WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Capabilities and Features Offered by SDN on the Cloud Network Infrastructure

Khwaja Hedayetulla Sidiqi [a], Zalmai Zormatai [b], Samiullah Mehraban [c]

[a] *Researcher, Bakhtar University*
[b] *Assistant Professor, Bakhtar University*
[c] *PhD scholar, Delhi Technological University*

A B S T R A C T

Cloud computing is an evolutionary approach of offering IT services to the industry and IT businesses. Alongside the advantages of cloud computing, it has raised many security, performance and network management concerns in the cloud datacenters. In this study, I present the implementation of SDN (software-defined networking) into the cloud network infrastructure to overcome issues related to network administration, monitoring and security. SDN is an approach to network virtualization which adds to the security and performance of the network and helps to automate and ease the network management by making the network flexible to changes and extensions.

The research methodology used is descriptive and analytical based on the recent research work done by other researchers in this domain using a systematic literature review approach. The implementation of SDN into the cloud network infrastructure is presented as a suitable proposed solution to overcome some (network security, network performance, and network management) of the current cloud network infrastructure issues.

Keywords: Cloud Computing, IT services, SDN, Network security

1. Introduction

Cloud computing is considered as a new field of study for researchers and academicians, cloud computing is a revolutionary change the way IT services are provided in organizations. Cloud computing avoids the necessity of organizations for owning on- premises data centers and network infrastructure facilities; which reduces the cost, need of IT expert staff and brings elasticity. When plugging an electric machine into a power socket, we care neither how electric power is produced nor how it gets to that power socket. This is probable because electricity is virtualized; that is, it is already available from a wall socket that hides power generation stations and a massive power supply grid. When we think about information technologies, this idea means providing useful functions while hiding how their internals work. Computing itself, to be considered fully virtualized, must allow computers to be made from distributed components such as processing, storage, data, and software resources. Such concept describes a business model where the consumers pay to the providers based on the theory of 'Pay-as-you-go'. "Cloud computing is a techno-business disruptive model of using distributed large-scale data centers either private or public or hybrid offering customers a scalable virtualized infrastructure or an abstracted set of services qualified by service-level agreements (SLAs) and charged only by the abstracted IT resources consumed (Buyya, Broberg, & Goscinski, 2011)". ISO/IEC defines cloud computing as follows "Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on- demand". The NIST (National Institute of Standards and Technology) definition of cloud according to the NIST Special Report 800-145 is: "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 quickly allocated and released with slight administrative effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models (Mell & Grance, 2011)".

2. Main Findings

The outcome of my work will demonstrate that why the conventional network infrastructures cannot meet the performance, security and network management needs of the cloud computing and will highlight that there are many problems with the current cloud computing as well. To overcome this issue the capabilities and opportunities (high performance and better oversight of the network bandwidth, access control and applications' security) of the DSN will briefly be described, why should we use SDN to address the problems associated with the cloud network infrastructure and the impact of the SDN on the cloud computing network infrastructure is stated in details.

3. Cloud Computing Essential Characteristics

a. On-demand self-service: A client can individually deliver computing resources, such as server time and network storage, as required dynamically without demanding human interaction with each cloud service provider (CSP).

b. Broad network access: Competencies are accessible over the public internet and accessed through standard procedures that support the use by various customer platforms (e.g., mobile phones, tablets, laptops, and workstations).

c. Resource pooling: The cloud service provider's computing resources are shared to assist numerous clients using a multi-tenant architecture, with various physical and virtual resources automatically assigned and reassigned according to user request. The consumers don't have any idea about the where their data is actually stored or maybe they are only have information regarding the location of data at a higher level (for example country, province, or datacenter).

d. Rapid elasticity: Computing resources (e.g. CPU) can be elastically provided to the clients and freed from clients, in some cases dynamically, to measure rapidly outward and inward proportion with demand. To the customer, the capabilities offered for provisioning often seem to be unlimited and can be expected in any amount at any interval of time.

e. Measured service: Cloud systems dynamically govern and adjust resource use by measuring and metering competency at some level of abstraction suitable to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be observed, controlled, and reported, providing transparency for both the cloud service provider and client of the used service (Mell & Grance, 2011; Mogull et al., 2017).

