ZIBELINE INTERNATIONAL PUBLISHING

ISSN: 2590-4043 (Online)
CODEN: AEMCDV

Acta Electronica Malaysia (AEM)

DOI: http://doi.org/10.26480/aem.01.2022.01.03

CrossMark

RESEARCH ARTICLE

NETWORK/SECURITY THREATS AND COUNTERMEASURES FOR CLOUD COMPUTING

Rajesh De, Ipseeta Nanda*

Faculty of Information Technology, Gopal Narayan Singh University, Jamuhar, Sasaram, Bihar-821305, India
**Corresponding Author Email: ipseeta.nanda@gmail.com*

ARTICLE DETAILS

Article History:

Received 10 September 2022
Revised 13 October 2022
Accepted 19 November 2022
Available online 23 November 2022

ABSTRACT

Small and medium-sized enterprises are now aiming to adopt a cost-effective computing resource for their business applications, i.e. by using the novel idea of cloud computing in their environment, in addition to major corporations. Utilizing less resources and management support, a shared network, valuable resources, bandwidth, software, and hardware in a cost-effective manner, and fewer service provider interactions, cloud computing enhances the performance of companies. In essence, it's a novel idea for giving consumers access to virtualized resources. Customers can use the cloud to store a lot of data from several locations and request services, applications, and solutions. But as cloud computing's popularity grows, there is a growing danger that security will overtake other concerns as the primary one. The current article suggests a backup strategy needed to address cloud computing security concerns.

KEYWORDS

Countermeasures, Network concerns, Security issues, and Cloud computing

1. INTRODUCTION

In contrast to earlier computing methods, cloud computing "became mainstream" in October 2007. (Wikipedia, 2012 a; Foster and Kesselman, 1998; Raleigh and Armonk, 2007; Naone, 2007; Reimer, 2007). The cooperation between IBM and Google to operate under a domain (Lohr., 2007; View et al., 2007) and the subsequent entry of (Wikipedia, 2012b; Vouk, 2008). A novel concept called "cloud computing" makes use of the internet and distant servers to maintain data and applications. It provides bandwidth, dynamic virtualized resources, and on- demand software to customers via the internet and assures the distribution of numerous financial advantages to its adapters. Customers benefit from reduced hardware, software license, and system maintenance usage. Therefore, users can use service applications on clouds simply accessing the internet (Ren and Lou, 2009). Additionally, customers can profit from cloud computing in terms of cost, on- demand self-services that respond quickly, and access to a large network.

The sorts of cloud computing and network/security challenges that are related to them are covered in detail in the current study. Denial-of-service attacks, man-in- the-middle attacks, network sniffing, port scanning, SQL injection attacks, and cross- site scripting are some of the threats that networks encounter. XML signature element wrapping, browser security, cloud malware injection assaults, flooding attacks, data protection, unsecure or incomplete data erasure, and locks-in are security issues that can arise with cloud computing.

2. CLOUD COMPUTING

Many businesses deal with the storage and retrieval of enormous amounts of data, and cloud computing makes it possible to do so effectively while spending the least amount of money, time, and flexibility possible. In addition to the advantages of cloud computing, organisations must address a variety of security concerns in order to segregate the data of one cloud user from that of another and maintain confidentiality, privacy, and integrity (Bugiel, Nurnberger, Sadeghi, and Schneider, 2011). Additionally, because the cloud service provider has complete control over the infrastructure, there is a security risk that the provider could manipulate or steal code (Cloud Security Alliance, 2010).

In terms of graphics, a network of networks is The world wide web appears as a cloud. Applications and services delivered to customers via the internet cloud are known as cloud computing. It was a paradigm change that occurred quickly, moving previous computing methods to a more modern one. As a result, the internet currently offers a variety of services to its users without the need for any specialised hardware or software. (Vaquero et al., 2009) developed a minimum definition with the following criteria after looking at 20 definitions.

Clouds are a sizable collection of readily available virtualized resources (including hardware, platforms for software development, and/or services). To adapt to a changing demand (scaling), these resources can be dynamically reconfigured, which also allows for optimal resource use. This resource pool is often used in a pay- per-use fashion, with the infrastructure provider providing guarantees through specialised service-level agreements.

Instead of offering a single product, cloud computing offers a variety of services. Three models were introduced by these services: infrastructure as a service (IAAS), platform as a service (PAAS), and software as a service (SAAS) (Iyer and Henderson, 2010; Han, 2010; Mell and Grance, 2010).

SAAS: it is primarily utilised by businesses and is operated by cloud service providers. Users can access it via the internet.

