Overcoming Network Security Issues in Cloud Computing and its Applications (A Major Challenge in Cloud Computing Applications)

Naveen Sharma[1,]Dimple Malik[2],Mahesh Kr. Saini[3]
Department of CSE, SITM, Rewari, MD University Rohtak, India[1, 2]
Department of IT, CBPGEC, Jaffarpur, IP University Delhi, India[3]

ABSTRACT

In this modern technologies world everything becomes very vast and more reliable .We makes our documentation on one pc and we can access and get this on other system but this can be happened with the help of internet. The rapid improvement of the capacity of online connectivity gave birth to cloud computing. Data and processes could be done online without the need of any local software or client. As long as the user knows the process and has the right security credentials, he could access the system and make the necessary changes, but there are major challenges and security issues in cloud computing that makes accessing somewhat difficult. In this paper we are giving a introduction to cloud computing and discussing and overcome this security issues that being coming in cloud computing applications.

1. INTRODUCTION

1.1 Cloud Computing

It simply, means "Internet Computing." The Internet is commonly visualized as clouds; hence the term “cloud computing” for computation done through the Internet. With Cloud Computing users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides, databases in cloud are very dynamic and scalable. Cloud computing is unlike grid computing, utility computing, or autonomic computing. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

1.2 Types of cloud computing services

IT people talk about three different kinds of cloud computing, where different services are being provided for you.

Infrastructure as a Service (IaaS) means you're buying access to raw computing hardware over the Net, such as servers or storage. Since you buy what you need and pay-as-you-go, this is often referred to as utility computing. Ordinary web hosting is a simple example of IaaS, you pay a monthly subscription or a per-megabyte/gigabyte fee to have a hosting company serves up files for your website from their servers.

Software as a Service (SaaS) means you use a complete application running on someone else's system. Web-based email and Google Documents are perhaps the best-known examples. Zoho is another well-known SaaS provider offering a variety of office applications online.

Platform as a Service (PaaS) means you develop applications using Web-based tools so they run on systems software and hardware provided by another company. Force.com (from salesforce.com) and the Google App Engine are examples of PaaS.

1.3 Type of clouds:

Public cloud:

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, like applications and storage, available to the general public over the Internet. Cloud services may be free or offered on a pay-per-usage model.

The main benefits of using a public cloud service are:

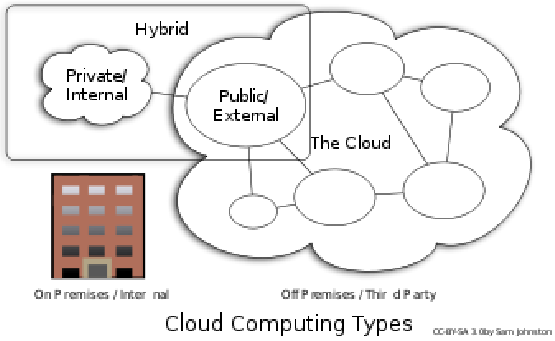
1. Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider.
2. Scalability to meet needs.
3. No wasted resources

Private cloud:

Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall.

Hybrid cloud:

A hybrid cloud environment consisting of multiple internal and/or external providers will be typical for most enterprises. It is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon's Elastic Compute Cloud (EC2) for general computing but store customer data within its own data center.



2. SOLUTION OF SECURITY ISSUES IN CLOUD COMPUTING

As new technologies emerge, they often tend to build on the success of previous developments. Cloud computing and storage, benefit from years of development and testing of large scale infrastructure. The most important take away is cloud storage is for everyone and every organization. From big to small, groups to individual, the use of grid infrastructure can be deployed for maximum return and efficiency. In response, Stone soft has identified five ways IT teams can protect themselves against cloud security threats and attacks, while helping ensure the success of their cloud computing strategies. They include:

2.1 Federated ID

Inherent in a cloud computing environment is the need for workers to log into multiple applications and services. This presents a formidable security pitfall, as organizations may lose control over their ability to ensure strong authentication at the user level. To mitigate this risk, organizations need “single sign-on” capabilities – such as those provided by the Stone Gate SSL VPN – that enable users to access multiple applications and services, including those located outside of the organization in the public cloud, through a single login. With this ability, organizations can streamline security management and ensure strong authentication within the cloud.

2.2 Always-on Connectivity

When the majority of an organization’s critical business data is stored in the cloud, network downtime can shut down business operations. Access to cloud services must be always available, even during maintenance, thus requiring high availability technologies and capabilities such as active clustering, dynamic server load balancing and ISP load balancing within the network infrastructure. Organizations should seek technologies that are built into their network solutions, rather than purchase them as standalone products to ensure effectiveness, ease of management and reduced network costs.

