A Perspective Analysis of Security Challenges and Performance Enhancement in Could Computing

[1]C. Ravichandiran and [2]Dr. Vaithiyanathan

[1]IT Infrastructure Manager
Zagro Singapore Pte Ltd, 5 Woodlands Terrace, Singapore 738430. ravichinn@gmail.com

[2]Professor and Associate Dean
School of Computing, SASTRA University, Thanjavur, India. vvn@it.sastra.edu

Abstract:

Cloud computing—delivering infrastructure, services, and software on demand via the network—offers attractive advantages to the public sector. It has the potential to reduce information and communications technology (ICT) costs by virtualizing capital assets like disk storage and processing cycles into a readily available, affordable operating expense. Unfortunately, architects more often than not assume that simply adding another server into the mix can fix any performance problem and security issues. Cloud is a platform shuffle that enables a fierce and contentious debate on the issues of security and performance surrounding how to secure information and instantiate trust in an increasingly open and assumed-hostile web operating environment. When you start adding new hardware/update existing hardware in a web cloud, the complexity starts increasing which affects performance and hence security. Here we will define the algorithms to keep both performance and data secure but flexible enough to allow for expandability. In this paper, we have highlighted the following critical issues for the leading Cloud Computing such as Characteristics of cloud computing, threats and performance analysis. This paper specifically discuss about the below-mentioned in detail.

i. Architecture, Service Models, Characteristics of cloud computing, and Deployment Models

ii. Challenges, Obstacles and opportunities of cloud computing

iii. Security Threats

iv. Algorithms of Improve Performance Issues-Equations, and Secure and Efficient Access to Outsourced Data

Keywords: *Cloud Computing, Cloud Infrastructure, Cloud Security, Cloud Platform*

1. INTRODUCTION

Cloud Computing, from becoming a significant technology trend in 2009, there is a wide spread consensus amongst industry observers that it is ready for noticeable deployment in 2011 and is expected to reshape IT processes and IT marketplaces in the next 3 years. The name Cloud computing was inspired by the Cloud symbol that's often used to represent the Internet in flow charts and diagrams. The underlying concept of Cloud computing dates back to 1960 when John McCarthy (an

American computer scientist) opined that, "computation may someday be organized as a public utility." In 1997, the first academic definition was provided by Ramnath K. Chellappa who called it a computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits. In 1999, Salesforce.com applied many technologies developed by companies such as Google and Yahoo! to its own business applications. In the early 2000s, Microsoft extended the concept of SaaS through the development of web services. IBM detailed these concepts in 2001 in the Autonomic Computing Manifesto. Amazon played a key role in the development of Cloud computing by modernizing their data centers after the dot-com bubble. They started providing access to their systems through Amazon Web Services on a utility computing basis in 2005. In 2007, Google, IBM, and a number of universities embarked on a large-scale Cloud computing research project. And, by mid-2008, Gartner Inc, the world's leading IT research & advisory company saw an opportunity for Cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them."

Cloud computing is the collection of virtualized and scalable resources, capable of hosting application and providing required services to the users with the "pay only for use" strategy where the users pay only for the number of service units they consume. A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way.

2. RELATED WORK

Cloud computing is Internet-based computing, whereby shared servers provide resources, software, and data to computers and other devices on demand, as with the electricity grid. Cloud computing is a natural evolution of the widespread adoption of virtualization, Service-oriented architecture and utility computing. Examples include Salesforce.com and Google Apps which provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. Salesforce.com is an easy-to-use Web-based CRM solution for sales, service, marketing, and call center operations that streamlines customer relationship management and boosts customer satisfaction. Google Apps is a collection of Google applications and utilities such as Web-based e-mail, instant messaging, calendar, word processing and spreadsheets. The informative video below shows how cloud computing works and how it can vastly improve the efficiency of your business while lowering technology costs.

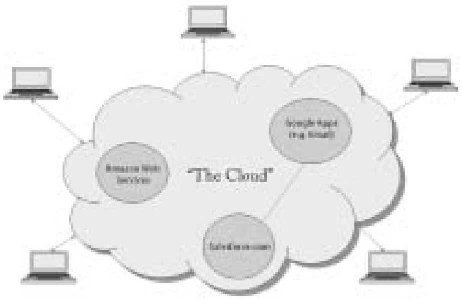

Figure 1: Cloud Computing Architecture

2.1 Service Models

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does 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.

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control 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): The capability provided to the consumer is 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).

