ADVANCED SECURITY CONCERNS TOWARDS CLOUD COMPUTING

Rashmi Sharma*

Anurag Sharma**

Dr. U.S. Pandey***

ABSTRACT

The Cloud Computing in its initial designing phase, the reason behind it is prompted by technical advancement and it is highly resource dependent that researches in academic Institutions, analysis and experiments are still made. Currently, a comprehensive and general understanding of Cloud Computing refers to the following concepts: - Grid Computing, Utility Computing, software as a service, storage in the cloud and virtualization. These are termed as a client using a provider's service remotely, known as cloud. This paper includes the various types of advanced computing environment like – cloud, grid and utility. The paper gives the brief introduction of grid and utility computing. This paper also cover the advantages and disadvantages in the way of cloud computing. This paper also tackles the important aspect of security concerned challenges which the researchers and authors are facing in the security of cloud computing.

Keywords: *Grid Computing, Utility Computing, IaaS, PaaS, SaaS, Security.*

*Research Scholar, Singhania University.

** Research Scholar, Karnataka State Open University, Karnataka.

***School of Open Learning, Delhi University, Delhi.

1. INTRODUCTION

The Cloud Computing is a latest concept to become popular in computer industry. The basic idea of Cloud Computing is the sharing of computing resources among a community of users. At present cloud computing emerged as a web based technology computing that provides a freedom in the establishment of IT infrastructure. Cloud is basically representing Internet and Web based applications. It basically works on user interactive software which is as simple as Web Browser. The various cloud vendors do not require their own infrastructure rather they can rent or use third party providers

2. WHAT ARE CLOUD, GRID AND UTILITY COMPUTING?

Cloud Computing - The Cloud Computing can be termed as internet based and are connected through the remote servers. Through this sharing of data processing tasks, online access to computer resources or services and centralized data storage. The best examples we give is that electric station, in which consumer use power without having the knowledge of infrastructure to provide the service. In the same manner, the cloud vendors use the resources as a service and pay only for resources that they use. Majority Cloud computing infrastructures includes services delivered through common centers and build on servers.

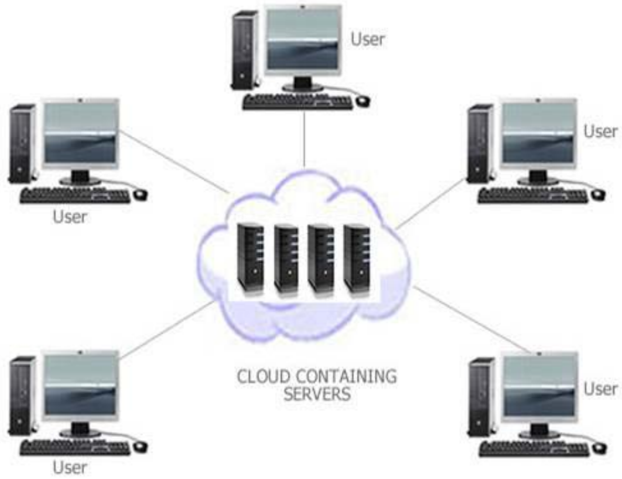

Fig.1 Cloud Containing Servers.

Grid Computing – Grid Computing attaches computers from multiple administrative spheres to reach a common goal for solving a single task. The strategies used by Grid Computing are to use middleware to divide the pieces of program among several computers. It includes computation in a distributed fashion. Grid Computing is providing the resources of many computers in a network to a problem at the same time – to a scientific or technical problem that needs large number of computers processing or ease to access large amount of data.

