ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

Cloud Computing: Network/Security Threats and Counter measures

M. Chandni Jain

Department of Computer Science & Information Technology, K.odaikanal Christian College, Kodaikanal, Dindigul

Abstract: Introducing a new concept of cloud computing in their environment. Cloud computing improves organizations performance by utilizing minimum resources and management support, with a shared network, valuable resources (The NIST Definition of Cloud Computing, 2009), 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. Current paper proposes a backup plan required for overcoming the security issues in cloud computing.

Keywords: Cloud computing, Network issues, Security issues, Counter measures.

1. INTRODUCTION

Cloud computing became "popular" in the presence of other computing techniques used before. The popularity was due to the partnership of IBM and Google to work under a domain followed by the entry of Cloud Computing was a new idea that uses internet and remote servers for maintaining data and applications. It offers through internet dynamic virtualized resources, bandwidth and on-demand software's to consumers and promises the distribution of many economical benefits among its adapters. It helps consumers to reduce the usage of hardware, software license and system maintenance. Hence by using internet consumers are able to use service application on clouds. Moreover by using cloud computing consumers can get benefit in the form of cost, on-demand self-services that reply rapidly, and can access broad network. Current paper discuss in detail cloud computing, its types and Network/security issues related to it. Networks structure faces some attacks that are denial off service attack, man in the middle attack, network sniffing, port scanning, SQL injection attack, cross site scripting. Security Issues that occur in Cloud Computing are XML signature element wrapping, Browser security, cloud malware injection attack, flooding attacks, data protection, insecure or incomplete data deletion, locks in.

2. CLOUD COMPUTING

Many Organizations deal with the storing and retrieving of huge data and cloud computing helps in performing it efficiently with minimum cost, time and maximum flexibility. Besides the benefits associated with the cloud computing, there are different security issues organization has to deal with in order to separate one cloud users data from the other in order to maintain confidentiality/ privacy, reliability and integrity (Bugiel, Nurnberger, Sadeghi, & Schneider, 2011). Moreover as cloud service provider has a complete control on the infrastructure, so security risk like manipulating or stealing of code by service provider exist. 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. A minimum definition containing essential characteristics "Clouds are a large pool of easily and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized service-level Agreements "Cloud computing provides different services rather than a unit of product.

These services put forwarded 3 models:
Software as a service (SAAS), platform as a Service (PAAS), and infrastructure as a Service (IAAS) (Iyer and Henderson, 2010; Han, 2010, Mell and Grance, 2010).

1. *SAAS*— it is run by cloud service provider and mostly used by organizations. It is available to users through internet.
2. *PAAS*— It is a tool (Windows, LINUX) used by developers for developing Websites without installing any software on the system, and can be executed without any administrative expertise.
3. *IAAS*— It is operated, maintained and control by cloud service providers that support various operations like storage, hardware, servers and networking.

There are four types of cloud computing models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud.

1. *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,. Public Organizations helps in providing the infrastructure to execute the public cloud.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

2. *Private Cloud*— 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.
3. *Hybrid Cloud*— The Cloud is a combination of two or more clouds (public, private and community). Basically it is an environment in which multiple internal or external suppliers of cloud services are used. It is being used by most of the organizations (IBM and Junipers Network, 2009).
4. *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. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud.

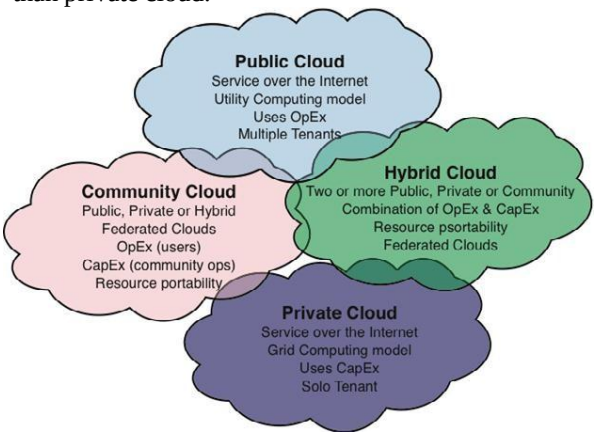

Fig. 1: Types of Cloud Computing

3. NETWORK ISSUES IN CLOUD COMPUTING

There are different network issues occur in cloud computing some of which are discussed below:

3.1 Denial of Service

When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests. For example a hacker hijacks the web server that could stop the functionality of the web server from providing the services. 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. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

3.2 Man in the 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. Counter measure for this attack is SSL should properly install and it should check before communication with other authorized parties.

3.3 Network Sniffing

Another type of attack is network sniffer, 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. Counter measure for this attack is parties should used encryption methods for securing there data.

3.4 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. Counter measure for this attack is that firewall is used to secure the data from port attacks.

3.5 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.

