A Review on Security Challenges: Communication Level in Cloud Computing

Shaitan Singh Meena
Department of Computer Science and Technology
Central University of Punjab
Bathinda (Punjab), India

Dr. Satwinder Singh
Department of Computer Science and Technology
Central University of Punjab
Bathinda (Punjab), India

***Abstract*--- The cloud computing exhibits, high-quality potential to offer value powerful, clean to control, elastic, and effective resources at the fly, over the net. The cloud computing, upsurges the talents of the hardware resources by most efficient and shared usage. Even the vital infrastructure, as an example, energy technology and distribution plant life are being migrated to the cloud computing paradigm. However, the offerings furnished through third party cloud carrier carriers entail additional protection threats. The migration of user's property**

(records, packages, and many others.) outside the executive manage in a shared environment wherein numerous customers are collocated escalates the security worries.

Keywords— Cloud computing, infrastructure, multi-tenancy, security, web service

1. INTRODUCTION

Cloud computing means putting the data over the internet and accessing those data by using any kind of medium like desktop, PC, mobile phones etc. it is a framework for enable the omnipresent of the data and also allowed the on- demand accessing of the resources which are available in the form of pool (which are shared). The resources may be anything like networks, servers, storage, application and services [4]. The national institute of standards and technology defines the term cloud computing as a model of three layers, which includes deployment models, service models and last one is essential characteristics.

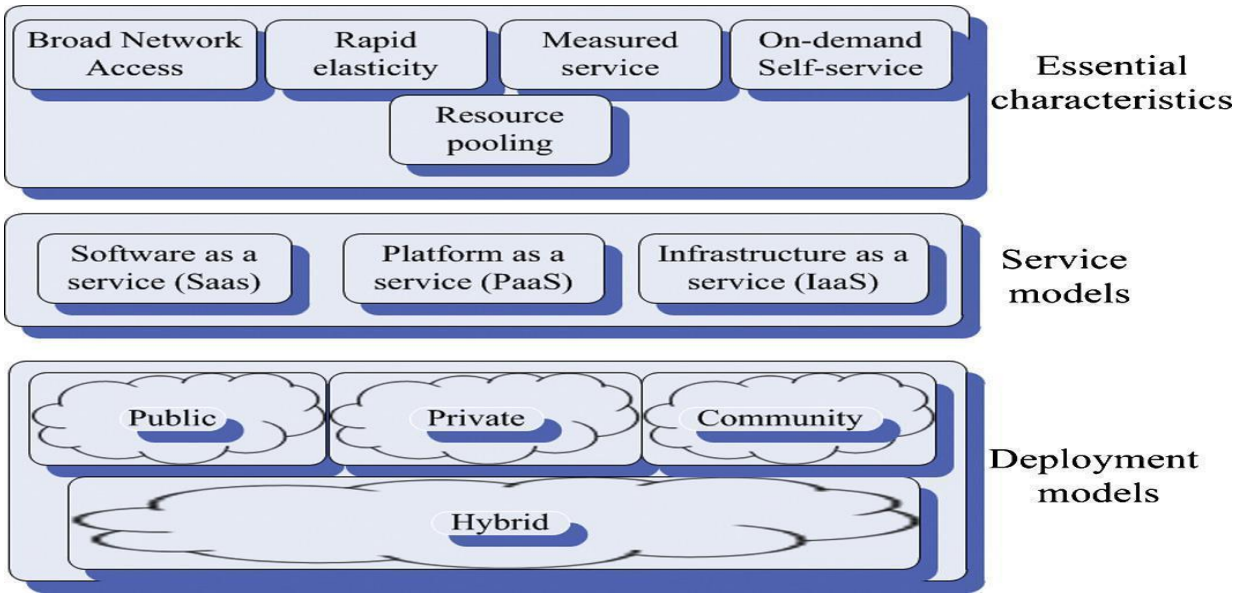

Fig. 1. NIST definition of cloud computing. [2]

1.1. Models of services:

a*) SaaS (software as a service):-* it is a software model which allows the service provider or vendor to host their application and made them usable and available to each and every customers and customers use them by using internet.

b) *PaaS (platform as a service*):- it is a prototype for deporting OS and services over the network without installation and downloading.

c) *IaaS (infrastructure as a service*):- it refers to the hardware information on network, storage and memory.

1.2. Models of deployment

Deployment models are basically of four types:- a) public cloud, b) private cloud, c)community cloud, and d)hybrid cloud. In public cloud, the infrastructure of the cloud is purveyed for completely open consumption by general public. It may be managed and owned up by academic, government organization, business or by some combination of them. The infrastructure of the cloud that are managed and owned by a third party, organisation or combination of them is called as private cloud [10]. Generally used by single organisation. The infrastructure of the cloud that is provisioned for single user by particular community of user from organisation that have dealt with common interest like security requirements , policy, mission and compliances considerations and the last one is hybrid cloud which is a combination of two or more different infrastructures of cloud [1].

