IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Survey on Security Threats in Cloud Computing

P. Anusha[1*], R. Maruthi[2]

[1,2]Department of Computer Science, PRIST University, India

Corresponding Author: rmaruthi2014@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—** Cloud computing, also referred to as 'on demand computing', is a recent concept making waves in the IT industry. When compared to other specific, dedicated infrastructures in computing, cloud concept gives the advantage of reliability, quantifiability, cost- effectiveness and improved performance. It is easy and convenient to have network access to other shared configurable computing resources using this concept. Another advantage of the concept is that the resources can be utilized with increasing efficiency and minimum overhead efforts. Clouds can be used for services, solutions, and applications and also for storing large amount of data in different locations. Data is stored over a set of resources which are networked so that the data can be accessed through any other virtual system. The security and privacy issues associated with data management is reduced considerably using the cloud computing facility as the data centers are literally beyond the reach and control of users. Further, server breakdowns which normally affect data storage and use does not seem to affect the user in cloud computing. But this system has its own set of disadvantages. This work is an attempt 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.

***Keywords*—** Cloud Computing, Data Integrity, Data storage, Security, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Interoperability, Denial of Service (DoS).

I. INTRODUCTION

Cloud Computing, the event and use of computing resources over a network, became very hip with new trends increasing its applications. Cloud computing reduces the value of maintenance and hardware whereas providing accessibility all round the world. This can be an automatic method that offers extensive flexibility to the user and eliminates the requirement for periodic computer code up-gradation. [1, 2].A number of definitions are in use for this new construct, Cloud computing. it's outlined as "a model for enabling present, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) which will be quickly provisioned and discharged with stripped management effort or service supplier interaction"[19]. With this new technology, the requirement for specific infrastructure is negligible and also the services may be accessed from anyplace. When put next to the prevailing methodologies, cloud computing offers benefits like quality, flexibility and multi-tenancy. Resources may be allotted and reassigned to the users and this could be done whereas observation the performance [19].

II. CLOUD CLASSIFICATION

Cloud computing is classified on the basis of type of usage and services offered. On the basis of the types of services offered, cloud computing is divided into different heads:

A. Software as a Service (SaaS)

In this service, whole application is provided over the internet on demand [3]. It follows pay-per-use model for payment. The complete application need not be installed and run on user's computer as it is made available over internet. This reduces the need for software maintenance. For example, in "Salesforce.com", an enterprise cloud computing company, the consumer interactions are stored in the cloud.

A. Platform as a Service (PaaS)

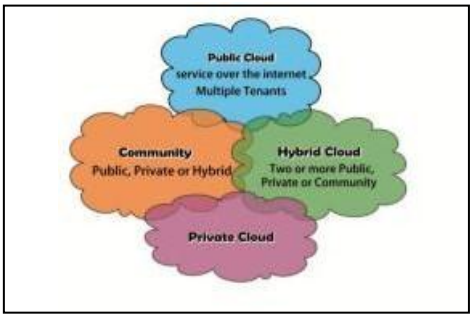
This is the middle layer in cloud computing. In this service model of cloud computing, software applications are shared with the customers over internet. Thus, the users in geographically different locations can work together for developing software.

A. Infrastructure as a Service (IaaS)

this is the lowest layer in the cloud computing and it offers basic infrastructural support to the users. Computing resources including lease processing and storage are supported in this service. Users can control the operating systems, storage and other applications, but the control of the cloud infrastructure remains with the service provider [3].

Cloud services can also be used based on customer's needs (based on deployment model)

1) *Public Cloud:* in this type, many customers use the support of cloud infrastructure which is maintained and managed by a third party [4].This allows multiple users to work on the cloud simultaneously. Computing resources are offered by an off-site service provider to the users through internet. As the service follows pay-per-use model, wastage of resources are minimized considerably.
2) *Private Cloud:* in this type, the infrastructure is provided to a specific user and it will be maintained and managed by themselves or given to a third party [4]. Private Cloud is a proprietary network and is based on the concept of virtualization of machines.
3) *Community Cloud:* in this type a number of organizations who share a common cause will use the cloud infrastructure. This may be managed by a third party or by the users themselves.
4) *Hybrid Cloud:* During this sort, 2 or additional cloud preparation models are joined in such some way that knowledge is transferred between the clouds.