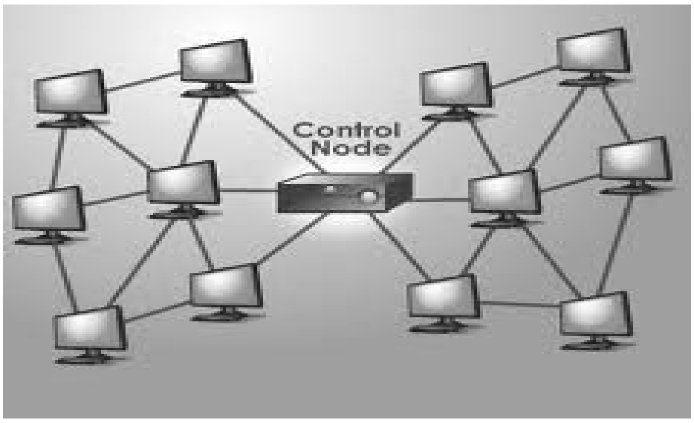

Fig.2 Grid Computing

Utility Computing – Utility Computing is the packaging of computation resources, such as computation, storage and service as a metered service. This model has the benefit of lesser cost to get hold of computer resources. Utility Computing can be same to some extent which has the features of very large computations or a sudden height of demand which are supported by a huge number of computers. Utility Computing is having some features of virtualization so the large amount of storage or computing power is utilized at a single time sharing computers.

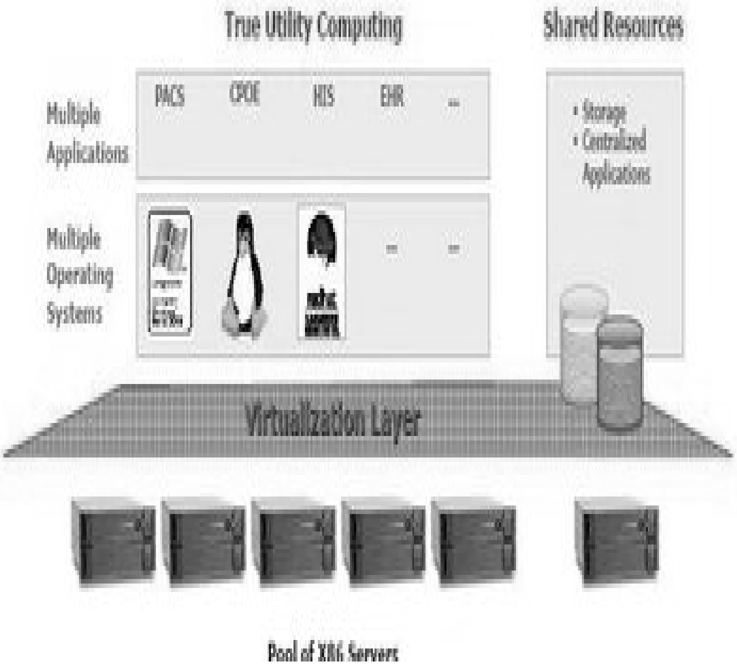

Fig.3 Utility Computing

3. SERVICE MODEL OF CLOUD COMPUTING

Cloud Computing provides both the software and hardware services through or over the Internet. The services are mainly classified into three categories:-

1. **Software – as – a – Service (SaaS)**:- This model is designed to provide everything and easily rent out the software to the user. It allows a user to use the software or application as service on – demand using the Internet.

2. **Infrastructure – as – a – Service(IaaS)**:- It allows a user to use IT infrastructure such as hardware, storage and networking components as a service. The user can access the operating system, storage and application.

3. **Platform – as – a – Service (PaaS)**:- The provider provides a platform for their own use and user.

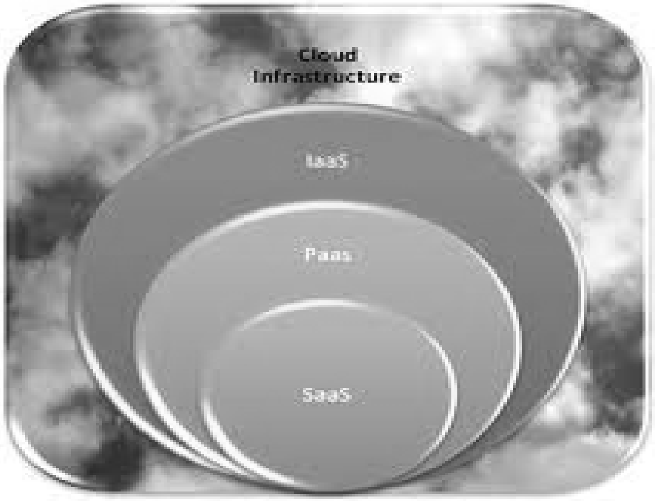

Fig.4 Service model of cloud computing

4. CLOUD COMPUTING MODEL

We divide cloud into various categories according to its features:-

1. **Private Cloud –** In this model, the infrastructure that has been used, and is maintained and operated for a specific company or organization.
2. **Community Cloud –** In this model, the infrastructure is shared among the various companies or organizations with similar areas of interests and requirements.
3. **Public Cloud –** In this model, the infrastructure is available to the public for business purpose by various cloud service providers.
4. **Hybrid Cloud –** In this model, the infrastructure can be the combination of private, public and community that supports the need to keep some information in an organization and also the necessity to offer services in the cloud.

