International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Toward Cloud Network Infrastructure Approach: Service and Security Perspective

Kalyar Myo San

Faculty of Computer Systems and Technologies, University of Computer Studies, Mandalay, Myanmar

How to cite this paper: Kalyar Myo San "Toward Cloud Network Infrastructure Approach: Service and Security Perspective" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.2198-2202, **https://doi.org/10.31142/ijtsrd27926**

IJTSRD27926

ABSTRACT

The primary goal of the paper is to support a complete integrated solution for a single communication platform providing cloud services to end-users. The paper presents a literature review of cloud computing concepts and technologies, including the requirements of cloud computing services and the key performance indicators. The paper also review and analyses the cloud management platform (Open Stack), software define networking (SDN), and also highlight the integration of Open stack and SDN. The paper provides the valuable information for secure network infrastructure with De-Militarize Zone (DMZ) designing and firewall implementations with cloud infrastructure. Finally, complete information is supported for secure cloud network infrastructure, which allows smooth implementation of additional services and functionalities.

KEYWORDS: *Cloud computing, DMZ, OpenStack, SDN, SDN controller*

INTRODUCTION

Nowadays, enterprises and service providers started to overcome the limitations of conventional network architecture. Cloud computing is becoming necessity as one of the ubiquitous paradigms in computing where computing infrastructure and solutions are delivered as a service. OpenStack is one of the open source cloud operating system, famous in the industry. OpenStack Networking (neutron) supports a plugin model that allows it to integrate with multiple different systems in order to implement networking capabilities for OpenStack.

On the other hands, software-Defined Networking (SDN) is an approach for dynamically programming networks, including the ability to initialize, change and manage network behavior using open interfaces. For the purpose of OpenStack integration with SDN controller, it offloads all networking tasks onto controller, which diminishes the processing burden for OpenStack. But the growth of cloud computing has brought some security challenges. These security issues should be protected by modernized security design levels in order to make cloud computing services more secured and reliable.

A. Cloud Computing

According to National Institute of Standards and Technology (NIST), cloud computing is a model for enabling ubiquitous, 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. This cloud model is composed of five essential characteristics, four deployment models and three service models. [1]

1. Cloud Computing Essential Characteristics:

According to the NIST cloud computing contains following five essential characteristics [1]:

A. **On-demand self-service:** Provision computing services and computing capabilities. It also provision server service without human interaction from each service provider.

B. **Broad network access:** Computing capabilities are available over the network and can be accessed through standard mechanisms that promote the use of heterogeneous client platform.

C. **Resource pooling:** The computing resources of the providers are pooled to support multiple consumers using a multi-tenant model with different virtual and physical resources dynamically assigned and reassigned according to consumer demand. The consumer has no idea or knowledge over the exact location of the resources but can access and use data at any time from any location at a higher level of abstraction.

D. **Rapid elasticity:** Computing capabilities can be rapidly and elastically provisioned. The resource pooling and self-service make it possible. The provider can automatically distribute more or less resources from available pool at any time.

E. **Measured Service:** Cloud systems, in this case, automatically control and manage resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service and providing transparency for both the provider and consumer of the utilized service.

According to [3, 4, 5], some researchers insist that multi-tenancy is also an important element of cloud computing. They are described briefly below.

F. **Multi-tenancy:** is an architecture in which a single instance of a software application serves to multiple customers or tenants. Multi-tenancy applies to all the three service models IaaS, PaaS and SaaS. It has many advantages and also has some challenges. The advantages are: cost savings on scaling IT resources and software licensing, etc. Security, capacity optimization and service delivery and high availability are the main challenges of multi-tenancy [6][2].

2. Cloud Computing Deployment Models:

There are four basic deployment models in cloud computing :public, private, community and hybrid cloud is defined according to where the infrastructure for the environment is located. [1][2]

Public cloud: Cloud Service Customer share the Cloud Service Provider's infrastructures through the internet along with other customers. This model is open to all andiIt may be owned, managed, and operated by a business, academic, or government organization, or some combination of them

Private cloud: Cloud Service Customer uses infrastructures exclusively located with an organization or premises and they also manage the resources. This model is not open to all it may be owned, managed, and operated by the organization, a third party, or some combination of them.

Community cloud: A private cloud is shared by many customers with common policies and procedures. This cloud gets benefits from both private and public clouds. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them.

Hybrid cloud: A combination of public, private and community clouds which gets the benefit from all the three cloud models.