2.3 Multi-layer Inspection

The rise of the cloud computing environment and increased sophistication of threats has created a need for a proper layered defense comprised of perimeter protection and intrusion detection and prevention capabilities within the network. Rather than implementing first-generation firewalls to protect the cloud at the perimeter, Stone soft recommends the deployment of virtual next generation firewall appliances– like the Stone Gate Virtual Next Gen Firewall – that integrate advanced firewall and IPS capabilities for deep traffic inspection. This will allow organizations to inspect all levels of traffic, from basic Web browsing to peer-to-peer applications and encrypted Web traffic in the SSL tunnel. Additional IPS appliances should be implemented to protect networks from internal attacks that threaten access to the cloud.

2.4 Centralized Management:

Human error is still the greatest network security threat facing both physical and virtual computing environments. As companies deploy additional network devices to secure their virtual networks, they exponentially increase this risk as device management, monitoring and configuration become more tedious and less organized. For this reason, Stone soft recommends companies use a single management console to manage, monitor and configure all devices – physical, virtual and third-party.

2.5 Virtual Desktop Protection

More and more organizations are deploying virtual desktops to realize the cost and administration benefits. However, these desktops are just as – if not more – vulnerable than their physical counterparts. To adequately protect virtual desktops, organizations should isolate them from other network segments and implement deep inspection at the network level to prevent both internal and external threats. Those organizations should deploy a multi-pronged approach to security by implementing IPS technology that prevents illegal internal access, protects the clients from malicious servers, as well as providing secure remote access capabilities through IP sec or SSL VPN that protects against unauthorized external access.

2.6 Data storage Location

Cloud compliance is difficult because you do not know where you data are located. Not only does an organization not know what is being done with its data, it may not even know who the providers are. Cloud computing models ignore these problems and make compliance and verification of compliance difficult.

2.7 Security and privacy

First among cloud computing data storage issues is security and privacy In fact, Software as a Services (SaaS) provider may be relying on other external providers for its backbone, infrastructure, and data storage. Cloud vendor uses encryption for securing data at rest and in transit. The cloud service provider should encrypt data on storage devices at all times in order to prevent data breaches. Companies have to make sure that their data is protected when transmitted over the Internet by always being encrypted and authenticated by the cloud provider.

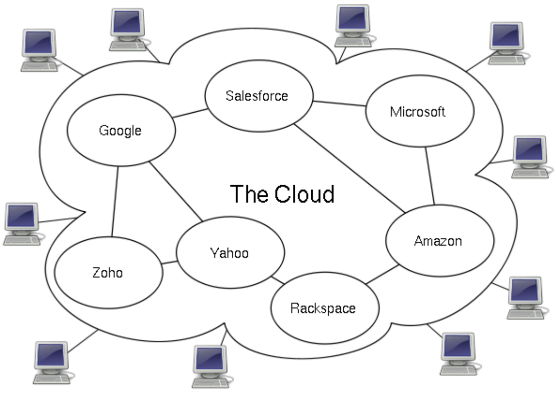
3. CLOUD COMPUTING APPLICATIONS

The applications of cloud computing are practically limitless. With the right middleware, a cloud computing system could execute all the programs a normal computer could run. There are some benefits and applications in cloud computing that makes it different from other concepts:

3.1 Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network.

3.2 It could bring hardware costs down. Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you. Instead, you could buy an inexpensive computer terminal. The terminal could include a monitor, input devices like a keyboard and mouse and just enough processing power to run the middleware necessary to connect to the cloud system. You wouldn't need a large hard drive because you'd store all your information on a remote computer.

3.3 Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of software or software licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company.



3.4 Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end.

3.5 Corporations might save money on IT support. Streamlined hardware would, in theory, have fewer problems than a network of heterogeneous machines and operating systems.

3.6 If the cloud computing system's back end is a grid computing system, then the client could take advantage of the entire network's processing power. Often, scientists and researchers work with calculations so complex that it would take years for individual computers to complete them. On a grid computing system, the client could send the calculation to the cloud for processing. The cloud system would tap into the processing power of all available computers on the back end, significantly speeding up the calculation.

4. Conclusion:

Cloud computing is a better concept because we can access our files, images and anything through the internet, but there are some security issues in using these applications .We have to overcome these security issues and after this we can used any cloud computing applications that’s makes cloud computing better option.

5. REFRENCES

[1] http://blog.animoto.com/2008/04/21/amazon-ceo-jeff-bezos-onanimoto/
[2] searchcloudcomputing.techtarget.com/definition/cloud-computing
[3] www.infoworld.com/.../cloud-computing/what-cloud-computing
[4] “Let it rise – A special report on corporate IT”, The Economist, October 25th, 2008
[5] Jeff Cogswell, “RightScale eases developing on Amazon EC2” eweek.com, October 21st, 2008
[6] Peter Wayner, “Cloud versus cloud – A guided tour of Amazon,
[7] Google, AppNexus and GoGrid”, InfoWorld, July 21, 2008
[8] James Staten, “Is Cloud Computing Ready for the Enterprise?”
[9] Forrester Report, March 7, 2009.