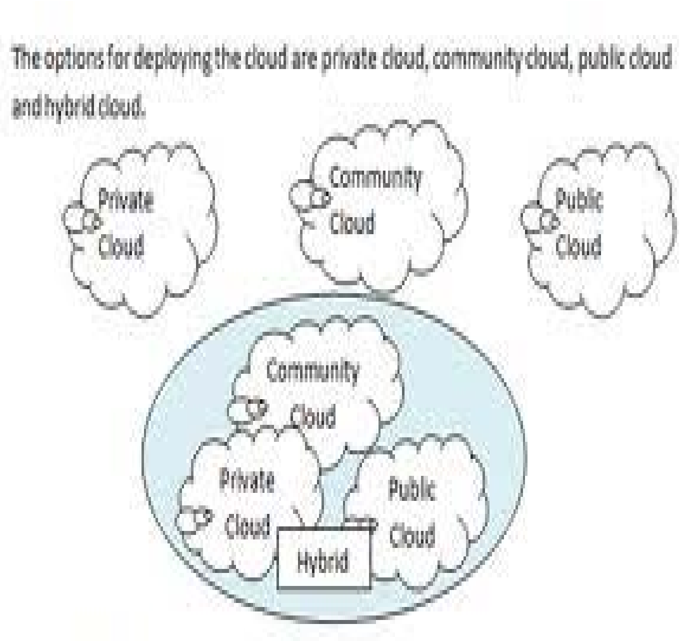
The options for deploying the cloud are private cloud, community cloud, public cloud and hybrid cloud.
Private Cloud
Community Cloud
Public Cloud
Community Cloud
Private Cloud
Public Cloud
Hybrid

Fig.5 Cloud computing model

5. ADVANTAGES OF CLOUD COMPUTING

1. Cost Benefits
2. Flexibility
3. Reliability
4. Maintenance
5. Mobile Accessibility

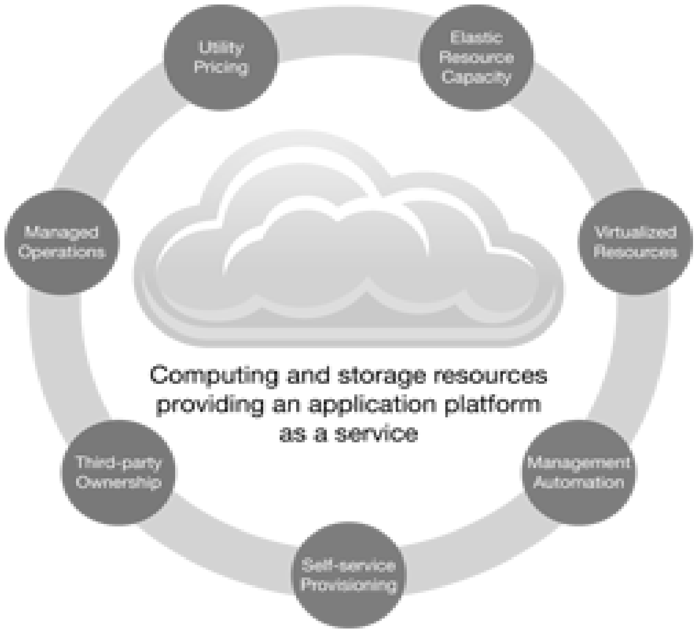
Utility Pricing
Elastic Resource Capacity
Managed Operations
Virtualized Resources
Computing and storage resources providing an application platform as a service
Third-party Ownership
Management Automation
Self-service Provisioning