PAAS: -Without installing any software on the system, developers can create websites with the help of the PAAS tool (Windows, LINUX), which can be used without any administrative experience.

Quick Response Code	Access this article online	
	Website: www.actaelectronicamalaysia.com	**DOI:** 10.26480/aem.01.2022.01.03

Cite the Article: Rajesh De, Ipseeta Nanda (2022). Network/Security Threats and Countermeasures for Cloud Computing. *Acta Electronica Malaysia, 6(1): 01-03.*

IAAS: Cloud service providers that support various operations including storage, hardware, servers, and networking are in charge of operating, maintaining, and controlling it.

NIST (2009) recognised four different cloud computing model types: community cloud, hybrid cloud, private cloud, and public cloud.

1. The term "public cloud" refers to a cloud that is accessible to the general public and where resources, web services, and applications are made available online.

Public organisations contribute to supplying the necessary infrastructure for running the public cloud.

1. Any employee within the company can access the data, services, and web apps, but users from outside the company are unable to access the private cloud, which is utilised by businesses internally and is just for a single organisation. The firm itself fully manages the infrastructure of the private cloud and fully maintains the business data.
2. A hybrid cloud is made up of two or more different types of clouds (public, private and community). In essence, it is a setting where numerous internal or external cloud suppliers are present.

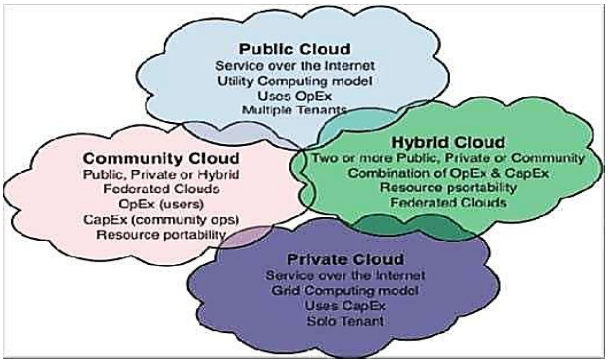

Figure 1: Different Cloud Computing Models

1. The cloud is essentially a combination of one or more public, private, or hybrid clouds that are used by numerous organisations for a single purpose (most often security). Infrastructure is shared by numerous organisations within a particular community with a common focus on security and compliance. It is either internally maintained or administered by a third party. Its cost is higher than private cloud but lower than public cloud.

3. Cloud Computing Network Issues

In cloud computing, a variety of network challenges can arise, some of which are covered below:

3.1 Denying Service

When hackers repeatedly request services from a network server or web server to harm the network, denial of service cannot keep up with them, and the server is unable to process regular client requests. For instance, if a hacker takes over a web server, the web server's ability to deliver services may be interrupted. In cloud computing, hackers attack the server by flooding it with thousands of requests, preventing it from responding to regular clients and causing the system to malfunction. Reduce the privileges of the user who connects to a server as a defence against this attack. The DOS attack will be lessened as a result. (Scarfone, 2007)

3.2 Man in the Middle Attack

If secure socket layer (SSL) is not properly setup, this is another security-related problem that may arise in a network. For instance, if two parties are corresponding with one another and SSL is improperly setup, the intermediary party could intercept all of the data exchanged between the two sides. SSL should be installed correctly and tested before communicating with other permitted parties as a defence against this attack.

3.3 Sniffing the Network

Network sniffer is a different kind of attack that poses a more serious threat to network security since it allows for the hacking of unencrypted data over the network, such as passwords that are not securely encrypted during communication. The data can be intercepted during transmission if the communication parties do not utilise encryption mechanisms to protect the data. To defend against this attack, parties should secure their data using encryption techniques.

3.4 Scanning of Ports

Due to the fact that Port 80 (HTTP), which is used to deliver online services to the user, is constantly open, there may be certain concerns with port scanning that might be leveraged by an attacker. Other ports, like 21 (FTP), are only opened when necessary, therefore until and until the server software is properly configured, ports should be secured by encryption. Firewalls are used to protect the data from port attacks as a defence against this attack. (Services, 2009)

3.5 Attack using SQL Injection:

Attacks known as "SQL Injection" occur when hackers utilise special characters to retrieve data, such as when SQL programming results in a where clause that can be changed by inserting more information. Since 1==1 always seems to be true, for instance, a variable y argument value or 1==1 may result in the return of the entire table.