4. Cloud Service Models

SaaS (Software as a service) The services or capabilities offered to the clients are that they can utilize the applications lying on a cloud hardware infrastructure. Clients usually access the data using a simple web browser, the customers cannot manage or control the underlying infrastructure of the cloud such as (Servers, storage, Operating Systems (OS), Network & etc…).

SaaS is multitenant applications running on PaaS or IaaS due to increased agility, resilience and economic benefits. Many providers offer the SaaS services using the public APIs to support the variety of clients, especially web browsers and mobile applications. Thus, the SaaS tends to have an application/logic layers and storage layer with an API on top, and there is one presentation layer which includes the web browsers, mobile applications and public APIs (Mogull et al., 2017).

IaaS (Infrastructure as a service) The competencies delivered to the clients are the provisioning processing, network, storage and other computing resources where the clients are able to set up their software applications. The clients will not have control over the cloud infrastructure but they can have limited control over their own network appliances (such as the firewall). The foundation of the IaaS is formed of the physical facility and hardware infrastructure. The resources (physical hardware, network & storage) are pooled using the abstract and orchestration. Abstracts free the resources from the physical constraints using virtualization to enable pooling.

Orchestration then (a set of core connectivity and delivery tools) ties these abstracted resources together to create pools and provide automation so that the resources are delivered to the customers. All these are facilitated using the APIs (Application programming interface). Most of the APIs these days use the REST (Representational State Transfer) which runs on the HTTP protocol making it very suitable for internet services. In most cases, these APIs are wrapped into a web-based interface for remote access which is called the cloud management plane (because the customers use it to manage and configure the resources). So the IaaS consists of a facility, hardware, abstract layer, and the orchestration layer. The IaaS design is simplified in Figure-1, which shows the storage and compute controllers for orchestration and the hypervisors for abstraction and the relationship between abstract and orchestration. "A series of physical servers each run two components: a hypervisor (for virtualization) and the management/orchestration software to tie in the servers and connect them to the compute controller. A customer asks for an instance (virtual server) of a particular size and the cloud controller determines which server has the capacity and allocates an instance of the requested size" (Mogull et al., 2017).

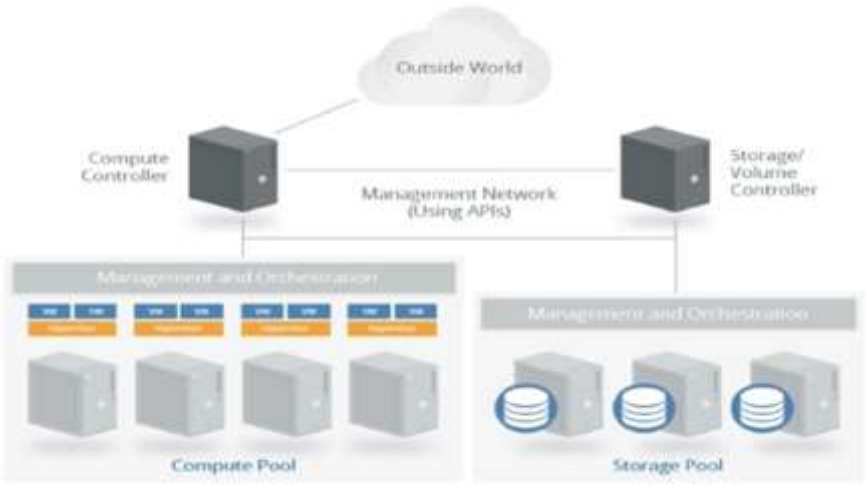

Figure 1 IaaS Platform Image source: Guidance, S. (2017). Security Guidance for Critical Areas of Focus for Cloud Computing.