Fig.6 Cloud computing advantages

6. CHALLENGES OF CLOUD COMPUTING

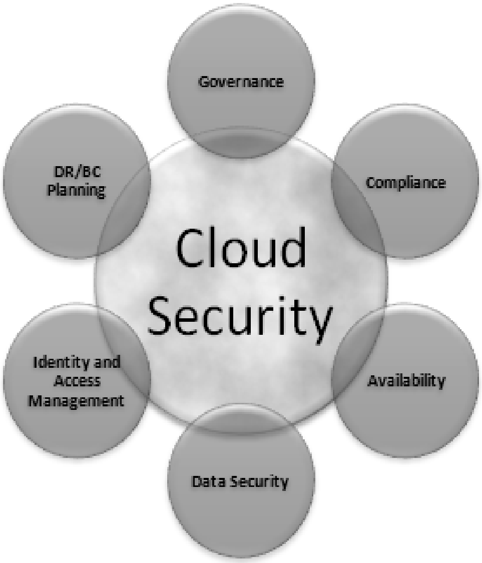

Fig.7 Cloud computing challenges

1. **Data Security –** Security is the main area of concern. A cloud vendor watches the usage of the cloud and the data. The person who is using the cloud doesn’t have the knowledge about the back-end data storage. The user doesn’t have the fair idea where they are storing their data. This can be rectified if vendors can provide a good security or strong firewall and if they adopt encryption facility.

2. **Data Recovery and Availability –** This challenge is faced by the vendors. The vendor should maintain a good recovery system and good maintenance management system.

3. **Management Abilities –** The management of platform and communication are in its starting phase. There is a huge requirement to improve on the scalability and load equal balancing features.

7. CLOUD SECURITY CONCERNS

The major security concerns that needs to be governed when considering critical and sensitive data to public and shared cloud environments. Some of which are:-

i. Where the data stores and who is having authority to use it?

ii. Are your regulatory and audit requirements fulfilled?

iii. Is your data secured from other users?

iv. What happens if there is a security breakage?

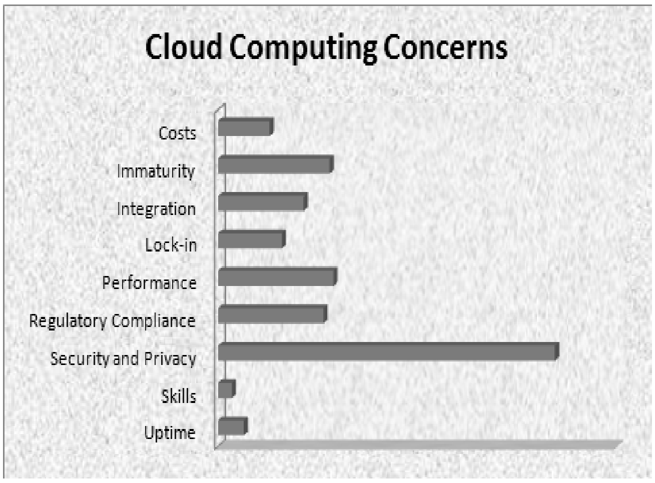

Fig.8 Cloud computing concerns

Security refers to the privacy, reliability and availability, which is a great challenge for cloud vendors.

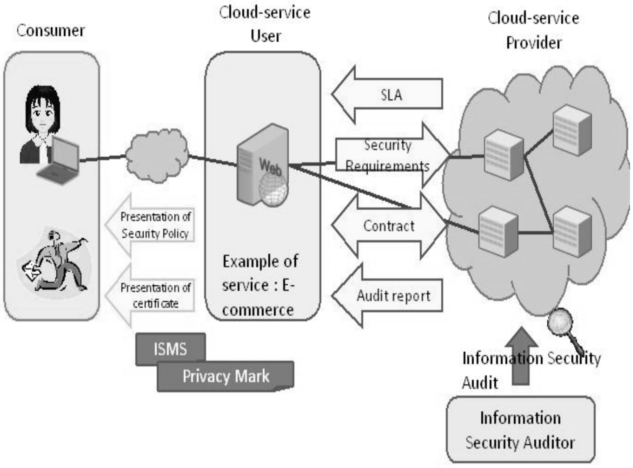
Consumer
Cloud-service User
Cloud-service Provider
SLA
Security Requirements
Contract
Audit report
Presentation of Security Policy
Presentation of certificate
Web
Example of service : E-commerce
ISMS
Privacy Mark
Information Security Audit
Information Security Auditor

Fig.9 Security Challenges in cloud computing

Famous researcher Gartner came out with the following issues:-

1. **Right to Privileged User –** The information transmitted from the client by the Internet poses certain amount of risk, due to the ownership of data, entrepreneur should spend time to know their providers and the rules and regulations.
2. **Regulatory Compliance –** Clients are fully answerable for the security and their solutions, as they can select 3rd party organization audit that keep an eye on all the levels of security.
3. **Data Location –** Based on contracts, some clients might never know what country or what jurisdiction their data is located.
4. **Data Isolation –** Encrypted information from multiple companies may be stored on the same hard disk, hence a method to separate data should be arranged by the vendors.

