International Journal of Advances in Engineering Research http://www.ijaer.com

(IJAER) 2012, Vol. No. 4, Issue No. III, September **ISSN: 2231-5152**

A SURVEY OF CLOUD COMPUTING: NETWORK BASED ISSUES PERFORMANCE AND ANALYSIS

***Dr Umesh Sehgal, #Shalini Guleria**

**Associate Professor,ARNI School of Computer Science,Arni University,KathagarhUmeshsehgalind@gmail.com*

#M.Tech student Arni University,Kathgarh shal.aries15@gmail.com

ABSTRACT

Cloud computing is current buzzword in the market. Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Cloud computing has recently experienced a significant increase in popularity as major companies such as Google and Microsoft have started to release cloud based products, advertise the use of the cloud. Cloud computing improves organizations performance by utilizing minimum resources and management support, with a shared network, valuable resources Bandwidth , software's and hardware's in a cost effective manner and limited service provider dealings. Basically it's a new concept of providing virtualized resources to the consumers. Consumers can request a cloud for services, Applications, solutions and can store large amount of data from different location. But due to constantly increase in the popularity of cloud computing there is an ever growing risk of security becoming a main and top issue. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. Current paper presents an elaborated study of IaaS components's security issues in cloud computing.

Keywords: *Cloud computing, Software as a Service (SaaS), Platform as a Service (PaaS) , Infrastructure as a Service (IaaS) , Network issues , Security issues.*

INTRODUCTION

Graphically network of networks i.e. Internet is shown globally as cloud. And cloud computing is referred as applications and services rendered to consumers through internet cloud. It is a paradigm shift that happened rapidly, transferring older computing techniques to a newer one. Hence nowadays internet provides different services to its consumers, and no special device or software is required to use those services.

The advantages of using cloud computing are:

i) reduced hardware and maintenance cost

ii) accessibility around the globe,

iii) flexibility and the highly automated process

Where in the customer need not worry about software up-gradation which tends to be a daily matter.

Private cloud: Private cloud can be owned or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is used by the organizations internally and is for a single organization, anyone within the organization can access the data, services and web applications but users outside the organizations cannot access the cloud. Infrastructure of private cloud is completely managed and corporate data are fully maintained by the organization itself [1].

It is more expensive and secure when compared to public cloud. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, since user's access and the networks used are restricted.

Public Cloud: It is for the general public where resources, web applications, web services are provided over the internet and any user can get the services from the cloud. A cloud infrastructure is provided to many customers and is managed by a third party and exists beyond the company firewall.[2]Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are fully hosted and managed by the cloud provider and fully responsibilities of installation, management, provisioning, and maintenance. Customers are only charged for the resources they use, so under-utilization is eliminated. Since consumers have little control over the infrastructure, processes requiring powerful security and regulatory compliance are not always a good fit for public clouds. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud providers such as Google or Amazon offer an access control to their clients.

Examples of a public cloud include Microsoft Azure, Google App Engine.

Hybrid Cloud: The Cloud is a composition of two or more cloud deployment models(public, private and community), linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider.[2]In this model, a company can outline the goals and needs of services . A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments, as well as those that are secondary to the business, such as employee payroll processing. The major drawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution. Services from different sources must be obtained and provisioned as if they originated from a single location, and interactions between private and public components can make the implementation even more

complicated. These can be private, community or public clouds which are linked by a proprietary or standard technology that provides portability of data and applications among the composing clouds. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security). Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives.[1] It is managed by third party or managed internally .Its cost is lesser then public cloud but more than private cloud.

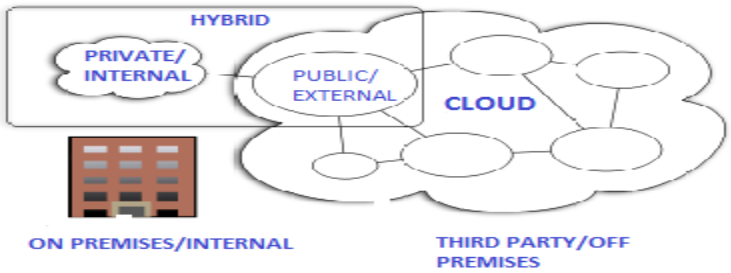

Fig1. Private Internal Hybrid Cloud network

CLOUD COMPUTING NETWORK ISSUES

There are number of network issues occur in cloud computing some of which are discussed below:[2]

Network Sniffing:

It is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party.

Solution for this attack is parties should used encryption methods for securing there data.

Middle Attack:

This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party.

Solution for this attack is SSL should properly install and it should check before communication with other authorized parties.

Port Scanning:

There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly.

Solution for this attack is that firewall is used to secure the data from port attacks.

SQL Injection Attack:

SQL injection attacks are the attacks where a hacker uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an argument value of variable y or 1==1 may cause the return of full table because 1==1is always seems to be true.

Denial of Service:

Denial-of-service attacks are most frequently executed against network connectivity. The goal is to prevent hosts or networks from communicating on the network. In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly.

Solution for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

Cross Site Scripting:

It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials.[1] For example user entered the URL in address bar and attacker redirects the user to hacker site and then he will obtain the sensitive data of the user.

ISSUE OF REUSED IP ADDRESSES:

Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user.

BGP PREFIX HIJACKING:

Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made and hence malicious parties get access to the untraceable IP addresses. On the internet, IP space is associated in blocks and remains under the control of AS's. An autonomous system can broadcast information of an IP contained in its regime to all its neighbors'. These ASs communicate using the Border Gateway Protocol (BGP) model. Sometimes, due to some error, a faulty AS may broadcast wrongly about the IPs associated with it. In such case, the actual traffic gets routed to some IP other than the intended one. Hence, data is leaked or reaches to some other destination that it actually should not.

CONCLUSION

Cloud computing is a new term that is introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In order to keep the Cloud secure, these security threats need to be controlled.

Moreover data residing in the cloud is also prone to a number of threats and various issues like confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. Auditing of the cloud at regular intervals needs to be done to safeguard the cloud against external threats.

This paper described numerous network issues facing cloud computing and their solutions.

There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

REFERENCES

1. Iyer B, Henderson JC (2010). Preparing for the future: understanding the seven capabilities of cloud computing.MIS Q Exec; Vol. 9 No. 2, pp:117-131.
2. Jamil, D., & Zaki, H. (2011a). cloud computing security.