1.3. Essential characteristics

It contains characteristics like broad network access, rapid elasticity, on- demand self-services, resources pooling and measured devices.

2. CLOUD SECURITY CHALLENGES

Cloud security services, technologies and model of deployment introduces specific cloud security vulnerabilities and risk in conventional infrastructure. The risk of security in cloud might contrast from the IT traditional risks. The usage of the same resources by different users can be possible only through multi-tenancy. Multi-tenancy stops the risk of visibility of information to dissimilar users and trace of the activities of the users. On- demand self-services is used by the users to use the resources according to their need and the user has to pay for it. Here the security risk is that the use of unapproved access of the resources by the attackers. The environment of virtualization causes its own vulnerabilities and risks that contains malicious involvement between virtual machines. The application of SaaS are conveyed and constructed over the PaaS and it is subjected on the underlying IaaS. Their dependency between the models on each other gets the security dependency as well. A compromised PaaS can prompt bargained with SaaS. To put it plainly, any bargained model of services offers access to the different layers of the models of services. There are risks associated with community, public and hybrid cloud because of vicinity of clients from various roots and the control of administration is done by third party.

Based on the above discussion the challenges are divided into 3 categories in cloud and these are (a) contractual and legal issues (b) architectural issues and (c) communication issues [2].

2.1. Challenges at communication level

The services of the cloud are generally accessible to the users through the internet. For the correspondence between the users standard web protocols are used. The challenges under communication level is further divided as :- 1) external communication issues and internal communication issues. External issues are arises when the communication is between the customers and cloud and internal issues arises when the communication is within the infrastructure of the cloud. The external communication issues are same as the issues in communication over the internet [5]. The external communication challenges includes IP- spoofing based flooding, man in middle , denial of service, eavesdropping and masquerading.

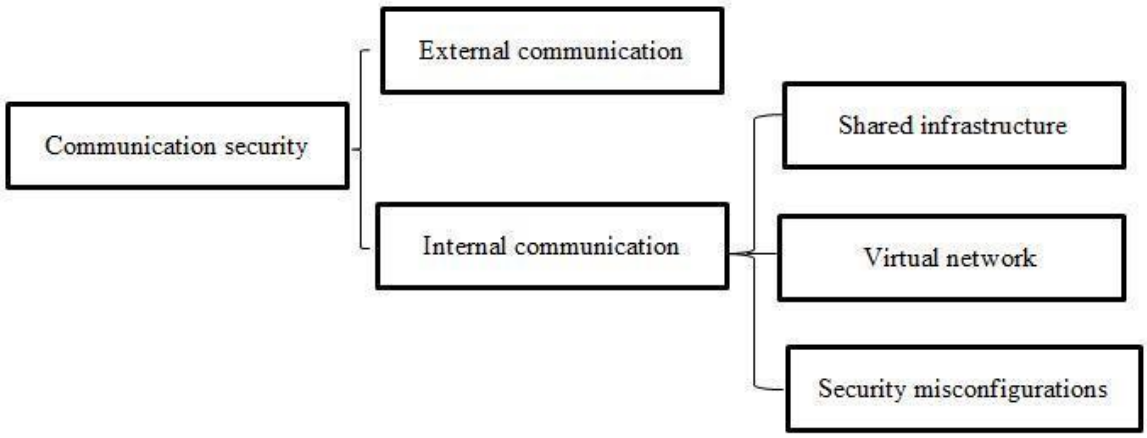

Fig. 2. Cloud security challenges in communication security.

2.1.1. Shared communication infrastructure

Sharing of storage resources network infrastructure components and computations are the results of resources pooling. The window is provided to the attacker for cross- tenant attack by the sharing of network components [3]. Because of the fact that it is difficult to make differences between an attacker's activity and legal vulnerabilities scan of network, generally these scans are not permitted by the provider of services. Likewise, as the resources of network are dynamically purveyed and freed up and these are not linked up to a especial circle of users. The attackers like spoofing and sniffing may be performed by malicious user with the access of super-user across the internet.

2.1.2. Virtual network

Virtualized network are also play a very significant role in communication which is not less than the communication that is happened in real network. The network that is made across the physical network is called as virtual network. This virtual network is creditworthy for the VMs communication. The components that are based on software like routers, bridges and software based network configuration helps the VMs for their networking across the same host [11]. The following challenges are generated because of virtual network: - protection and security procedures are not capable to supervise the virtualized network traffic. Because of this malicious user can prevent them from the supervising of the tools of security. Attacks like sniffing, spoofing and denial of service are possible because of the sharing of virtualized network across the number of virtual machines. The transmission of data that are belongs to the user may be suffer from the breaches due to the risks mentioned above.

