ISSN: 2321-7782 (Online)
Volume 2, Issue 8, August 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Cloud Computing Opportunities, Emerging Threats and Ways to Overcome Future Challenges - A Study in Context of Developing Nation India

Pankaj Kamboj
Deputy Manager
HCL Technologies Ltd
Noida – India

Abstract: ***In last several decades, there is dramatic increment in computing power, networking and storage technology that have allowed the human race to generate, process, and share increasing amounts of information in dramatically new ways. As new applications of computing technology are developed and introduced which has lead to new demands for even more powerful computing infrastructure. To meet these computing-infrastructure demands, system designers are constantly looking for new system architectures and algorithms to process larger collections of data more quickly than is feasible with today's systems. Here, we refer to the hardware and software environment that implements this service-based environment as a cloud-computing environment. Some people use the terms Cloud Computing, Grid Computing, Utility computing, or Application service providers to describe the same storage, computation, and data-management ideas that constitute Cloud computing.***

The recent IDC cloud research shows that worldwide revenue from public IT cloud services exceeded $21.5 billion in 2010 and will reach $72.9 billion in 2015, representing a compound annual growth rate (CAGR) of 27.6%. This rapid growth rate is over four times the projected growth for the worldwide IT market as a whole (6.7%). By 2015, one of every seven dollars spent on packaged software, server, and storage offerings will be through the public cloud model [1].

In Cloud computing data is stored and maintained at Data Center of hosted service providers like Google, Microsoft, Amazon, HP, Salesforce etc. which in turn increase the risk of data and information security. The risk and threats may be in form of internal threats, data security leakage and insure web access. This research paper outlines the risk, challenges and way to overcome the risk and threats created by Cloud model.

Keywords: Cloud Computing, Green Computing, Virtualization.

I. INTRODUCTION

The origin of the term *cloud computing* is obscure, but it appears to derive from the practice of using drawings of stylized clouds to denote networks in diagrams of computing and communications systems. The word *cloud* is used as a metaphor for the Internet, based on the standardized use of a cloud-like shape to denote a network on telephony schematics and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. The cloud symbol was used to represent the Internet as early as 1994 [2].

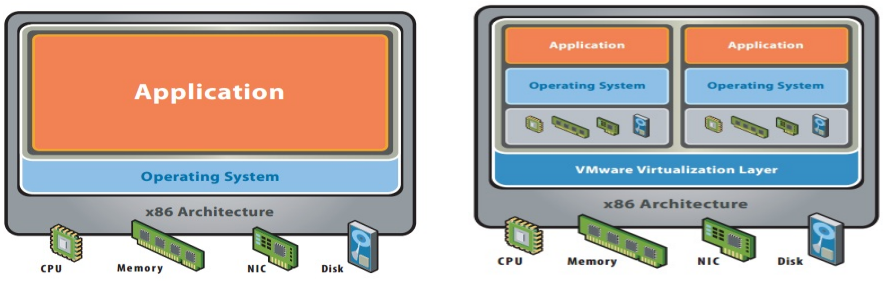
However in the coming year, Cloud computing is going to play a pivotal role in the growth of IT service industry as more and more clients shifting towards cloud model due to uncertain global market. As per Gartner report, Worldwide Cloud Services Market to surpass $109 Billion in 2012. The public cloud services market is forecast to grow 19.6 percent in 2012 to total $109 billion worldwide, according to Gartner, Inc. Business process services (also known as business process as a service, or BPaaS)

represent the largest segment, accounting for about 77 percent of the total market, while infrastructure as a service (IaaS) is the fastest-growing segment of the public cloud services market and is expected to grow 45.4 percent in 2012 [3].

While Gartner estimates that Cloud Computing market in India is expected to surpass $326 million (up 32.4%) in 2012 in which Software as a service (SaaS) is the largest segment and is forecasted to touch $115.6 million and infrastructure as service (IaaS) is estimated to touch $ 42.7 million in 2012.Cloud computing refers to pay-per-use model of computing where applications and softwares are accessed over the internet and not owned by users. Companies can save huge costs on these products as they would not have to invest in purchasing them; resulting in reduced IT costs [4].