2.2 Characteristics of cloud computing

Cloud computing exhibit five essential characteristics defined by NIST (National Institute of Standards and Technology).

On-demand self-service: A consumer can unilaterally provision computing capabilities.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

Resource pooling: The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

2.3 Deployment Models

Private Cloud: The Cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

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, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public Cloud: The Cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

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).

3. OPPORTUNITY AND CHALLENGES

3.1 Advantages of Cloud Computing

The following are some of the major advantages of cloud computing:

Virtualization: Virtualization is defined as decoupling and separation of the business service from the infrastructure needed to run it.

Flexibility to choose vendor

Elasticity: Elastic nature of the infrastructure allows to rapidly allocate and de-allocate massively scalable resources to business services on a demand basis.

Cost Reduction: Reduced costs due to operational efficiencies, and more rapid deployment of new business services.

3.2 Obstacles and opportunities of cloud computing

The following table shows the top ten obstacles and opportunities of cloud computing.

Despite of these obstacles as well as opportunities and advantages, cloud computing raises several security issues and hence security is still the primary concern of many customers who want to leverage public cloud services.

3.3 Security Threats

Top security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are:

i. Abuse and Nefarious Use of Cloud Computing: Abuse and nefarious use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and

Table 1

Obstacles and opportunities of cloud computing

S N	**Problems**	**Opportunities**
1	Availability / Business Continuity	Use Multiple Cloud Providers
2	Performance Unpredictability	Improved VM Support; Flash memory; Gang Schedule VMs
3	Data Confidentiality and Audit ability	Deploy Encryption, VLANs, Firewalls
4	Data Transfer Bottlenecks	FedExing Disks; Higher BW Switches
5	Software Licensing	Pay-for-use licenses
6	Scalable Storage	Invent Scalable Store
7	Reputation Fate Sharing	Offer reputation-guarding services like those for email
8	Scaling Quickly	Invent Auto-Scalar that relies on ML; Snapshots for Conservation
9	Data Lock-In	Standardize APIs; Compatible SW to enable Surge or Hybrid Cloud Computing
10	Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs

use the power of the cloud infrastructure to attack other machines.

ii. Insecure Application Programming Interfaces: As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

iii. Malicious Insiders: The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

iv. Shared Technology Vulnerabilities: Sharing infrastructure is a way of life for IaaS providers. Unfortunately, the components on which this infrastructure is based were not designed for that. To ensure that customers don't thread on each other's "territory", monitoring and strong compartmentalization is required.

v. Data Loss/Leakage: Be it by deletion without a backup, by loss of the encoding key or by unauthorized access, data is always in danger of being lost or stolen. This is one of the top concerns for businesses, because they not only stand to lose their reputation, but are also obligated by law to keep it safe

vi. Account, Service & Traffic Hijacking: Account service and traffic hijacking is another issue that cloud users need to be aware of. These threats range from man-in-the-middle attacks, to phishing and pam campaigns, to denial-of service attacks.

3.4 Security in Cloud computing

Infrastructure Security: The security challenges at various levels namely network level, host level and application level are not specifically caused by cloud computing instead are exacerbated by its use. The issues of infrastructure security and cloud computing can be addressed by clearly defining trust boundaries by understanding which party provides which part of security.

Data Security and Storage: Data security is a significant task, with a lot of complexity. Methods of data protection, such as redaction, truncations, obfuscation, and others, should be viewed with great concern. Not only are there no accepted standards for these alternative methods, but also there are no programs to validate the implementations of whatever could possibly be developed. Homomorphic encryption can be used for data security encryption. But with this approach key management is a problem.

Identity and Access Management (IAM): The key critical success factor to managing identities at cloud providers is to have a robust federated identity management architecture and strategy internal to the organization. Using cloud-based “Identity as a Service” providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with cloud providers.

Security Management: From a security management perspective, a key issue is the lack of enterprise-grade access management features. The scope of security management of cloud services will vary with the service delivery model, provider capabilities, and maturity. Customers will have to make trade-offs with respect to the flexibility and control offered by the SPI services. The more flexible the service, the more control you can exercise on the service, and with that come additional security management responsibilities. In a virtualized environment where infrastructure is shared across multiple tenants, your data is commingled with that of other customers at every phase of the life cycle—during transit, processing, and storage. Hence, it is important to understand the location of the service, service-level guarantees such as inter-node communication, and storage access (read and write) latency.