3.6 Site-to-Site Scripting

When a user enters the correct URL for a website, a hacker on the other site can reroute them to their own website and steal their login information. For instance, once the user entered the URL in the address bar, the attacker redirected them to a hacker website, where he subsequently obtained the victim's sensitive information. Cross- site scripting attacks can lead to buffer overflows, denial-of-service attacks, and the insertion of malicious software into web browsers in order to violate user credentials. (Yang, 2003)

4. Cloud Computing Security Issues

The following is a discussion of cloud computing security issues:

4.1 Wrapping an XML Signature Element

The excellent and well-known attack for web services is element wrapping for XML signatures. It is used to protect a component's name, attribute, and value from unauthorised parties, but it cannot safeguard the location in the documents. (Jamil and Zaki, 2011b) The attacker manipulates the SOAP messages and inserts anything the attacker desires in order to target the component. The digital certificate, for example, can be used as a defence against this assault. A specific component uses X.509 that has been approved by a third party, such as certificate authorities, as well as a combination of WS-security and XML signature. To be able to reject messages including harmful files as well as unexpected messages from the client, XML has to provide a list of components.

4.2 Browser Safety

Browser security is the second problem. When a client uses a web browser to send a request to a server, the browser must use SSL to encrypt the user's credentials in order to verify their identity. Since SSL only supports point-to-point connection, any intermediary hosts can decrypt the data. The attacker may obtain the user's credentials and use them in the cloud system as a legitimate user if the hacker instals sniffing packages on the intermediary host. (Jensen, 2009) As a defence against this attack, vendors could make use of the WS-security concept on web browsers. WS-security operates at the message level, using XML encryption to continuously encrypt SOAP messages so that mediator hosts are not required to decrypt them.

4.3 Attack via Cloud Malware Injection

The third problem is a cloud malware injection attack that seeks to harm a specific service, application, or virtual machine. It is mandatory for an intruder to create his or her own vindictive application, service, or virtual machine request and submit it to the cloud infrastructure (Booth, 2004). As soon as the malicious software is added to the cloud infrastructure, the attacker treats it as a genuine request. If a successful user requests a vindictive service, hostile behaviour is put into practise. Attackers install malicious software to the cloud infrastructure. As soon as cloud structure maintenance is provided as a legitimate service, a virus is introduced and destroys the cloud structure. In this instance, hardware is harmed, and the attacker's goal is to harm the user. When a user requests a vindictive programme, a cloud sends the virus to the client via the internet. The client computer has a virus infection. The attack's defence is the authenticity verification of communications that are received. Utilizing the hash function, save the original picture file from the request, then compare it to the hash value of each subsequent service request. Attackers can deal with cloud systems or gain access to the cloud systems in this way by creating a genuine hash value.

4.4 Flooding Assaults

Attack from flooding is the fourth problem. Attacker openly targets the cloud system. The provision of highly scalable resources is the cloud system's most important characteristic. When there are additional requests from clients, cloud systems constantly expand to accommodate them by initiating fresh service requests. A flooding attack generally involves sending a lot of pointless requests to a specific service. When an attacker makes several requests, the cloud system will try to block them by adding more resources, but eventually it will run out of resources and be unable to respond to user requests that are more typical in nature. Attackers then target the service server. DOS assaults result in additional payments for the consumer when using resources. The provider of the service is required to make additional compensation due to an unforeseen circumstance. It's difficult to stop Dos Attacks, which is a defence against this attack. An intrusion detection system will filter malicious requests and establish a firewall to prevent attacks on the server. A phoney alarm may occasionally be sent by an intrusion detection system, misleading the administrator.

4.5 Privacy Protection

Although it may be challenging for a cloud customer to effectively monitor the cloud provider's actions, he may be confident that data is handled legally as a consequence. However, it is unfortunate that this issue is made worse in the event of different data transformations. The defence against this attack is for cloud computing users to verify if data handling is done legally or not.

4.6 Missing Data Removal

In cloud computing, incomplete data deletion is too unsafe since it does not erase completed data because copies of the data are stored on other servers. For instance, when a client requests to remove a cloud resource, most operating systems will not accurately remove the resource. Because copies of the data are kept in the closest replica but are not accessible, accurate data erasure is not possible. (Jamil and Zaki, 2011a) A countermeasure is to utilise virtual private networks to secure the data and to use a query that deletes all of the data from the primary servers and all of its replicas.