3.6 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. 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. Cross site scripting attacks can provide the way to buffer

Overflows, DOS attacks and inserting spiteful software in to the web browsers for violation of user's

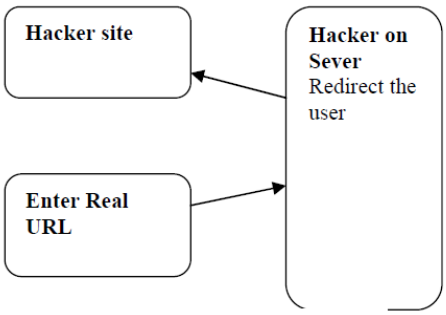

Fig. 2: Cross Site Scripting

4. SECURITY ISSUES IN CLOUD COMPUTING

XML Signature Element Wrapping— XML signature Element Wrapping is the fine renowned attack for web service. It is use to defend a component name, attribute and value from illegal party but unable to protect the position in the documents. Attacker targets the component by operating the SOAP messages and putting anything that attacker like. Counter measure for this attack is using the digital certificate e.g. X.509 authorized by third party such as

Certificate authorities and also uses the mixture of WS-security with XML signature to a particular component. XML

Should have the list of components so that it can reject the messages which have malicious file and also reject the unexpected messages from the client.

Browser Security— The second issue is Browser Security. As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user.SSL support point to point communication means if there is third party, intermediary host can decrypt the data. If hacker installs sniffing packages on intermediary host, the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user. Counter measure for this attack is Vendor should use WS-security concept on web browsers because WS-security works in message level that use XML encryption for continuous encryption of SOAP messages which does not have to be decrypted at mediator hosts.

Cloud Malware Injection Attack— The third issue is Cloud Malware Injection Attack, which tries to damage a spiteful service, application or virtual machine. An interloper is obligatory to generate his personal spiteful application, service or virtual machine request and put it into the cloud structure. Once the spiteful software is entered into the cloud structure, the attacker care for the spiteful software as legitimate request. If successful user ask for the spiteful service then malicious is implemented. Attacker upload virus program in to the cloud structure. Once cloud structure care for as a legitimate service the virus is implemented which spoils the cloud structure. In this case hardware damages and attacker aim is to damage the user. Once user asks for the spiteful program request the cloud throws the virus to the client over the internet. The client machine is infected by virus. Counter measure for this attack is authenticity check for received messages. Store the original image file of the request by using hash function and compare it with the hash value of all upcoming service requests. In this way attacker create a legitimate hash value to deal with cloud system or to enter into the cloud system.

Data Protection— Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behavior of the cloud supplier and as a result he is confident that data is handled in a legal way, but it does not like that this problem is intensify in case of various transformation of data**.** Counter measure for this attack is that a consumer of cloud computing should check data handle either it is handled lawfully or not.

Incomplete Data Deletion— Incomplete data deletion is too much risky in cloud computing, it does not remove completed data because replica's of data is placed in other servers for example When a client request to remove a cloud resource then with most operating systems this will not remove accurately. Accurate data deletion is not possible because copies of data are stored in the nearest replica but are not available. Counter measure is that Virtualized private networks should use for securing the data and used the query that will remove the complete data from the main servers along with its replica's.

Locks in— Another issue is locks in; at this time there is a small tender in the manner of tools, standard data format or procedures, services edge that could undertake data, application and service portability. This will not enable the customer to shift from one cloud provider to another or shift the services back to home IT location.

5. 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. Some security issues and their counter measures are discussed in this paper. It has several models to protect its data for the business users. An organization used private clouds within its organization to prevent from loss of data. Cloud computing have several deployment models that help in retrieving the information. SAAS, PAAS, IAAS are the three models for cloud computing. Security in cloud computing consist of security abilities of web browsers and web service structure.

REFERENCES

[1] Bugiel, S., Nurnberger, S., Sadeghi, A.-R., & Schneider, T. (2011). Twin Clouds: An Architecture for Secure Cloud Computing. Workshop on Cryptography and Security in Clouds . Zurich.

[2] Cloud Security Alliance (2010). Top threats to cloud computing, version 1.0.

[3] Foster, I., & Kesselman, C. (1998). The Grid: Blueprint for a New Computing Infrastructure (The Elsevier Series in Grid Computing). Morgan Kaufmann. Han Y (2010). On the clouds: a new way of computing. Inf Technol Libr, Vol. 29 No. 2, pp: 87-92.

[4] 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.

[5] Jamil, D., & Zaki, H. (2011a). cloud computing security. International Journal of Engineering Science and Technology (IJEST) , Vol.3 No.4, 3478-3483.

[6] Jensen, M. (2009, September). On Technical Security Issues in Cloud Computing. IEEE International Conference in Cloud Conouting , 109-116.

[7] Peter Mell and Tim Grance, (2009)The NIST Definition of Cloud Computing, version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).

[8] Ren, K., & Lou, W. (2009). Ensuring Data Storage Security in Cloud Computing. Retrieved from http://www.ece.iit.edu/~ubisec/IWQoS09.pdf

[9] Scarfone K, S. A. (2007). Guide to Secure Web Services. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

[10] Services, A. W. (2009, April). Amazon Virtual private Cloud. Retrieved from http://aws.amazon.com/vpc/