3. Cloud Computing Service Models:

There are three service models in cloud computing: IaaS, PaaS and SaaS. IaaS is the basic layer in the cloud computing model and, PaaS is the middle layer in the cloud computing model where PaaS can be built on top of IaaS. SaaS is the final layer in the cloud computing model and it can be built on top of IaaS and PaaS.[1][2]

Infrastructure as a Service (IaaS): Cloud Service Provider provides the computing resources like processor, storage, network and other fundamental computing resources to Cloud Service Customer. Other services become Cloud Service Customer's responsibility.

Platform as a Service (PaaS): Cloud Service Provider provides customers with all the IaaS services (processing, storage, networks, and other fundamental computing resources) plus the operating system, middleware and runtime services.

Software as a Service (SaaS): Cloud Service Customer can access the software through internet uploaded by the Cloud Service Provider and can use of the Cloud Service Provider's infrastructure, platforms and all other functionalities on a pay-per-use approach.

B. Open-source cloud management Platforms (CMPs)

Cloud services are developing the next generation of cloud management systems. The four biggest players in the market currently are OpenStack, CloudStack, Eucalyptus and OpenNebula. Each of them is creating new ways for organizations to connect various cloud services, OpenStack is leading the way and it becomes a mature product set with some very high profile users.

1. OpenStack

OpenStack is a free and open source platform for cloud computing under the terms of the Apache license. The software is developed for a control of wide range of processing, storage and networking resources throughout a data centre. It provides a modular architecture that gives the flexibility in the clouds design, including integration with existing systems and third-party technologies, e.g., Amazon EC2, GoGrid, Rackspace. [7], [8]. [9].

The newest version of the OpenStack platform Stein released on 10 April 2019. It has plenty of service such as Nova, Neutron, Cinder, Glance, Swift, Horizon, Key-stone, Heat, Mistral, Ceilometer, Trove, Sahara, Ironic, Zaqar, Manila, Designate, Searchlight, Barbican, Magnum, Vitrage, Aodh. The most important and core services are:
Compute (Nova service) - module for arranging, managing and providing power massively scalable, on demand, self service access to compute resources.

OpenStack Networking (Neutron service) - module for managing networks and IP addresses and also gives users self-service ability over network configurations.

Object Store (Swift service) - module for creation and managing scalable object storage system

Image Service (Glance service) - module which provide a service for uploading, discovering, registration and delivery services for disk and server images. It retrieves and process data about virtual machine images.

C. Overcommitting CPU and RAM in OpenStack

In OpenStack, default environment configuration allow creating up to 10 instances and assigning among others 20 VCPUs, 50 GB of memory and 1 TB of storage.

TABLE 1 show the default set of virtual resources and it can also customize. It allow customers to overcommit CPU and RAM on compute nodes. This allows the customer to increase the number of instances running on the cloud at the cost of reducing the performance of the instances. The Compute service uses the default ratios are describe below: [8][9]

- CPU allocation ratio: 16:1
- RAM allocation ratio: 1.5:1

The formula for the number of virtual instances on a compute node is

$$(OR*PC)/VC \quad (1)$$

where:
OR - CPU overcommit ratio (virtual cores per physical core)
PC - Number of physical cores
VC - Number of virtual cores per instance

TABLE I. Default set of virtual resources

Flavor Name	Virtual resources		
	VCPUs	RAM	Root Disk
m1.tiny	1	512MB	1G
m1.small	1	2G	20G
m1.medium	2	4G	40G
m1.large	4	8G	80G
m1.xlarge	8	16G	160G

TABLE2. SDN Controller Features

Controller Name	Controller Features				
	Northbound API	Southbound API	Language	Architecture	Support Platform
Flow Visor	JSON RPC	Open Flow 1.0,1.3	C	Centralized	Linux
Floodlight	REST, Java RPC, Quantum	Open Flow 1.0, 1.3	Java	Centralized	Linux, MacOS, Windows
ODL	REST, RESTCONF XMPP, NETCONF	Open Flow 1.0,1.3	Java	Distributed Flat	Linux, MacOS, Windows
Open Contrail	REST	BGP, XMPP	C,C++, Python	Centralized	Linux
RYU	REST	Open Flow 1.0-1.5	Python	Centralized	Linux, MacOS

D. Software Define Networking

Software Defined Networks offer dynamic, more efficient and intelligent network operations by separating conventional network into a centralized control plane and a programmable data plane.[32] SDN southbound APIs (eg., OpenFlow) are used to communicate between the SDN Controller and the switches and routers of the network. SDN northbound APIs (eg., Rest APIs) are usually used to communicate between the SDN Controller and the services and applications running over the network. FlowVisor [11], Floodlight [13], OpenDaylight (ODL) [14], OpenContrail [15] and RYU [16] are some of the well known open source controllers for customers who want to deploy a fully open-source solution and avoid possible vendor lock-in [12]. SDN Controller's Features is shown in TABLE 2.