5. **Recovery –** Every vendor should have a disaster healing procedure to protect their data.
6. **Investigative Hold –** If a client suspects faulty activity from the vendor, it may have legal ways to follow an examination.
7. **Long Term feasibility –** It refers to the ability to retract a contract and all data if the current vendor is taking out by another firm.

CONCLUSION

Cloud Computing is artifact of highly advanced research done for virtualization, distributed computing with usages of software and its related services and also networking. It completely opens a new advanced and secured world of occasions for businesses, but mixed with the offers and high level of security challenges that needs to be definitely considered when society using the advanced cloud computing concepts. In this research paper we are presenting the various hidden security challenges to be precisely and closely monitor. In this paper we also discussed the intrinsic use of virtual systems as a tool for implementing an improved and advanced cloud environment.

FUTURE SCOPE

We closely examined the cloud security environment management problem. Our main target is to improve and enhanced the security procedures and actions

adopted by the cloud vendors. To resolve such problems we need to adopt the following measures: - (1) Capture different vendor’s security necessities from different outlook and different levels of details; (2) Plan security requirements to the cloud architecture, advanced security models and security enforcement apparatus; and (3) Provides the overall feedback about the current advanced security management problems. The various security measures is going to adopt for improving and enhancing the current cloud security model and keeping cloud vendor aware with the overall security status.

REFERENCES

[1]. Integrated Security Framework for Secure Web Services, Z.Wenjun.

[2]. Business Adoption of Cloud Computing . A berdeen Group.

[3]. Government of India portal. [Online] Available http://www.india.gov.in

[4]. Cloud computing-Resource management for effective E-governance – Savita Bhatnagar.

[5]. Pant Durgesh, Sharma M.K ,”Cloud Computing “, CSICommunication-2009,pp10-13,Vol-32,Issue

[6] OWASP.(2010), “The ten most critical Web Application Security Vulnerabilities”

[7]. "The NIST Definition of Cloud Computing" 2009, Peter Mell and Tim Grance

[8] http://thecloudcomputing.org/2009/2/ACM-AD4CLOUD2009.pdf

[9] www.cloudforum.org

[10] www.amazonwebservices.com

[11] http://www.trigyn.com/Default.aspx

[12] http://www.sinlung.com/2011/09/e-governance-gaining-ground-in.html

[13] http://soliver-reflectiveteacher.blogspot.com/

[14] http://t3.gstatic.com/images?q

[15] www.soasymposium.com/home2008.asp

[16].http://blogs.msdn.com/b/ukschools/archive/2011/03/30/what-why-and-how-of-cloud-computing-for-schools.aspx

[17]. http://www.zhen.org/zen20/category/security-compliance/

[18]. http://computer.howstuffworks.com/grid-computing.htm

[19]. http://doctordalai.blogspot.com/2008/08/virtual-servers-and-pacs.html

[20]. http://www.esri.com/technology-topics/cloud-gis/service-models.html

[21]. http://www.techno-pulse.com/2010/04/infrastructure-as-service-iaas-cloud.html

[22]. http://cloudcomputingtechnologybasics. blogspot.com/2011/08/cloud-computing-deployment-models.html

[23]. http://www.jmir.org/2011/3/e67/

[24]. http://www.pixmule.com/cloud-computing/2/

[25]. http://oakleafblog.blogspot.com/2009 /04/windows-azure-and-cloud-computing-posts.html

[26]. http://techgenie.com/softwares/page/13/

[27]. http://www.maintec.com/blog/find-your-way-to-secure-cloud-part-2/

[28].Manish Pokharel and Jong Sou Park, "Cloud Computing Future solution for e-Governance"

[29] Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller

[30]. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.

[31]. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe

[32]. Dot Cloud: The 21st Century Business Platform Built on Cloud Computing Peter Fingar