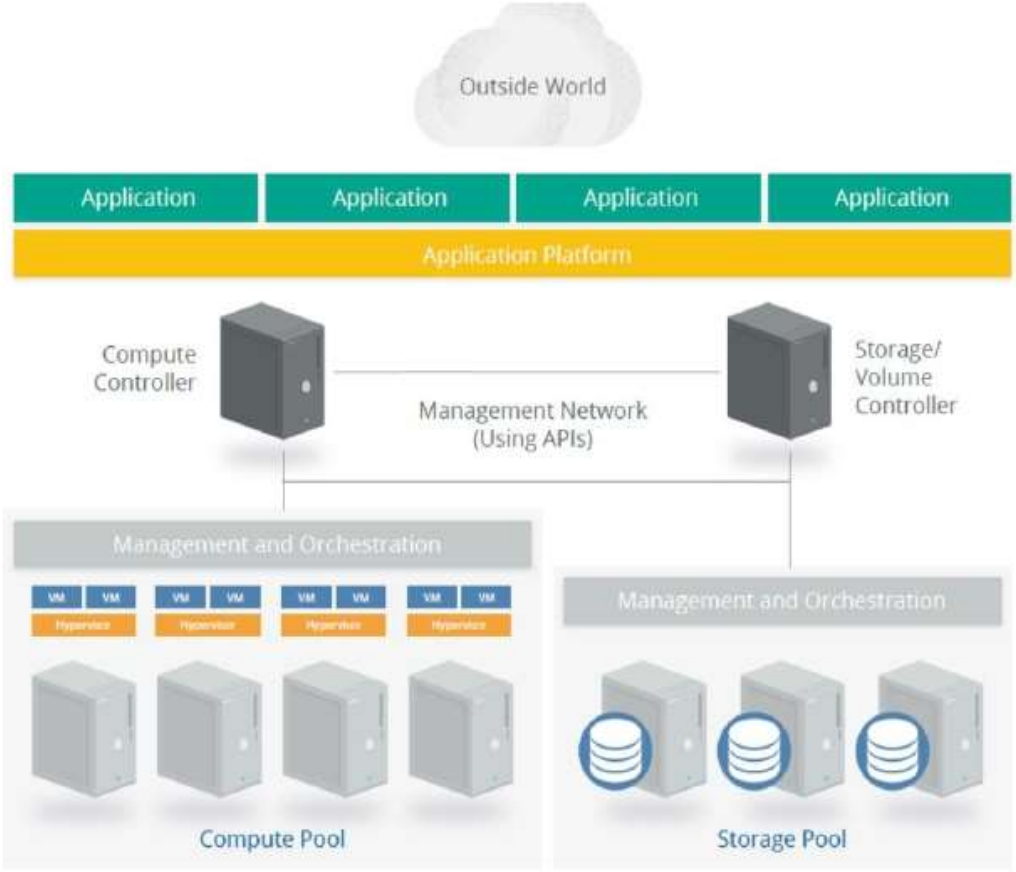

Figure 2 *PaaS running on the IaaS infrastructure*
Image source: Guidance, S. (2017). Security Guidance for Critical Areas of Focus for Cloud Comput ing

PaaS (Platform as a service)

The competencies delivered to the consumers are the deployment of the customer's applications on the cloud infrastructure that are developed using the cloud-supported programming languages and libraries. Again, the consumers cannot control and manage the underlying cloud infrastructure. PaaS is a layer of integration and middleware built on the IaaS. It is then pooled together, orchestrated and made available to the customers using APIs. An example of PaaS is the application deployment platform where the developers can run the application codes without managing the underlying infrastructure (Mogull et al., 2017). Figure 2 shows the simplified diagram of PaaS built on the IaaS.

5. Cloud Deployment Models

a. Private cloud: The private cloud infrastructure is owned by a single organization. The organization itself or a third party will control and manage the cloud infrastructure, it may exist on or off the premises.

b. Community cloud: The cloud infrastructure is owned, managed and controlled by one or more organizations of a community and provides services to a specific community only. It may exist on or off the premises.

c. Public cloud: The public cloud provides services to everyone who is interested to use it. It is owned, managed and controlled by a business, academic or a governmental organization. The public cloud exists on the premises of the Cloud Service Provider (CSP).

d. Hybrid cloud: A combination of two or more of private, public and/or community cloud infrastructure that remains unique entities but are bound by a standard or proprietary technology which enables data and application portability(Mell & Grance, 2011; Mogull et al., 2017).

