data will be distributed over these individual computers regardless of where your base repository of data is ultimately stored. Industrious hackers can invade virtually any server, and there are the statistics that show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet, with nearly 16 percent due to insider theft [9].
- **Reliability** Servers in the cloud have the same problems as your own resident servers. The cloud servers also experience downtimes and slowdowns, what the difference is that users have a higher dependent on cloud service provider (CSP) in the model of cloud computing. There is a big difference in the CSP's service model, once you select a particular CSP, you may be locked-in, thus bring a potential business secure risk.
- **Legal Issues** Regardless of efforts to bring into line the lawful situation, as of 2009, supplier such as Amazon Web Services provide to major markets by developing restricted road and rail network and letting users to choose "availability zones" [10]. On the other hand, worries stick with safety measures and confidentiality from individual all the way through legislative levels.
- **Open Standard** Open standards are critical to the growth of cloud computing. Most cloud providers expose APIs which are typically well-documented but also unique to their implementation and thus not interoperable. Some vendors have adopted others' APIs [11] and there are a number of open standards under development, including the OGF's Open Cloud Computing Interface.
- **Freedom** Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers. Customers will contend that this is pretty fundamental and affords them the ability to retain their own copies of data in a form that retains their freedom of choice and protects them against certain issues out of their control whilst realizing the tremendous benefits cloud computing can bring [12].
- **Long-term Viability** You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company [13].
- **System Integrity** Clouds require protection against intentional subversion or sabotage of the functionality of a cloud. Within a cloud there are stakeholders: subscribers, providers, and a variety of administrators. The ability to partition access rights to each of these groups, while keeping malicious attacks at bay, is a key attribute of maintaining cloud integrity. In a cloud setting, any lack of visibility into a cloud's mechanisms makes it more difficult for subscribers to check the integrity of cloud-hosted applications[14].
- **CONCLUSION**

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of their competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security. Data encryption, Identity management

## REFERENCES

[1] www.ibm.com/developerworks/websphere/zones/hipods/

[2] ANALYSIS OF SECURITY ISSUES AND PERFORMANCE ENHANCEMENT IN CLOUD COMPUTING Herminder Singh1 & Babul Bansal2 International Journal of Information Technology and Knowledge Management July-December 2010, Volume 2, No. 2, pp. 345-349

[3]http://en.wikipedia.org/wiki/File:Cloud_computing_layers.png

[4] Xue Jing 1 Zhang Jian-jun2 "A Brief Survey on the Security Model of Cloud Computing" 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science

[5] Standards and Technology Draft Special Publication 800-144 60 pages (Jan. 2011)

Guidelines on Security and Privacy in Public Cloud Computing

[6] Anthens, G. "Security in the cloud". Communications of the ACM 53 (11). DOI:10.1145/1839676.1839683.

[7] Swiss Carbon-Neutral Servers Hit the Cloud.. Retrieved 4 August 2010.

[8] Berl, Andreas, et al., Energy-Efficient Cloud Computing, The Computer Journal, 2010.

[9] Elinor Mills, January 27,2009. "Cloud computing security forecast: clear skies".

[10] C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, [2005] "Live migration of virtual machines" In Proc. Of NSDI'05, pages 273-286, Berkeley CA, USA, 2005. USENIX Assiciation.

[11] Eucalyptus Completes Amazon Web Services Specs with Latest Release.

[12] Jack Schofield. Wednesday 17 June 2009 22.00 BST,http://www.guardian.co.uk/technology/2009/jun/17/cloud-computingjack- schofield.

[13] Gartner. "Seven cloud-computing security risks". http://www.infoworld.com July 02,2008.

[14] Enhancing Security in Cloud Computing Joshi Ashay Mukundrao (Corresponding author) D.Y. Patil College Of Engineering, Akurdi, Pune University of Pune, Maharashtra, India Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011 40 | P a g e www.iiste.org Enhancing

**Rini Mahajan (M. Tech & BE. Computer Science & Engg),** Working as HOD & Asst. Prof in the Department of Computer Science & Engg. At QIFGOI Jhanjeri ,Mohali. I Am Having 9 years of teaching experience and I have published 16 research papers in National & International Journals /Conferences.

**Dr. Dheerendra Singh**, having **B.E., MTech, PhD** in Computer Science & Engineering, is working as Professor & Head of Computer Science & Engineering Department at Shaheed Udham Singh College of Engineering & Technology, Tangori, Mohali, Punjab. He is life Member of IETE, New Delhi (Member No. M- 208777). He has published and presented 24 research papers in National & International Journals /Conferences. He is a member of reviewer Panel of International Journal of Information Technology & Knowledge Management. He is having 11 years of experience of teaching at various reputed Engineering Institutes which includes 7 years of experience as Head of Department. He is guiding PhD and MTech students in Computer Science & Engineering.