II. Inside the Cloud Virtualization

Virtualization in computing is the creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system, a storage device or network resources [5]. In cloud computing it refers primarily to platform virtualization or the abstraction of physical IT resources from the people and applications using them. Virtualization allows servers, storage devices, and other hardware to be treated as a pool of resources rather than discrete systems, so that these resources can be allocated on demand. In cloud computing, it allows a single server to be treated as multiple virtual servers, and *clustering*, which allows multiple servers to be treated as a single server. The commonly used base layer of virtualization is Vmware ESX layer or Microsoft hypervisor. This thin software layer is installed on the naked machine and on the top of it we may install multiple O.S like Linux, windows etc. which solve the purpose of rather buying multiple hardware and O.S. The virtualization technique enable to deploy multiple application on the same server with functionally like high availability, fault tolerance, zero downtime, load balancing etc. The below diagram shows the virtual layer of physical hardware before and after virtualization [6].



Before Virtualization:
- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Underutilized resources
- Inflexible and costly infrastructure

After Virtualization:
- Hardware-independence of operating system and applications
- Virtual machines can be provisioned to any system
- Can manage OS and application as a single unit by encapsulating them into virtual machines

Figure-1 Comparison among Physical and Virtual Machine

WHAT IS CLOUD COMPUTING?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure [7]. Cloud computing is a new consumption and delivery model inspired by consumer Internet services. The clients generally used to access are web browser, mobile app, thin clients etc. The below diagram shows the Non-Exhaustive view of cloud formation.

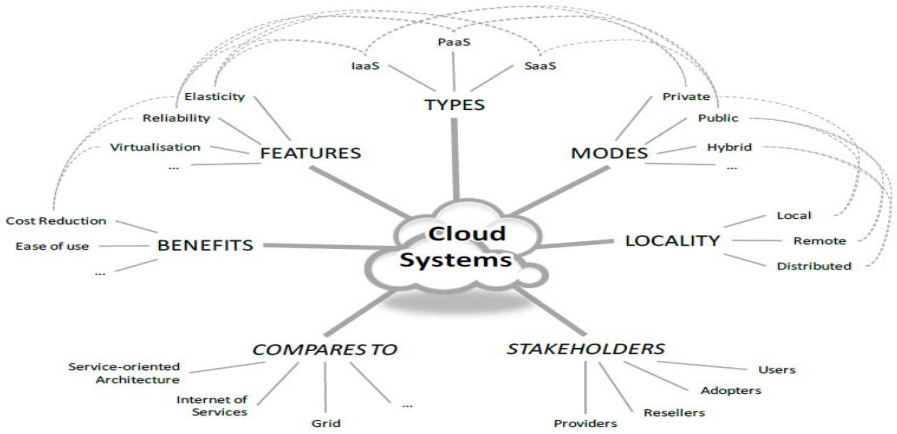


Figure-2 Non Exhaustive view on forming Cloud System
Source: The Future of Cloud Computing "Opportunities for European Cloud Computing beyond 2010"

Characteristics of Cloud Computing

Optimum Utilization Ratio — In Late 1999 and 2000, organization used to spent huge amount of their IT budget on buying server, software etc. but with the virtualization technologies and cloud computing , organization use the existing infrastructure to maximum and save lot of cost. Indeed, it is a great shift towards Green computing which means existing systems can be consolidated, so purchases of additional server capacity can be delayed or avoided [8].

IT Consolidation — As Virtualization allows for consolidation of IT infrastructure. One of the advantages is centralization of IT infrastructure with better control and manageability which was earlier, segregated. Now, with cloud computing organization can focus on core areas while effectively managing systems architecture, application infrastructure, data and databases, interfaces, networks, desktops, and even business processes, resulting in cost savings and greater efficiency.

Less power usage/costs — The electricity required to run enterprise-class datacenters is no longer available in unlimited supplies, and the cost is on an upward spiral. For every dollar spent on server hardware, an addition dollar is spent on power (including the cost of running and cooling servers). Using virtualization to consolidate makes it possible to cut total power consumption and save significant money.