Privacy: Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. The following tips are recommended for cloud system designers, architects, developers and Testers.

i. Minimize personal information sent to and stored in the cloud.

ii. Protect personal information in the cloud.

iii. Maximize user control.

iv. Allow user choice.

v. Specify and limit the purpose of data usage.

Audit and Compliance: A programmatic approach to monitoring and compliance will help prepare CSPs (Cloud Service Provider) and their users to address emerging requirements and the evolution of cloud business models. To drive efficiency, risk management, and compliance, CSPs need to implement a strong internal control monitoring function coupled with a robust external audit process. To gain comfort over their in-cloud activities, CSP users need to define their control requirements, understand their CSP's internal control monitoring processes, analyze relevant external audit reports, and properly execute their responsibilities as CSP users.

Security-as-a [cloud] Service: Security-as-a-service is likely to see significant future growth for two reasons. First, a continuing shift in information security work from in-house to outsourced will continue. Second, several other information security needs are present for organizations currently, but they will accelerate in need and complexity with the growing adoption of cloud computing. The two proactive controls are important to the growth of cloud computing: identity management that is inter-cloud and scalable to the cloud size, and (encryption) key management. The two reactive controls are needed for audit and compliance purposes as well: scalable and effective SIEM, and data leakage prevention (DLP). Providing solutions to each of these controls will be difficult and requires significant complexity that must be hugely scalable and yet easy to use.

4. PERFORMANCE ANALYSIS

Everybody seems to be talking loud about Cloud Computing nowadays. But the recently reported outages at Salesforce, Amazon and Google has made us think otherwise and wonder if the cloud is really ready to meet all the hype and attention its getting. No doubt, there are cost savings related to licensing, maintenance and application / server management. But does this ensure that your end users are getting the online experience you want them to have?

Many Cloud Computing providers provide custom built management consoles or control panels for managing server resources. These consoles provide customers with availability statistics and status messages in the event of significant outages that impact end users.

4.1 Improve Performance Issues-Equations

The first and foremost thing to keep in mind is that even you are hosting on a Cloud or have a SAAS app running somewhere, your end user expectations are no different then the regular client server application. So in a generic sense User Acceptance Testing is not much different then testing on a Client Server Architecture.

Remember web based application environment in the cloud is a jigsaw puzzle of pieces. At the core you have your virtual hardware followed by your operating system. Each of your servers is then configured differently depending on its specific duty. You may have application servers, web servers, and search servers, database servers etc. Each of these servers needs to be monitored from several points of view - both internally and externally.

Though you don't have direct access to performance monitoring like in a Client Server Architecture but still you can follow following steps to make sure your users are getting the experience you want them to:

```
At interval time $T_i$, construct $IR_i$, as follows-
$IR_i = \{[gid, t] \mid (gid . \{IR\}) \wedge ((T_i - T_{low} * w) < t < Ti)\}$;
Broadcast $IR_i$, $T_{low}$;
Receive $R_{data}$;
For every $id_r . R_{data}$ broadcast $d . D$ {
        Update $Counter_{client}$
        Execute Step B if $T_{th}$ is reached and
        $Counter_{client} > Client_{th-low}$;
        Execute Step C if $T_{th}$ is reached and
        $Counter_{client} > Client_{th-high}$
        }
```

Table 3: Fast Mode (Cloud Performance)

```
At interval time $T_i$, construct $IR_i$, as follows-
$IR_i = \{[d, t] \mid (d . D) \wedge ((T_i - T_{fixed} * w) < t < Ti)\}$;
Send $IR_i$, $T_{fixed}$ point to point;
Execute Step B after $T_{fixed}$ is elapsed;
```

Table 4: Fast Mode (Cloud Performance)

T_{low} : Time interval for the slow mode
T_{high} : Time interval for the fast mode
T_{fixed} : Time interval for the super-fast mode
T_{th} : Threshold time
C_{size} : Cloud size
id_r : id for Resources
gid: group of Resources
D : the set of Resources
IR_i : the set of resource ids
$Client_{th-low}$: the lower threshold number of clients for the cloud
$Client_{th-high}$: the higher threshold number of clients for the cloud
R_{data} : an id list of resources that a client has requested from the cloud
$R_{broadcast}$: an id list of data items that server received in the last IR interval; initialized to the empty
$R_{performance}$: Performance of cloud and timestamp for all resources
S_r : Start Resources
S_t : Stop Resources
Performance : $S_r(n)_t \ldots S_t(n)_t$
$Performance_i$: Performance issue $= S_r(n)_t - S_t(n)_t$

