Security Issues In Cloud Computing And Their Solutions

Mr. Vinod K. Lalbeg

Lecturer (Management), NWIMSR, Pune-1

&

Ms. Anjali S. Mulik

Lecturer (Management), NWIMSR, Pune-1

ABSTRACT

Cloud Computing offers many benefits to organizations, such as reduced capital and operating costs and as-needed scalability. So why aren't more businesses taking advantage of the on-demand computing resources services collectively known as 'the cloud'? Security concern is obviously the main concern in deploying the cloud. Although no form of computing is entirely risk-free all the time, cloud computing isn't necessarily any more or less secure than non-virtualized or non-cloud environments. Fortunately, many service providers and others in the cloud computing industry are collaborating to provide ever-greater security, visibility and control to consumers of cloud services. And there are plenty of things enterprises can do to take advantage of cloud computing benefits without compromising security. In the present study, we the researchers have tried to explain cloud computing and its benefits. The researchers also intend to study the security issues and find out what the service providers in the cloud computing industry are doing to overcome the security issues.

Key Words

Cloud, Computing, Software as a Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), interoperability, line-of-business(LOB), portal, mobility, buffer, IP spoofing, RIP attacks, ARP poisoning (spoofing), DNS poisoning.

Background

Cloud computing has evolved through a number of phases which includes grid and utility computing, application service provision (ASP), and Software as a Service (SaaS).

The idea of an "intergalactic computer network" was introduced by J.C.R. Licklider in 1969. Some of the experts believe that the concept of Cloud Computing was contributed by the computer scientist John McCarthy who proposed the idea of computation being delivered as a public utility. But due to limited Internet bandwidth, the idea could not materialize.

One of the first milestones for cloud computing was the arrival of Salesforce.com in 1999, which pioneered the concept of delivering enterprise applications via a simple website. The services firm paved the way for both specialist and mainstream software firms to deliver applications over the internet.

The next development was Amazon Web Services in 2002, which provided a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk.

Then in 2006, Amazon launched its Elastic Compute cloud (EC2) as a commercial web service that allowed small companies and individuals to rent computers on which to run their own computer applications. It was the first widely accessible cloud computing infrastructure service which provided its SaaS online video platform to UK TV stations and newspapers.

Another big milestone came in 2009 with the introduction of Web 2.0, while Google and others started to offer browser-based enterprise applications, though services such as Google Apps. The leading technology giants such as Microsoft and Google contributed to cloud computing by introducing “killer apps”. These companies provided reliable and easy to consume IT services.

Factors like high-speed bandwidth, maturing of virtualisation technology, universal software interoperability standards and slowdown in global economy were the key factors that enabled Cloud Computing to grow across the world.

Introduction:

Definition: Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that’s often used to represent the Internet in flowcharts and diagrams.

There are two types of services namely public and private. A Public Cloud sells services to anyone on the Internet. E.g. Amazon Web Services (EC2). Whereas a Private Cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. e.g. Google (GOOG) – Apps Engine, Salesforce.com (CRM) etc. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

The three categories of Cloud Computing are:

Infrastructure-as-a-Service like Amazon Web Services provides virtual server instances with unique IP addresses and blocks of storage on demand. Customers use the provider’s application program interface (API) to start, stop, access and configure their virtual servers and storage. In the enterprise, cloud computing allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed; it’s also referred to as utility computing.

Platform-as-a-service in the cloud is defined as a set of software and product development tools hosted on the provider’s infrastructure. Developers create applications on the provider’s platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer’s computer. Force.com and GoogleApps are examples of PaaS.

In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS services can be anything from Web-based email to inventory control and database processing. As the service provider hosts both the application and the data, the end user is free to use the service from anywhere.

Objectives

- To study the benefits of Cloud Computing

- To study security issues concerning Cloud Computing
- Finally to highlight steps taken by various service providers to overcome the security issues

BENEFITS OF CLOUD COMPUTING

Cloud Computing offers various benefits that organizations would like to take advantage of. In one of the survey conducted by IDC of 244 IT executives/CIOs and their line-of- business(LOB) colleagues about their companies' use of , and views about IT Cloud Services reveals that the key benefits of Cloud Computing are as follows:

Easy and fast deployment

The slow pace of IT development and deployment of business systems has forced the executives of different companies to approach cloud computing. Service providers like Salesforce, Zoho, Salesboom and CRMForecast are getting huge demands for SaaS CRM software. Thus users see cloud services as an important answer to the need for speed in their business, and consequently in the IT that supports their businesses.

Reduce Cost (improving business economy)

Migrating to a cloud-computing model has rendered significant cost savings for many organizations. Instead of investing in costly infrastructure and building out their own communications room, organizations can outsource that infrastructure to a third-party and manage all of their data and applications from a simple Web address on the Internet. New and smaller scale companies can particularly benefit from this model, as they typically do not have a surplus of upfront capital to invest in their own infrastructures or IT staffs. Organizations can store more data than on private computer systems. This again helps in reducing cost on storage.