Space Savings — servers which usually acquire enormous amount of space in most organization datacenters, but increasing a server every time for new application is not always a solution. Instead, Virtualization can alleviate the strain by consolidating many virtual systems onto fewer physical systems.

Business Continuity — Virtualization can increase overall service-level availability rates and provide new options for disaster recovery solutions.

Reduced Operational Costs — The average enterprise spends $8 in maintenance for every $1 spent on new infrastructure. Virtualization can change the server to-admin ratio, reduce the total administrative workload, and cut total operations costs.

WHAT COMPRISES OF CLOUD COMPUTING?

Cloud computing providers offer their services according to three fundamental models [9]: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models [10].

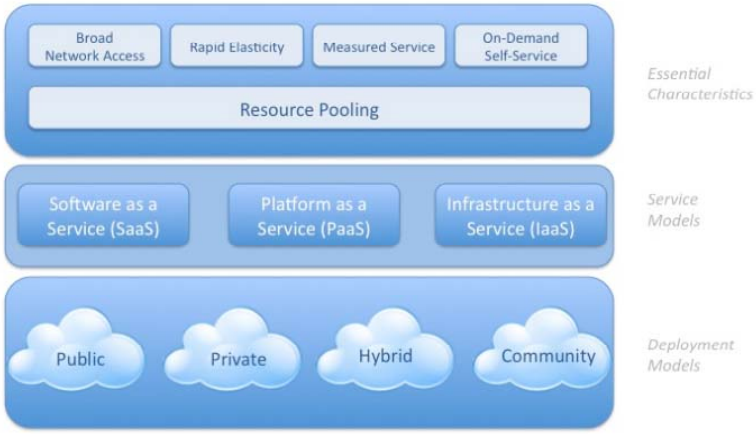


Figure-3 Source: NIST Visual Model of Cloud Computing Definition [11]

The 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively — and below are the types of Cloud:

• **Cloud Software as a Service (SaaS)** This model provides the consumer to use the applications running on cloud infrastructure. However, this cloud application can be accessed through client interface like web browser over the internet. The consumer is less bothered about backend infrastructure and doesn't not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. Since SAAS is pay per usage model. Hence, consumer pays on specific usage [12].

• **Cloud Platform as a Service (PaaS)** This model provides the consumer to deploy the applications or acquired applications created using programming languages and tools onto cloud infrastructure. The consumer is least bothered about managing or controlling the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

• **Cloud Infrastructure as a Service (IaaS)** This model provides the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

MODES OF CLOUD COMPUTING

The cloud Models are deployed (SaaS, PaaS, or IaaS) in the following ways. With the growing demand of Cloud computing, organization may opt below models, depend upon the business need [13]:

• **Public Cloud** In Public Cloud, the infrastructure is made available to the general public or a mass industry group and is owned by an organization selling cloud services.

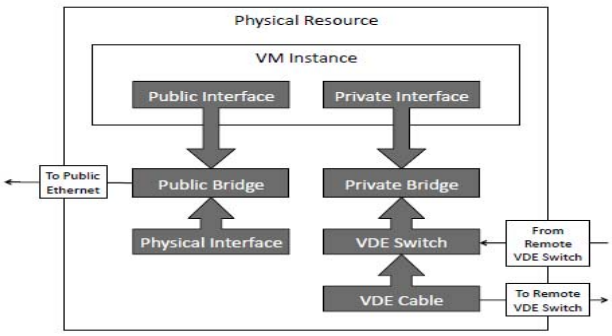


Figure-5, Source: The Eucalyptus Open-source Cloud-computing System, Page No.3

• **Private Cloud** The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises.

• **Community Cloud** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

• **Hybrid Cloud** The cloud infrastructure is a composition of two or more clouds (private,

Community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).However, now a days many organization have their own private cloud for their mission critical applications but are opting for hybrid cloud for services like Microsoft office 365, Google mailing solution and salesforce for CRM applications.

WHY SHOULD WE GO FOR CLOUD?

The Frost & Sullivan report shows the growth story of cloud computing market in India. In 2011, cloud computing market was INR 1350 Cr and it is estimated that it will surpass Rs. 11,000 Cr by 2016.Hence, from all this reports, it is obvious to see huge demand for cloud computing in India. However, BFSI and Govt. verticals emerge as the potential early adopter of cloud technology in India. Surprisingly, the top adopters' countries are Brazil, China, India and Germany followed by USA, Mexico, Australia and Far East countries [14].