2.1.3. Security misconfigurations

For providing cloud service security the security configuration of the network of the cloud infrastructure is very important. Misconfiguration basically consist of the security of application, customers and the whole system. Customer's thoughts that the cloud environment is safe to outsource their data and application. The configuration requires to be good not only at the time of cloud infrastructure deployment, development and operation but also requires alterations is the security policies. The most usual misconfiguration happen when the user selects SECURITY tools by which he is familiar but it does not deal with all the requirement of security. The movement of application, data and VMs over the number of physical node alter in the patterns of topology and traffic can create the demand of different security policies. Similarly, any weakness in the configuration of securing and protocols can be used for session hijacking by the attacker and it will also help the attacker to gain the access to the sensitive data of the user [14].

3. SECURITY SOLUTION IN LITERATURE ON COUNTER MEASURES FOR COMMUNICATION ISSUES:-

For the security of network and communication the guidelines of CSA encourages to employ the use of mixer of IPS, IDS, firewalls and virtual LANs to secure the transmitted data.

The author in [8] suggested a scheme called ACPS (Advanced cloud protection system). Its main focus is to give large security to the resources of the cloud. Their security includes data of the cloud service provider and the network against the attack on the user. Using this scheme cross- tenant attacks can also be minimised by the continuous monitoring of the running virtual machines. The advanced cloud protection system is parted into number of modules. For the detection of malicious activities the interrupt module is responsible. If it detects any malicious activity than it is kept by the detected module and the warning module is responsible to warn the user for the particular activity. Evaluator module evaluates the recorded activities. At the setup time it calculates the checksum of the infrastructure. The malicious activity is determined by precomputing the check sum. In case if any suspicious activity found, it will be send to the evaluator. ACPS is used to avoid the cross virtual machine attacks.

Author in [7] proposed a tool which is used for security purpose in cloud computing used to provide security of virtual network by using the deployment of the virtual network devices. This tool is called CyberGuarder. The data is generally transmitted in the form of peer- to-peer without passing through the central server. CyberGuader is basically used for securing the virtual network and virtual machines. Cyberguarder is also responsible for the isolation of network and virtual machines.

Author in paper [12] suggested a model of virtual network which is used for the safeguards of the virtual network against spoofing and sniffing attacks. To demonstrate the suggested model the Zen hypervisor is used. The author divides the proposed model as 1) routing, 2) shared network layer and 3) firewall. The routing layer is used to establish a logical channel between physical and virtual network. To safeguard the network against spoofing attack Firewall layer is used. And the last layer disallow the communication between the

virtual machines that are belongs to the different virtual network.
Author in paper [6] represents a novel tree- rule firewall which used for the solution of cloud network security. The author also implement it. This is used to eliminate the problem of redundant and shadowed firewalls rules. It uses non-sequential firewall rule searching approach to search the redundant firewall.
Author in paper [9] suggested a technique for the isolation of virtual networks for various VMs. this technique is called DCPortalsNg. DCPortalsNg communicate with the open stack using a plugin of neutron and all the information of the virtual network is obtained by it. And then it creates its own database. This will help in safeguard the DOS attack.

Author in paper [13] suggested a system that is used for the prevention of intrusion in the environment of cloud. This system is called SnortFlow. SnortFlow uses the functionality of open flow and anort system. This is a kind of prototype which is created and tested over the Xen based cloud. The snortflow demon is used to collect the suspicious traffic and an alert is pushed into alert interpreter and this alert interpreter is used to analyse the alert that is generated by the snortflow demon. And now it will invokes the rules generator. Now rule generator creates rules for the malicious traffic and forward the rules to the openflow devices. Now the openflow device reconfigure the network according to the rules that are develop by rules generator. This is used to prevent the traffic against intrusion.

Work	**Technology proposed**	**Work done by Authors**	**My findings and research gap**
[8]	Architecture for monitering integrity of VM and infrastructure components	According this paper, The provided several contributions to secure clouds via virtualization.	Security can be improved by combining cloud with other approaches.
[7]	Cyber-guarder: a virtualization security	This paper suggested a scheme called cyberguard which is a virtualised security assurance architecture. Each safeguard offers three types of services that are: 1) a virtual network security service, 2) a virtual machine security service and 3) a policy based trust management services. .	This work can be improved by using a scalable and reliable NetApp operating system. Using advanced virtualisation technologies it will support. It will provide be beneficial for the cloud that are the group of public and private clouds. .
[12]	Network security for virtual machine in cloud computing	The proposed scheme concentrate on the virtual network security. Also the key technology of cloud platform is virtual network. To improve inter communication security between the VMs this paper suggest a new framework of virtual network which are based on the analysis of Xen.	The proposed scheme in this paper can be improved by the execution of the suggested model in the platform of Xen. This is used to formalize the security. Different platform can be used to test the proposed model.
[6]	cloud network security using the tree-rule firewall	This according Tree-Principle firewall uses conventions in a tree information structure, and sending choice of an information bundle in	This research can be enhanced by expanding the amount of columns in the structure of tree to let in greater than 3 attributes. For example MAC address column and adding protocol. Also enquire the ordering of the localization of the columns as the tree rule