4.7 Locks In

Another problem is locks; at the moment, there is a limited supply of tools, techniques, or standard data formats or services that might handle data, application, and service portability. This prevents the consumer from switching cloud providers or returning the services to their home IT location. (Catteddu, 2010)

5. Conclusion

A new concept called "cloud computing" has entered the business world, allowing users to communicate directly with virtualized resources while saving customers money. This paper discusses a few security concerns and the solutions to them. It uses a variety of models to safeguard users who are businesses. In order to prevent data loss, an organisation deployed private clouds internally. There are various deployment strategies available in cloud computing that aid in information retrieval. The three models for cloud computing are SAAS, PAAS, and IAAS. Security in cloud computing includes web browser security features and web service architecture.

References

Booth, D. 2004. Web service architecture. Retrieved from http://www.w3.org: http://www.w3.org/TR/ws-arch/wsa.pdf

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

Catteddu, D. 2010. Cloud Computing. Retrieved from http://www.enisa.europa.eu/act/rm/files/de liverables/cloud-computingrisk-assessment Cloud Security Alliance (2010). Top threats to cloud computing, version 1.0.

Cloud Security Alliance. 2010. Top Threats to Cloud Computing V1.0. Cloud Security Alliance (CSA).

Foster, I., and Kesselman, C. 1998. The Grid: Blueprint for a New Computing Infrastructure (The Elsevier Series in Grid Computing). Morgan Kaufmann. http://www .cloudsecurityalliance.org/topth reats/csathreats.v1.0.pdf.

Han Y. 2010. On the clouds: a new way of computing. Inf Technol Libr, Vol. 29 No. 2, pp: 87-92.

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.

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

Jamil, D., and Zaki, H. 2011b. Security Issues In Cloud Computing And Counter Measures. International Journal of Engineering Science and Technology (IJEST) , Vol. 3 No. 4, 2672-2676. Jensen, M. 2009. On Technical Security Issues in Cloud Computing. IEEE International Conference in Cloud Computing, 109-116.

Lohr, S. 2007. Google and I.B.M. Join in 'Cloud Computing' Research. Retrieved 1 28, 2012, from The Newyork Times: http://www.nytimes.com/2007/10/08/techn ology/08cloud.html

Mell P, Grance T. 2010. The NIST definition of cloud computing. Commun ACM; Vol. 53 No. 6, pp:50. NAONE, E (2007, September 18). Computer in the Cloud. Retirived 1 24, 2012, from Technology Review, MIT: http://www.technologyreview.com/printerfriendly article.aspx?id=19397

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).

Raleigh, NC and Armonk, NY. 2007. North Carolina State University and IBM help bridge digital divide in North Carolina and beyond. Retrieved 1 27,2012, from IBM: http://www-03.ibm.com/press/us/en/pressrelease/21506.wss

Reimer, J. 2007. Dreaming in the "Cloud" with the XIOS web operating system. Retrieved 1 24, 2012, from ars technical: http://arstechnica.com/news.ars/post/20070408-dreaming-in-the-cloud-with-the- xios-web-operating-system.html

Ren, K., and Lou, W. 2009. Ensuring Data Storage Security in Cloud Computing. Retrieved from http://www.ece.iit.edu/~ubisec/IWQoS09.pdf

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

Services, A. W. 2009. Amazon Virtual private Cloud. Retrieved from http://aws.amazon. com/vpc/Vaquero .

LM, Rodero-Merino L, Caceres J, Lindner M. 2009. A break in the clouds: towards a cloud definition. ACM SIGCOMM Comput Commun, Vol. 39 No. 1, pp:50-55. View, M. Calif and Armonk. (2007, October 8). Google and IBM Announced University Initiative to Address Internet-Scale Computing Challenges. Retrieved 1 28, 2012, from IBM: http://www-03.ibm.com /press/us/en/pressrelease/22414.wss

View, M. Calif and Armonk. 2007. Google and IBM Announced University Initiative to Address Internet-Scale Computing Challenges. Retrieved 1 28, 2012, from IBM: http://www-03.ibm.com/press/us/en/pressrelease/22414.wss

Vouk, M. 2008. Cloud Computing-Issues, Research and Implication. Journal of Computing and Information Technology - CIT, Vol. 16, no.4, pp. 235–246.

Wikipedia. 2012a. Amazon Elastic Compute Cloud. Retrieved 1, 27, 2012, from Wikimedia Foundation Inc. http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud.

Wikipedia. 2012b. Cloud Computing Retrieved 1, 28, 2012, from Wikimedia Foundation Inc. http://en.wikipedia.org/wiki/Cloud_computing

Yang, A. 2003. Guide to XML Web Services Security. Retrieved from http://www.cgisecurity .com/ws/WestbridgeGuideToWebServicesSecurity.pdf