Offer latest functionalities

Organizations can take advantage of the latest available technologies and techniques. The latest applications of cloud computing technology includes hosted email, online data backup, software-as-a-service (SaaS), offer built-in disaster recovery functionality and hosted IP based phone service (hosted VoIP).

More mobility

Cloud computing allows users to connect even without their own computers, meaning you can do your work from anywhere in the world as long as you have an internet connection and a computer access. So you can take your work with you where ever you go on vacations. Employees can access information wherever they are, rather than having to remain at their desks.

Allows IT to Shift Focus

No longer having to worry about constant server updates and other computing issues, employees are free to concentrate on innovation and other important activities in their organizations.

Despite of all the above mentioned advantages, customers are still reluctant to venture into it. The reason being various issues like security, lack of control, transparency and performance.

Security threats in Cloud Computing:

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. Some of the security treats in cloud computing are :

Web application vulnerabilities, such as cross-site scripting and sql injection which are symptomatic of poor field input validation, buffer overflow; as well as default configurations or mis-configured applications.

Accessibility vulnerabilities, which are vulnerabilities inherent to the TCP/IP stack and the operating systems, such as denial of service and distributed denial of services.

Authentication of the respondent device or devices. IP spoofing, RIP attacks, ARP poisoning (spoofing), and DNS poisoning are all too common on the Internet. TCP/IP has some "unfixable flaws" such as "trusted machine" status of machines that have been in contact with each other, and tacit assumption that routing tables on routers will not be maliciously altered.

Data Verification, tampering, loss and theft, while on a local machine, while in transit, while at rest at the unknown third-party device, or devices, and during remote back-ups.

Physical access issues, both the issue of an organization's staff not having physical access to the machines storing and processing a data, and the issue of unknown third parties having physical access to the machines.

Privacy and control issues stemming from third parties having physical control of a data is an issue for all outsourced networked applications and storage, but cloud architectures have some specific issues that are distinct from the usual issues. All virtual machines are brought into existence clean, when in reality a compromised hypervisor can spawn compromised VMs, or all VM operating systems are known and available for audit, when in reality the Windows source-code, among others, is not available for audit.

Security Solutions provided by CSA:

Various groups are developing standards and security solution for cloud computing. Cloud Security Alliance (CSA) gathered solution providers, non-profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. The Cloud Standards web site has collected and coordinated information about cloud-related standards.

The Open Web Application Security Project (OWASP) maintains a "top 10" list of vulnerabilities to cloud-based or Software as a Service deployment models which is updated as the threat landscape changes ("OWASP," 2010). The Open Grid Forum publishes documents to containing security and infrastructural specifications and information for grid computing developers and researchers ("Open Grid Forum," 2010).

Web Application Solutions

The best security solution for web applications is to develop a development framework that takes care of authentication, authorization and proper designing.

Accessibility Solutions

Solution to accessibility vulnerabilities is to stop unused services, keep applications and patches updated, and reduce permissions and access rights of applications and users.

Authentication Solutions

To avoid IP spoofing encrypted protocols must be used wherever possible. It is also suggested to avoid ARP poisoning by requiring root access to change ARP tables; using static, rather than dynamic ARP tables; or at least make sure changes to the ARP tables are logged.

Data Verification, Tampering, Loss and Theft Solutions

Resource isolation can help to ensure security of data during processing, by isolating the processor caches in virtual machines, and isolating those virtual caches from the Hypervisor cache.

Privacy and Control Solutions

Allowing a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to a documents if you fail to pay a bill? The issues of privacy and control cannot be solved, but merely assured with tight service-level agreements (SLAs) or by keeping the cloud itself private.

Physical access solutions

One simple solution, which Milne states to be a widely used is to simply use in-house “private clouds”

Conclusion:

After studying the benefits and security issues in Cloud Computing, we noticed that lots need to be still done to make the customers feel the urge of implementing Cloud in their organization. Even though many service providers are available and eager to provide cloud computing, it is very difficult to say whether they will be able to take care of all the problems which are arising in cloud computing. If we search for cloud computing service providers on the Google Search engine we find thousands of service providers with various offers on cloud computing. But the major concern remains whether these service providers really have enough funds, infrastructure, and technical staff to handle the various challenges faced by cloud computing. During the research we found that Cloud Security Alliance (CSA) is working hard to address the various issues / challenges evolved while implementing cloud. We are of the opinion that more researchers should do thorough research and come up with new & innovative solutions to the various challenges faced in Cloud Computing.

References:

1. www.kurzweilai.net
2. www.computerweekly.com
3. www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman
4. www.cloudsecurityalliance.org
5. Document provided by Cloud Security Alliance (CSA) – security best practices for cloud computing – 2009 & CloudStandards – 2010.
6. http://cloud-standards.org