III. NETWORK ISSUES IN CLOUD COMPUTING

Some of the common network issues encountered in cloud computing include:

A. Denial of Service

In denial of service attack (DoS attack), attackers or hackers try to overload the network in such a way that the legitimate users of the service are not able to avail or use the service. This disrupts the server from providing the services to the regular users. In cloud computing, hackers may send innumerable requests to the server, which affects the functionality of the cloud for its clients. In cloud computing, DoS attack can be reduced to a large extent by reducing the privileges of the users connected to the server [18].

B. Man in the Middle Attack

This security issue arises with improper configuration of secure socket layer (SSL). With lacunae in SSL, hacker is able to intercept any data communication between two parties. Proper installation of SSL and checking before the initiation of the communication with other parties can prevent or reduce this network issue.

C. Network Sniffing

Network sniffing is a major issue, particularly with encrypted data. When the encryption techniques used for data, for example passwords, is not secure enough data can be captured by a third party during its transmission. Using appropriate and secure encryption techniques for data is the most ideal method for reducing network sniffing.

D. Port Scanning

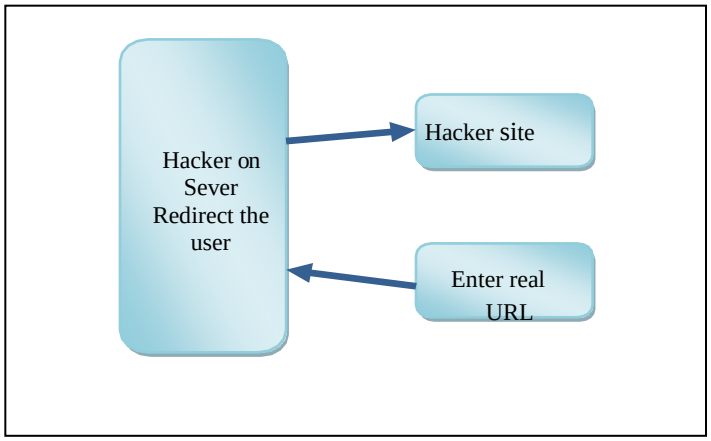
As Port 80 (HTTP) is always open for providing the required services to the user, network issues may arise due to port scanning. Others like Port 21 (FTP), opens only on requests. Securing the ports through encryption techniques until the configuration of the server software is very important to reduce the attack. Firewalls also may be used to secure the data from attacks [19].

E. SQL Injection Attack

This is a special code injection technique used by the attackers by using special characters to return the data. For example, 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.

F. Cross Site Scripting

In this network issue, mostly found in Web applications, attacker redirects the users to hacker site and hack the credentials and other sensitive details of the user. This may further make the system susceptible to buffer overflows, DoS attacks, and insertion of unwanted software into the web browser leading to the violation of credentials of the user [26].



IV. SECURITY ISSUES IN CLOUD COMPUTING

Some of the common security issues associated with cloud computing include:

A. XML Signature Element Wrapping

This technique is usually used to protect a component, name, attribute and value in a web service from illegal parties. But this technique does not provide adequate protection for the position in the documents [9]. In XML Signature Element Wrapping attack, hacker attacks the component using the SOAP messages and changes the component. Using digital certificates like X.509 which is authorized by third party and contain a mixture of WS-security with XML signature helps to protect the component from such attacks. Providing a list of components in XML helps to reject the messages with malicious files and also unexpected messages from the clients.

B. Browser Security

Generally, any client request to the server by the web browser is checked by SSL for credentials of the user. This will ensure that there is no third party who can decrypt the data during communication. Installing sniffing packages on the intermediary host helps the hacker to get the credentials of the user. This can be used by the intermediary host to act as a regular user of the cloud system [10]. Using WS- security concept on the browser helps to prevent such attacks. This is particularly because WS-security works in the level of messages that uses XML encryption for SOAP messages which are not decrypted by the intermediary hosts.

C. Cloud Malware Injection Attack:

In this issue, the attacker uses an interloper to create a spiteful application, service or virtual machine request which is loaded into the cloud structure [1]. Whenever a user request for the spiteful service, it becomes malicious and launches an attack. Hackers may also upload virus programs into the cloud which may later damage the cloud structure. The virus may attack the client's system when the user asks for the spiteful program. Ensuring and checking the authenticity of the received messages will reduce the chances of such an attack. The original image file of the request should be stored using the hash function which can be later compared with the hash functions of all new requests. This will prevent the attacker from creating a hash value for dealing or entering the cloud system.