Figure-6, The Cloud Computing market is expected to grow at a CAGR of 52% for the next 5 years, Source: Frost & Sullivan Study

III. RESEARCH METHODOLOGY

The idea of writing this paper is to study, analyze and examine the risk and challenges of Cloud computing. So, this research papers aims to develop a research model which can justify this paper and find out the possible risk, challenges and threats in cloud computing. Hence, we have taken a Descriptive Type Research Methodology. The source of Primary data was collected by conducting Telephonic interviews and by questionnaire sent through email and secondary data was collected from the newspaper, magazine, journals and internet.

Data Collection Methods:

1. Primary Data: The Primary data for this paper was collected using telephonic interview with IT personnel from about 50 industries which includes BFSI, Manufacturing, IT/ITES across Maharashtra. The study has been carried out in the organization who are currently using cloud computing or virtualization. The data is collected through structured interview of sequenced questions (given in last of paper in Appendix). Also, an email questionnaire was also being sent to collect the primary data. The questionnaire was focused towards security, availability, performance, pay per usage model, lack of interoperability standards, Integration with existing Infrastructure, able to customize, bring back-in-house etc.

2. Secondary data: The Secondary data was collected using internet, journals, magazines (CTO forum and Business Worlds) and Newspaper.

IV. RESEARCH FINDING

This chapter concluded with discussion regarding the finding of this study on the possible risks, threats of Cloud Computing and compared and contrasted the research findings with those found in the literature review.

Demographic Information

The areas selected for this study consisted of organization who have implemented virtualization within organization and hosted some of their server/ applications outside the premises. Also the respondents were subsequently contacted through Postal Mail, E-mail and telephonically to explain the context of the present research work, its significance and to clarify any queries/doubts to facilitate comprehensive and clear-cut responses to the Questionnaire. Since the interview questions were constructed specifically for this study, there are no measures of validity or reliability.

Analysis of Data Collected

However, we have discussed about the advantages of Cloud Computing but there are lots of security risks and threats are also encapsulated with new emerging technology-Cloud Computing. To avoid security gaps, service providers and consumer has to be very careful and need to take certain precautionary measures. As per Verizon Business Risk team which found the same risk and threats on vulnerability of data "90% of known vulnerabilities exploited had patches available for at least six months prior to the breach**"** Data Breach Investigations report, 2008. Indeed, it is true, whenever we bring new technology, it allows the threat to come too. With the upcoming cloud computing, the traditional security measures are not sufficient to keep the bad guys out. Since in Cloud computing, the computing resources (hardware/ software) are shared among multiple customers with multiple browsers hence chances of getting Virtual machines more vulnerable.

Analysis using Factor Rating Method

There are several concerns raised by IT professional while going with cloud computing:

To test this hypothesis factor rating method was used and the factors were analyzed on a scale of 5 in terms of risk and threats faced by cloud computing customers.

1= Not Concerned

5= Very much Concerned

The below table represents the different factors of adoption with their score and weighted score.

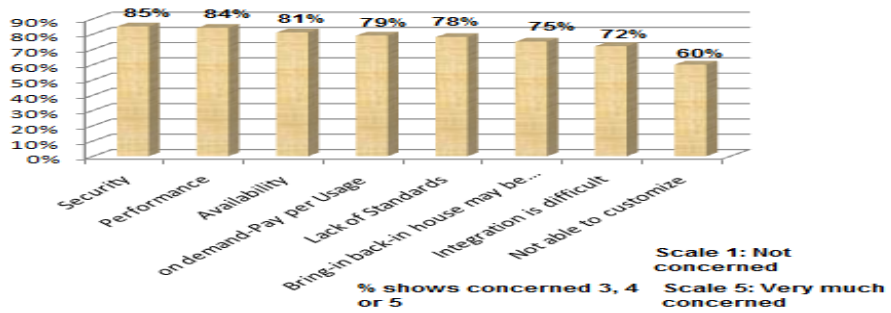


Figure-7, n=50

So, from the above chart, it is clear that the customer are more concern about security and several steps has to be taken while ensuring security as major factors towards cloud computing.