		light of tree standards will take after the tree structure so that the choice on the parcel turns out to be faster.	firewall speed dependent on the specified attribute for root node.
[9]	DCPortalsNg: virtual network security	In this paper, the author suggested DCPortalsNg. This a kind of system used for virtual networks to allow isolation of traffic in an environment of virtualized datacentres.	The research work can further be improved by focussing the research on mixing DCPortalsNg. This will provide the isolation of the networks.
[13]	intrusion prevention system in cloud environment	This paper suggested a system which is used for the prevention of the openflow- based intrusion. In Zen based environment of cloud this system is called SnortFlow. .	In future research the controller is capable to check number of OVS and OFS at the same time.

Table 1: Research gap and findings of various technologies proposed in the above literature

CONCLUSIONS:

There are number of advantaged of cloud computing, number of services are provided to the users, number of security policies are also provided which forces the user to adopt the cloud. But there are still number of challenges/ issues are there which needs to be focussed on. This paper highlights the communication challenges/issues. This paper also focussed on some of the counter measures to remove that issues. But still there are number of issues which needs focus. The analysis of different technologies discussed in different papers is represented in the form of table, which shows the name of the technology, the brief description of the approach that is used by the authors and at last columns the findings and future work that can be done in coming future is explained.

REFERENCES

[1]. Albanese, M., Jajodia, S., Jhawar, R., & Piuri, V. (2014). Secure Cloud Computing. *Secure Cloud Computing*, 239–259. http://doi.org/10.1007/978-1-4614-9278-8

[2]. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*,*305*,357–383. http://doi.org/10.1016/j.ins.2015.01.025

[3]. Bilal, K., Ur, S., Malik, R., & Khan, S. U. (2016). Trends and Challenges in Cloud Datacenters.: IEEE cloud computing , 1 , 2325-2356

[4]. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Incio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security*, *13*(2), 113–170. http://doi.org/10.1007/s10207-013-0208-7

[5]. Ficco, M., & Rak, M. (2015). Stealthy denial of service strategy in cloud computing. *IEEE Transactions on Cloud Computing*,*3*(1),80–94. http://doi.org/10.1109/TCC.20142325045

[6]. He, X., Chomsiri, T., Nanda, P., & Tan, Z. (2014). Improving cloud network security using the Tree-Rule firewall. *Future Generation Computer Systems*, *30*(1), 116–126. http://doi.org/10.1016/j-future.2013.06.024

[7]. Li, J., Li, B., Wo, T., Hu, C., Huai, J., Liu, L., & Lam, K. P. (2012). CyberGuarder: A virtualization security assurance architecture for green cloud computing. *Future Generation Computer Systems*, *28*(2), 379–390. http://doi.org/10.1016/j.future.2011.04.012

[8]. Lombardi, F., & Di Pietro, R. (2011). Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, *34*(4), 1113–1122. http://doi.org/10.1016/j.jnca.2010.06.008

[9]. Moraes, H. M. B., Nunes, V., & Guedes, D. (2014). DCPortalsNg : Efficient Isolation of Tenant Networks in Virtualized Datacenters. *The Thirteenth International Conference on Networks*, (c), 230–235.

[10]. Popović, K., & Hocenski, Z. (2010). Cloud computing security issues and challenges, (April), IEEE computing, 1(1) , 344–349.

[11]. Sen, J. (2013). Security and Privacy Issues in Cloud Computing. *Architectures and Protocols for Secure Information Technology*, (iv), 42. http://doi.org/10.1109/HICSS.2011.103

[12]. Wu, H., Ding, Y., Winer, C., & Yao, L. (2010). Network security for virtual machine in cloud computing. *2010 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, 18–21. http://doi.org/10.1109/ICCIT.2010.5711022

[13]. Xing, T., Huang, D., Xu, L., Chung, C. J., & Khatkar, P. (2013). SnortFlow: A OpenFlow-based intrusion prevention system in cloud environment. *Proceedings - 2013 2nd GENI Research and Educational Experiment Workshop, GREE 2013*, 89–92. http://doi.org/10.1109/GREE.2013.25

[14]. Xu, Wu, Daneshmand, Liu, W. (2015). A data privacy protective mechanism for WBAN. *Wireless Communications and Mobile Computing*, (February 2015), 421–430. http://doi.org/10.1002/wcm