International Journal of Computing Science and Information Technology, **2013, Vol. 01 (01), 29-32**
ISSN: 2278-9669, January 2013 (http://ijcsit.org)

A Survey on Network Security Issues in Cloud Computing

T.John Jeya Singh,
Assistant Professor, Sambhram Academy of Management Studies, Bangalore, India.
Johnjsingh_2001@yahoo.co.in

V. Praveen Kumar
Assistant Professor, Sambhram Academy of Management Studies, Bangalore, India.
praveenkumar_1243@yahoo.co.in

A.Janet Mary
Assistant Professor, St Anne's College, Bangalore, India.
Janu_annes@yahoo.co.in

C.Menaka
Assistant Professor, Faith British Academy, Bangalore, India
Menu_mca_03@yahoo.co.in

Abstract

Cloud computing in a new technology we can use third party facilities and resources as a service to perform out computing needs. Cloud computing can offer a verity of services including hosted services over internet. Cloud computing is a model for enabling convenient on demand network access to a shared pool of configurable computing resources(e.g. Networks, Servers, Storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this paper we discus in detail about cloud computing and its types and network security issues in cloud computing. We gave solution for against cloud network security.

Keywords:: Cloud computing, security, development models, international and industry standards.

1. Introduction

Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make on entry into it. The main advantages of cloud computing are cost saving, high availability and easy scalability[1]. One of the must be very careful to understand the security risks and challenges posed in utilizing these technologies. Network security technology needed in service cloud computing. In this paper we discuss in detail cloud computing its types and cloud computing security issues.

2. Cloud Service Models

2.1. Software as a Service (SaaS)

Employs the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web based email), or a program interface. Example SalesForce CRM is an example of the SaaS provider, Google apps and Zoho.

2.2. Platform as a Service (PaaS)

Consumer created or acquired applications supported by the provider are deployed onto the cloud infrastructure which the provider manages or controls Examples Force.Com, Microsoft Azure and Google App Engine.

2.3. Infrastructure as a Service (IaaS)

The consumer provisions 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. Example Amazon EC2 and S3, Rackspace, AT&T and Verizon.

3. Cloud Deployment Models

3.1. Community Cloud

Shares infrastructure between several organizations from a specific community with common concerns (e.g., security, compliance, jurisdiction), whether managed internally or by a third party and hosted internally or externally.

3.2. Public Cloud

The cloud infrastructure is provisioned by the cloud provider for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.

3.3. Private Cloud

Infrastructure provisioned solely for a single organization, whether managed internally or by a third party and hosted internally or externally.

3.4. Hybrid Cloud

A composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.

4. Characteristics of Cloud

National Institute of Standards and Technology[2], Information Technology Laboratory (NIST) given five Essential Characteristics of Cloud.

4.1. On demand self service

Resources should be always available when you need them, and you have control over turning them on or off to ensure there’s no lack of resource or wastage happen.

4.2. Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

4.3. Resource pooling.

The provider’s computing resources are pooled to serve multiple consumers using a multi tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

4.4. Rapid elasticity.

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

4.5. 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 .e.g. storage, processing, bandwidth, and active user accounts.

5. Network security challenges

Network security is a combination of activities which protect your network usability, reliability, integrity and safety of data. The biggest issues facing computer technology today is data security and the problem has gotten worse because users are working with sensitive information more than often while number of threats is growing and hackers are developing new types of attacks.

All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as secure socket layer (SSL) and the Transport layer security (TLS) for security.

In case of Amazon web services (AWS) it network layer provides significant protection against traditional network security issues, such as MITM (Man-In-The-Middle) attacks. IP spoofing, port scanning, packet sniffing etc. for maximum security Amazon S3 is accessible via SSL encrypted end points.

6. Security industry standards

In this section we explain overview current existing international and industry standards, guidance, and best practices towards security.

The ISO/IEC 27000 series of standards especially ISO/IEC 2700:2005[3] for information security management system (ISMS). ISO/ISE 27002:2005 for developing effective security management practices and ISO/IEC 27005:2011[3] for information security risk management (ISRM) have been developed as general purpose standards.

Another security control based guidance is NIST’s special publication 8000-53R3. As well as NLST’s special publication 800-39 for risk management at the organizational level.

7. Network Issues in cloud computing

There are many different network issues occur in cloud computing, some of the issues are discussed below.

7.1. Phishing attacks

Phishing is a method of online fraud that attempts to acquire sensitive information such as username, passwords, credit card details and other data by masquerading as a trustworthy entity in an electronic communication. Today phishing attacks continue to increase in number and effectiveness. Phishing attacks jumped 37 percent last year and have proven to be exceptionally costly, with the average attack resulting in $4500 in stolen funds.