Discussion

The primary objective of this study was to evaluate the risk and challenges of cloud computing. On one side, it has advantages in terms of lower power cost, space saving, higher utilization rates, improve business continuity and reduced operation cost etc. but on the flip side there are many business risk/threats involved on which service providers has to take precautionary steps to avoid gaps. While going for Cloud computing deployments, investors must have to know about primary concerns and make sure service providers has all the below compliance/ perimeter in place.

Control and Monitor the access: In traditional way, users were given to access the applications and server as per its job requirement. Hence, more controlled administrative approach and on-premise access was enabled. In Cloud Computing, administrative control must be monitor via internet, decreasing risk and threats. It is extremely important to monitor and Control user behavior.

Security state of Virtual Machine: Virtual machines are prone to viruses and malware attacks because of their dynamic in nature. Virtual Machine can be cloned and seamlessly moved between physical machines. The dynamics nature of VM sprawl leads to consistent security issues. However, it is difficult to audit the record of security state of any virtual machine. Hence, it is become significant to see the security state of a system, irrespective of its location or proximity to other, potentially insecure virtual machines.

Passive Virtual Machines: The VM's who are dormant in nature are likely to get infected. As and when VM's sitting on hypervisor are not online, antivirus patches will not be updated. So, when we backed up or archived on storage or disk, chances of getting infected other data lying on storage or disk is very high. Hence, it is the responsibility of cloud providers to scan the dormant machines regularly.

Data Encryption: Due to rise in loss/theft of credit card fraud and confidential information, it is important to know whether the cloud provider is PCI-DSS and HIPPA compliance which can protect in case of breach or loss of data/ information**.** Hence, application and data has to be encrypted to keep away unauthorized access.

Virtual Patching: As per Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach. Also, as per" A Trend Micro White Paper, August 2009, Making Virtual Machines Cloud-Ready, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. If patching is impossible or unmanageable, compensating controls such as "virtual patching" need to be considered.

ISO compliant: Organizations has to follow necessary compliance due to significant pressure on compliance and ISO standard such as GLBA, HIPPA, ITIL, SOX and FISMA etc to improve level of Security standard. Hence, service providers has to comply with security standards, irrespective of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources.

Creation of DMZ: In cloud computing, perimeter security plays a pivotal role to protect the cloud from external threats like malware, viruses, internal threats and unauthorized access. However, it is always suggestible to do role based/ IP based configuration and therefore, instead of deploying antivirus on each VM machine, it is always a better idea to create a separate VM machine for antivirus which will keep on monitoring and safeguard against viruses. The virtual machines must be self-defending, effectively moving the perimeter security to the virtual machine itself.

WAYS TO OVERCOME RISK AND CHALLENGES…BUT HOW?

As we talked about, Virtualization is the base for cloud computing. Now a days, Organization are looking for server and Data Center consolidation which is a big step towards Green Computing but alarmed the security issues. The following are the five distinct security technologies—Unified Threat Box, intrusion detection and prevention, Monitoring of systems and

application, Log inspection with SIEM tool and Vulnerabilities protection—that can be deployed as software on virtual machines to enhance protection and improve compliance integrity of servers[15].

Firewall or Unified Threat Box:

A bi-directional stateful firewall, deployed on individual virtual machines can provide centralized management of server firewall policy. It should include pre-defined templates for common enterprise server types and enable the following:

- Virtual machine isolation
- Fine-grained filtering (Source and Destination Addresses, Ports)
- Coverage of all IP-based protocols (TCP, UDP, ICMP, …)
- Coverage of all frame types (IP, ARP, …)
- Prevention of Denial of Service (DoS) attacks
- Ability to design policies per network interface
- Detection of reconnaissance scans on cloud computing servers
- Location awareness to enable tightened policy and the flexibility to move the virtual machine from on-premise to cloud resources.

Intrusion Detection and Prevention (IDS/IPS)

As discussed earlier, virtual machines and cloud computing servers use the same hypervisor technology. Deploying intrusion detection and prevention as software on virtual machines shields newly discovered vulnerabilities in these applications and OSs to provide protection against exploits attempting to compromise virtual machines.