E. Scalable integration of SDN and Openstack

OpenStack provides the foundation to build a private or public cloud in which virtualized compute resources, together with required networking and storage, can be dynamically instantiated and destroyed as needed. This dynamic environment requires a programmable networking solution that is equally dynamic in other words, OpenStack needs SDN. There are several approaches which have been described to integrate various SDN controllers with Openstack e.g., Ryu and OpenDayLight. [17][31]

F. Cloud Network Infrastructure Security

1. De-Militarized Zone

The De-Militarized Zone is a process of building up a semi-secure network which is used to secure the internal network of any organization from external threats [18]. DMZ is used to protect the servers such as FTP [10], DNS, Web, SMTP.

2. Level of designing DMZ

According to Jack et al. [19] [20], there are four common levels of DMZ designing and comparative analysis of different level are described below.

Level 1 DMZ Design: It creates a single point of protection and filtering with least complicated, lowest security and cost among the four levels.

Level 2 DMZ Design: It creates a single point of protection and filtering with multiple network segments or VLANs. It is more secure as compare to level 1 DMZ design and providing multiple DMZs utilizing multiple ports off the firewall.

Level 3 DMZ Design: It creates double boundary firewall design for internal and external traffic to protect the trusted network. It is more secure, more complex design and higher cost than compare to level 1 DMZ design

Level 4 DMZ Design: It creates double boundary firewall design with multiple firewalls pairing to create the boundaries between DMZs. It is the most secure, most complicated and expensive design as compare to level 1 DMZ

3. Firewall Implementations

In cloud based firewall, according to [21], SDN can capable of layer 7 firewall functions by replacing expensive firewall equipments. It uses Firewall Client Agent to talk SDN Controller via REST API and will communicate to Cloud Firewall agent (firewall application and Firewall Server agent) through REST APIs.

In SDN, there is absence of built-in security limits its adoption, as described in some campus adopters [23]. On the other hand, the centralized design of SDN framework can introduce security challenges such as denial-of-service (DoS) attacks, targeted at SDN controller and OpenFlow switches [24].

In SDN-based Stateful Distributed Firewall [22], they pointed two main issues : existing centralized firewall architecture [25], [26], [27], [28] and lack of state information [29]. It is difficult to discover attacks originating in SDN-data plane [30] are identified. And then, scalable distributed states management solution (SDN-based Stateful Distributed Firewall) [22] is introduced at the data plane to track packets and flow states to against data plane attacks.

G. Conclusion

This paper presents various aspects of cloud computing and its services. As cloud computing is enhancing more and more , it brings challenges which include many security issues. Cloud computing has essential ability to protect these challenges by using different information that suite different needs. This paper describe and point out difference in methodologies and their best suited deployment flavors for cloud infrastructure with security and service perspective.

References

[1]. NIST SP 800-145, "A NIST definition of cloud computing",https://csrc.nist.gov/publications/detail/sp/800-145/final

[2]. P. Ravi Kumar1, P. Herbert Raj2, P. Jelciana3, " Exploring Security Issues and Solutions in Cloud Computing, Services – A Survey"

[3]. Aldossary, S., W. Allen. "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions." International Journal of Advanced Computer Science and Applications, Vol. 7, 2016, No 4.

[4]. Catteddu, D., G. Hogben. Cloud Computing: Benefits, Risks and Recommendations for Information Security. European Union Agency for Network and Information Security (ENISA), 2009, pp. 1-125.

[5]. Reed, A., C. Rezek, P. Simmonds. Security Guidance for Critical Area of Focus in Cloud Computing. V3.0. Cloud Security Alliance (CSA). 2011, pp. 1-177.

[6]. Price, D. "The Challenges of Multi-Tenancy. 26 March2014."https://cloudtweaks.com/2014/03/challenges-multi-tenancy/

[7]. D. Grzonka, M. Szczygieł, A. Bernasiewicz, A. Wilczyński, and M. Liszka, "Short analysis of implementation and resource utilization for the OpenStack cloud computing platform", in Proc. 29th Eur. Conf. Modell. Simul. ECMS 2015, Albena (Varna), Bulgaria, 2015, pp. 608–614.