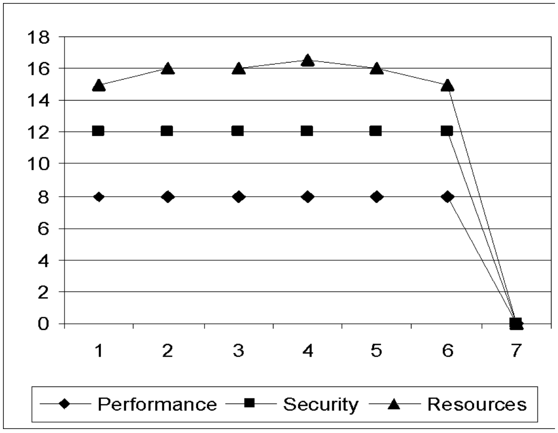

Figure 2: General Graph Performance of a cloud

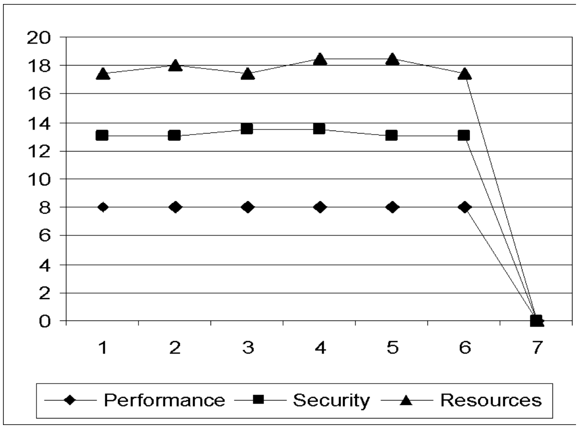

Figure 3: Graph in Slow Mode Performance of a Cloud

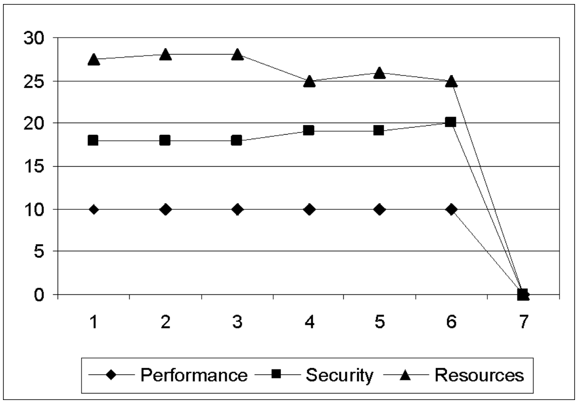

Figure 4: Graph in Fast Mode Performance of a Cloud

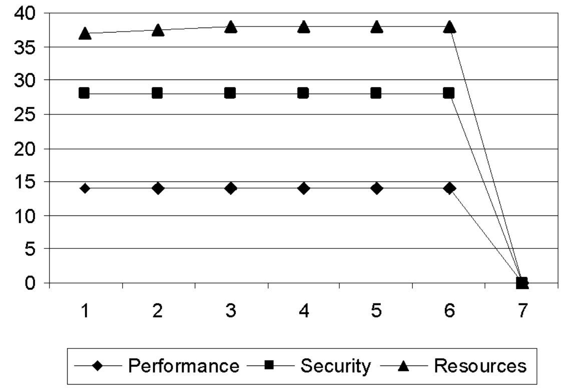

Figure 5: Graph in Super Fast Performance of a Cloud

4.2 Secure and Efficient Access to Outsourced Data

Providing secure and efficient access to outsourced data is an important component of cloud computing and forms the foundation for information management and other operations.

Problem: Figure 6 shows the typical owner-write-userread scenario. Only the owner can make updates to the outsourced data, while the users can read the information according to access rights. Since the data owner stores a large amount of information on the untrusted service provider, the owner has to encrypt the outsourced data before putting on the server. The outsourced data will be accessed by different end users all over the network and hence computationally expensive operations on the data blocks (smallest unit of data) should be avoided and the amount of data stored in the end users must be reduced. Right keys should be provided to the end users to control their access.