D. Flooding Attacks

In this method, the hacker attacks the cloud structure directly by sending a number of non-sense requests to a certain service. With increased number of requests the cloud system increases the size and direct more resources towards it. This consumes most of the resources affecting the regular supply to the normal users of the cloud. With diminished resources in the cloud, the hacker then attacks the server. DoS requires the user to pay extra fees for the available resources. Unfortunately, it is not very easy to stop DoS attacks on the clouds. Intrusion detection systems are useful in filtering the requests by installing firewall. But the major disadvantage with the intrusion detection systems are that it may provide fake alerts.

E. Data Protection

In cloud computing protection of data is very important, especially during transformations. It is hard to check the behavior of a cloud supplier and hence the handling of data in a cloud. Any consumer should check the data handling to prevent the attack on data.

F. Incomplete Data Deletion

Incomplete deletion of knowledge is another issue with cloud computing as data clones is also gift in different servers. Complete information deletion is tough as information copies are also keep however aren't accessible [8]. Virtualized personal networks may be wont to keep the information secured and to fully take away the information from the most servers.

G. Locks in

It prevents the user to shift from one cloud provider to another and return back home [27].

V. CONCLUSION

Cloud computing is very popular and is often referred to as the next generation architecture in the field of information technology and 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 It has a number of advantages that has improvised the computing world but is not safe from its own banes. It has a number of security issues at different levels including networking and applications. Clouds are secure and safe only when these issues are dealt with. Apart from the security threats, data storage in clouds also faces confidentiality and integrity issues. Before getting the storage services from a service provider, one should consider these problems at length. To protect the clouds from external threats, regular auditing is necessary. Moreover, one should ensure that SLA‟s are ascertained and errors are minimal so that performance is smooth. 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. This 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]. R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate," 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19- 22,2009. ISBN: 978-1-4244-4357-4.

[2]. Harold C. Lin, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, "Automated Control in Cloud Computing: Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centers and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[3]. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[4] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[5].Foster, I., & Kesselman, C. (1998). The Grid: Blueprint for a New Computing Infrastructure (The Elsevier Series in Grid Computing). Morgan Kaufmann

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

[7]. 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.

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

[9]. Jamil, D., & 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.

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

[11]. Lohr, S. (2007, October 8). 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/technology/08cloud.html

[12]. Mell P, Grance T (2010). The NIST definition of cloud computing. Commun ACM; Vol. 53 No. 6, pp:50.

[13]. NAONE, E (2007, September 18). Computer in the Cloud. Retirived 1 24, 2012, from Technology Review, MIT: http://www.technologyreview.com/printerfriendlyarticle.aspx?id=19397

[14]. 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)

[15]. RALEIGH, NC & ARMONK, NY (2007, May 7). North Carolina State University and IBM help bridge digital Divide in North Carolina and beyond. Retrived 1 27, 2012,from IBM:ttp://www-03.ibm.com/press/us/en/ press release /21506.wss

[16]. REIMER, J (2007, April 8). Dreaming in the "Cloud" with the XIOS web operating system. Retrived 1 24,2012, from are technical: http://arstechnica.com/news.ars/post/20070408- d reaming- in- the-cloud- with- thexios- web- oper ating - system.html

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

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

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

[20] 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.

[21].View, M. Calif & 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

[22].View, M. Calif & 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

[23]Vouk, M. (2008). Cloud Computing-Issues, Research and Implication. "Journal of Computing and Information Technology - CIT" , Vol. 16 No.4, pp. 235–246. [24]Wikipedia (2012a, January 26). Amazon Elastic Compute Cloud Retrived 1 27, 2012, from Wikimedia Foundation Inc. http://en.wikipedia.org/wiki/Amazon_Elastic_Compute Cloud.

[25].Wikipedia (2012b, January 27). Cloud Computing Retrieved 1 28, 2012, from Wikimedia Foundation Inc. http://en.wikipedia.org/wiki/Cloud_computing

[26].Yang, A. (2003). Guide to XML Web Services Security. Retrieved from http://www.cgisecurity.com/ws/WestbridgeGuideToWebServicesSecurity.pdf[27]. Zurich.Catteddu, D. (2010). Cloud Computing. Retrieved from http://www.enisa.europa.eu/act/rm/files/deliverables/ cloud- computingrisk- assessment

[27]. Zurich.Catteddu, D. (2010). Cloud Computing. Retrieved fromhttp://www.enisa.europa.eu/act/rm/files/ deliverables/ cloud-computingrisk- assessment