[8]. OpenStack Website and Documentation , :http://www.openstack.org/

[9]. D. Grzonka "The Analysis of OpenStack Cloud Computing Platform: Features and Performance", Journal of Telecommunication and Information Technology, 2015

[10]. Joseph M. Adams "FTP Server Security Strategy for DMZ" https://www.giac.org/paper/gsec/805/ftp-server-securitystrategy-dmz/101713

[11]. R. Sherwood, G. Gibb, K.-k. Yap et al., "Flow Visor: A Network Virtualization Layer," Network, p. 15, 2009.

[12]. Five must-know open source SDN controllers https://searchnetworking.techtarget.com/news/2240225732/Five-must-know-open-source-SDN-controllers

[13]. Big Switch Networks, "Project Floodlight." [Online]. Available: http://www.projectfloodlight.org/floodlight/

[14]. "Open Daylight: A Linux Foundation Collaborative Project." [Online]. Available: https://www.opendaylight.org/

[15]. "Open Contrail An open-source network virtualization platform for the cloud." [Online]. Available: http://www.opencontrail.org/

[16]. Ryu SDN Framework Community, "Ryu Controller." [Online]. Available: https://osrg.github.io/ryu/index.html

[17]. O. Tkachova, M. J. Salim, and A. R. Yahya, "An analysis of SDN-OpenStack integration," PIC S&T, 2015.

[18]. K. Dadheech, A. Choudhary, G. Bhatia "De-Militarized Zone: A Next Level to Network Security", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

[19]. Jack Webb "Network Demilitarized Zone". http://www.infosecwriters.com/Papers/jwebb_network_demilitarized_zone.pdf.

[20]. K. Dadheech, A. Choudhary, G. Bhatia "De-Militarized Zone: A Next Level to Network Security", Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Xplore Compliant - Part Number: CFP18BAC-ART; ISBN:978-1-5386-1974-2

[21]. Mahesh. A, Adhiyan Chandrasekaran, ArunKumar. R, SivaKumar. K, Vigneshwaran. N , "Cloud based firewall on OpenFlow SDN network", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), IEEE, DOI:10.1109/ICAMMAET.2017.8186699

[22]. Chowdhary, D. Huang, A. Alshamrani and A. Sabur "SDFW: SDN-based Stateful Distributed Firewall" , arXiv:1811.00634v1 [cs.CR] 1 Nov 2018, DOI: 10.13140/RG.2.2.11001.93281

[23]. J. Networks, "Readiness, benefits, and barriers: An SDN progress report," https://www.usebackpack.com/resources/7178/download?1451715494,

[24]. S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in Future Networks and Services (SDN4FNS), 2013 IEEE, pp. 1–7.

[25]. Hu, W. Han, G.-J. Ahn, and Z. Zhao, "Flowguard: building robust firewalls for software-defined networks," in Proceedings of the third workshop on Hot topics in software defined networking. ACM, 2014, pp. 97–102.

[26]. P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A security enforcement kernel for

openflow networks," in Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, pp. 121–126.

[27]. M. Suh, S. H. Park, B. Lee, and S. Yang, "Building firewall over the software-defined network controller," in Advanced Communication Technology (ICACT), 2014 16th International Conference on. IEEE, 2014, pp. 744–748.

[28]. S. Zerkane, D. Espes, P. Le Parc, and F. Cuppens, "Software defined networking reactive stateful firewall," in IFIP International Information Security and Privacy Conference. Springer, 2016, pp. 119–132.

[29]. V. H. Dixit, S. Kyung, Z. Zhao, A. Doup´e, Y. Shoshitaishvili, and G.-J. Ahn, "Challenges and preparedness of sdn-based firewalls," in Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, 2018, pp. 33–38.

[30]. S. Gao, Z. Li, B. Xiao, and G. Wei, "Security threats in the data plane of software-defined networks," IEEE Network, 2018.

[31]. S. Chen , R.Hwang , "A Scalable Integrated SDN and OpenStack Management System",2016 IEEE International Conference on Computer and Information Technology (CIT), DOI: 10.1109/CIT.2016.27

[32]. D. Kreutz, M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, ans S.Uhlig, "Software-Defined Networking: A Comprehensive Survey", arXiv:1406.0440v3 [cs.NI]