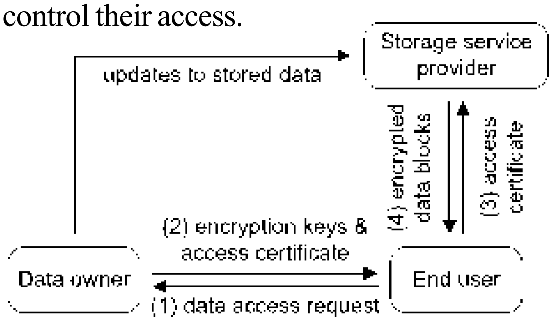

Figure 6: Illustration of application scenario

Solution: Fine-grained access control should be provided for the outsourced data by encrypting every data block with a different symmetric key. (Please refer [17] for key derivation method).

Data Access Procedure:

i. End user U will send a data access request to the data owner O. U -> O: {U, O, EKou , (U, O, request index, data block indexes, MAC code)}

ii. Data owner O authenticates the sender, verify the request and determine the smallest key set O-> U: { U, O, EKou, (O, U, request index, ACM index, seed for P(), K|, cert for S, MAC code)} The cert in the packet is a certificate for the service provider and it has the following format: {EKos, (U, request index, ACM index, seed, indexes of data blocks, MAC code)}

iii. End user U sends {U, S, request index, cert} to the service provider S.

iv. Service Provider S verifies the cert, check the user and ACM index, and retrieve data blocks, and conduct over encryption as follows. Using seed as the initial state of P(), the function will generate a long sequence of pseudo random bits. S will use this bit sequence as one-time pad and conduct the xor operation to the encrypted blocks. The computation results will then be sent to U.

v. End user U receives the data blocks, use seed and K| to derive keys, and then recover the data.

5. CONCLUTION

In conclusion, natural or physical disaster to the datacenter which houses the cloud in hardware form would be the main matter of concern to the company or those involved in the running of the datacenter. On the other hand, regardless of company size or volume and magnitude of the cloud, from the findings discussed within this paper, network or computing downtime is the most detrimental effect to have on the end user. If you have no connectivity to the Internet or from the Internet to the datacenter where the cloud is hosted, you cannot access what you need to and the entire cloud concept is therefore made redundant.

References

1. Siani Pearson. Taking Account of Privacy when Designing Cloud Computing Services. CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pages 44-52. May 2009
2. Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, Peng Ning. Managing security of virtual machine images in a cloud environment. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96. November 2009.
3. Miranda Mowbray, Siani Pearson. A Client-Based Privacy Manager for Cloud Computing. COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middleware . June 2009
4. Foley, M., J., 2008. Microsoft 2.0: How Microsoft Plans to Stay Relevant in the Post-Gates Era. Indianapolis: Wiley.
5. Whittaker, Z., 2008. Egnyte: using and Sustaining Enterprise 2.0 | Enterprise Alley | ZDNet. [Online]. Available at: http://blogs.zdnet.com/enterprisealley/?p=289 [Accessed 6th November 2008].
6. Mills09] Elinor Mills, “Cloud Computing Security Forecast: Clear Skies”,2009 http://news.zdnet.com/2100- 9595_22-264312.html.
7. Flavio Lombardi, Roberto Di Pietro. Transparent Security for Cloud. SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415. March 2010.
8. Weichao Wang, Zhiwei Li, Rodney Owens, Bharat Bhargava. Secure and Efficient Access to Outsourced Data. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, pages 55-65. November 2009
9. Togio, J., W., 2002. Disaster Recovery Planning: Preparing for the Unthinkable. 3rd ed. New York: Prentice Hall.
10. Beard, H., 2008.Cloud Computing Best Practices for Managing and Measuring Processes for On-Demand Computing, Applications and Data Centers in the Cloud with SLA’s. Amazon.com: Emereo.
11. Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina. Controlling Data in the Cloud Outsourcing Computation without Outsourcing Control. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, pages 85-90. November 2009.
12. Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, Sangoh Jeong. Securing Elastic Applications on Mobile Devices for Cloud Computing. CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, pages- 127-134. November 2009.
13. The NIST Definition of Cloud Computing, version 15,by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST),

Information Technology Laboratory (www.csrc.nist.gov)

14. Weiss, A., 2007. Computing in the Clouds, NetWorker, 11(4), pp. 16-25.

15. Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas: 16 November 2008.

16. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. Communications of the ACM , Volume 53 Issue 4, pages 50-58. April 2010.

17. Shilpashree Srinivasamurthy, David Q. Liu, Survey on Cloud Computing Security – Technical Report. Department of Computer Science, Indiana University Purdue University Fort Wayne July 2010.