7.2. Spyware

Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet and transmits the information in the background to a third party. Over the past few years there has been an increase in spyware collecting information about email addresses and even password and credit card numbers.

7.3. A man-in-the-middle (MITM)

A man-in-the-middle attack can be defined as a form of eavesdropping in which the attacker is able to reads insert and modify messages between two parties at will, without either party becoming aware that the link between them has been compromised. MITM attack is also known as monkey-in-the-middle attack or fire brigade attack.

7.4. Denial of service attacks

A dos attack is an attempt to make the services assigned to the authorized users unable to be used by them [5]. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error.

7.5. Hidden field manipulation

While accessing a web page there are fields that are hidden [6] and contain the pages related information and basically used by developers. However, these fields are highly prone to a hacker attack as they can be modified easily and pushed on the web page[7].

7.6. Google hacking

Google hacking refers to using Google search engine to find sensitive information that a hacker can use to his benefit while hacking a users account. A Google hacking[8] event was observed recently when login details of various Gmail users were stolen by a group of hackers in china.

7.7. 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.

8. Solutions for against cloud Security Problems

There are several traditional solutions to mitigate security problems, that exit in the internet environment, as a cloud infrastructure, but nature of cloud causes some security problem that they are especially exit in cloud environment.

- First solution is of finding the right cloud provider.
- Cloud providers can add more resource to protect themselves from attacks.
- The service providers should prove adequate set up and the effectiveness of the firewall.
- Developers should develop the application which providers encrypted data for the security.
- Data backup should be carried out in regular intervals.
- Install trusted Antivirus and spyware, Antivirus Updates must be done without fail
- Never download on unknown antispyware program, avoid Freeware downloads [9].
- .Buy an intrusion detection system[10] .
- Regulating device description downloads based on Router Hops. [11]

9. Conclusion

The past few years cloud computing has grown from being a promising business idea to one of the fastest growing parts of IT. There are various issues that need to be dealt with respect to security and privacy in a cloud computing. Cloud service providers must ensure that all the SLA is meet the human errors. In other hand they are also risk of attacks like powerful DDos Cloud service provider should protect themselves from this type of attacks. In this paper we discussed various network security issues in cloud computing and given suitable solutions.

REFERENCES

[1] R.Maggiani,Communication consultant,solari communication “Cloud computing is changing How we communicate”2009 IEEE International professional conference.Ipcc,pp,1-4,waiki,Hi,USA,July 19-22,2009.

[2] National Institute of Standards and Technology : http://www.nist.gov/index.html

[3] Cloud Computing SUCKS-Cloud Crashes and Insecurity-Privacy Rightshttp://cloudcomputingsucks.com/cloud-technology/cloud-spyware-tool

[4] CloudTweaks, Going Beyond Blocking an attack http://research.cloudtweaks.com/technology/security/anti_spyware

[5] Software Engineering Institute Carnegie Mellon,denial of Service Attacks.www.cert.org/tech_tips/denial_of_service.html

[6] Available from http://www.scribd.com/doc/53420815/51/Hidden-Field-Manipulation-Hidden-Field-Manipulation

[7] Ian Rathie, “An Approach to Application Security,” White Paper, SANS Institute. http://www.sans.org/reading_room/whitepapers/application/approach-application-security_16.

[8] D. Gollmann, “Securing Web Applications,” Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK, DOI: 10.1016/j.istr.2008.02.002.

[9] Tips to stop or Reduce Threats Posted by DDoS,9/14/2011http://brighthub.com/computing/enterprise-security/articles/106930.aspx

[10] Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf

[11] Available from http://support.microsoft.com/kb/315056.aspx

Author Biography

John Jeya Singh.T He is currently working as Assistant Professor in Sambhram Academy of management studies,Bangalore University. His current research includes Neural Network, Cloud computing. He has also published several Technical papers in national conferences.

Praveen Kumar.He is currently working as Assistant Professor in Sambhram Academy of management studies,Bangalore University. His current research includes Cloud computing. He has also published several Technical papers in national conferences.

Janet Mary.A She is currently working as Assistant Professor in St Anne’s College,Bangalore University. Her current research includes, Cloud computing. She has also published several Technical papers in national conferences.

Menaka.C She is currently working as Assistant Professor in Faith British Academy, Bangalore University Her current research includes, Cloud computing. She has also published several Technical papers in national conferences.