Monitoring of critical application and systems

It is imperative to monitor critical operating system and application files (files, directories, registry keys and values, etc.) for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

An integrity monitoring solution should enable:

- On-demand or scheduled detection
- Extensive file and directory level monitoring and PCI-DSS compliance
- Flexible, practical monitoring through includes/excludes
- Reports should be audited

Log Inspection with SIEM tool

Log inspection collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level. Log inspection software on cloud resources enables:

- Suspicious behavior detection
- Collection of security-related administrative actions

- Optimized collection of security events across your datacenter

Vulnerabilities Protection

VMsafe APIs to secure both active and dormant virtual machines. Layered protection uses dedicated scanning virtual machines coordinated with real-time agents within each virtual machine. This ensures that virtual machines are secure when dormant and ready to go with the latest pattern updates whenever activated. Virtualization-aware malware protection can also preserve performance profile of virtual servers by running resource-intensive operations such as full system scans from a separate scanning virtual machine.

- Protection from vulnerabilities as dormant VM machines are more prone towards malware exploitation
- Prevention from spyware, malware, viruses and knowingly or unknowingly installed patch software
- Close integration with virtualization management consoles such as VMware vCenter
- Autodeploy security configuration of new virtual machines

V. FINDING

It is found that most of the service providers are focusing on providing features to customers at less cost but less concerned about security of cloud. Hence, it is imperative to focus on security of cloud alongwith low cost solutions with better deployment which will improve the customer service and enhance efficiency of IT services. However, service providers are not giving complete assurance on security of their products and services. However, it is clearly highlighted the security threat "Given the well-publicized concerns about the potential risks to organizations' sensitive and confidential information in the cloud, we believe it is only a matter of time when users of cloud computing solutions will demand enhanced security features. However, until this happens users of cloud computing should be aware of their responsibility to assess the risks before migrating to the cloud." [16]

Also it is concluded in this study, consumer should be educated of usage of cloud computing applications and well aware of risk and threats if used without proper security checks. In addition to this, the applications which users are going to access should have necessary security checks. Lastly cloud users and providers should give priority to security before cost and features.

References

1. http://www.idc.com/prodserv/idc_cloud.jsp
2. http://en.wikipedia.org/wiki/Cloud_computing
3. http://www.gartner.com/it/page.jsp?id=2163616, STAMFORD, Conn., September 18, 2012
4. http://www.computerworld.in/news/gartner-cloud-services-market-india-surpass-us-326-million-2012-31882012, Computerworld India bureau, 8-oct-2012
5. http://en.wikipedia.org/wiki/Virtualization
6. Managed Virtualization Services(2012), Tulip Telecom Limited.
7. http://en.wikipedia.org/wiki/Cloud_computing
8. IDC Enterprise Panel, 3Q 09
9. The NIST Definition of Cloud Computing". National Institute of Science and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. Retrieved 24 July 2011.
10. Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing". In R. Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms. New York, USA: Wiley Press. pp. 1–44. ISBN 978-0-470-88799-8.
11. A white paper produced by the Cloud Computing Use Case Discussion Group, Version 2.0 30 October 2009, http://groups.google.com/group/cloud-computing-use-cases
12. The Eucalyptus Open-source Cloud-computing System, Page No.3
13. Cloud Computing : Indian Market Perspective, Ravi Pandey, Frost & Sullivan, Page No. 4
14. Sun Cloud Computing, Page No 15
15. Making Virtual Machines Cloud-Ready, A Trend Micro White Paper , August 2009

16. Security of Cloud Computing Providers Study, Sponsored by CA Technologies Independently conducted by Ponemon Institute LLC Publication Date: April 2011, Page No. 16

AUTHOR(S) PROFILE

Pankaj Kumar Kamboj, an MBA graduate and has more than 7 years of experience in security solutioning, consulting and presales for various customers across globe. He is an expert in the area of proposing security strategies & innovation and lead security strategies for vertical. He presently works for HCL Technologies Ltd., Noida, India as Security Presales for Product Management Group.