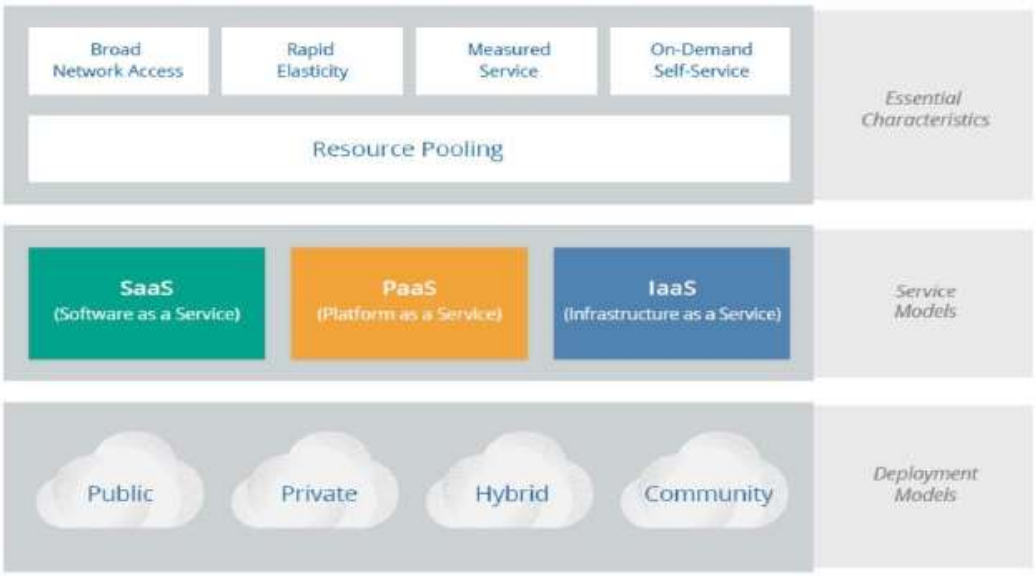

Figure 3 *Cloud Deployment Model, Service Model & Characteristics*

Image source: Guidance, S. (2017). Security Guidance for Critical Areas of Focus for Cloud Comp

The cloud d uting. the cloud services and whether the cloud infrastructure is on the premises. Figure 3 shows the cloud characteristics, cloud deployment and services models, and Figure 4 illustrates the cloud deployment models with its corresponding owner.

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization / Third-Party Provider	Organization / Third-Party Provider	On-Premises / Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

Figure 4 *Cloud Deployment Model*

Image source: Guidance, S. (2017). Security Guidance for Critical Areas of Focus for Cloud Computing.

Cloud computing is an emerging technology which can benefit the businesses by providing on-demand IT services for the payment based on the principle of pay-as-you- go. The traditional on-premises IT infrastructure requires a well-equipped facility, purchase of hardware devices, hiring professional staff, staff training, operational and maintenance costs. Such requirements cause a huge increase in overall service cost. The lack of network security, high

reliability, availability, network management, network extension, network monitoring, high network performance, traffic and network isolation, network flexibility and disaster recovery are the main problems with the on-premises network infrastructure. To overcome these problems, an organization has to use the cloud computing and rent IT infrastructure or services from the Cloud Service Providers. Cloud offers the IT services at low cost, with high reliability and availability, high performance, on-demand services, no operational or maintenance cost, and security measure at place. With all these benefits and opportunities, the cloud computing still experience the network security, performance, and network management issues.

6. Discussion

SDN on the other hand is a new technology which provides new opportunities and benefits for both the CSP and cloud users. SDN provides a virtualized environment and decouples the data plane from the control plane. The SDN controller is a logical centralized server which enforce policies on SDN-enabled switches, Routers, firewalls and access points. The switches usually communicate with the SDN controller using the OpenFlow protocol and update the policies into their flow tables. The benefits of SDN include but are not limited to packet filtering, network virtualization, traffic and network isolation, increased security, high performance, better network management, energy efficient, inexpensive, load balancing, fault tolerance and logical centralized control.

7. Conclusion

The research questions that were posted at the beginning of my thesis were: what are the weaknesses, vulnerabilities, data security, network infrastructure security and performance issues of the current cloud network infrastructure? What are the capabilities and features offered by SDN? What will be the impact of SDN implementation on current cloud network infrastructure? To answers to these questions I have conducted a systematic literature review and selected around 62 articles from IEEE, ACM and science direct journals based on the selection criteria mentioned in Chapter 6. I have reviewed and analyzed those articles and I arrived at the following findings**:**

 Cloud computing is vulnerable to various security threats, the main areas where the security vulnerabilities exist are the cloud network infrastructure and cloud virtualization. Cloud computing also experience the network management and network performance issues.

 SDN provides various opportunities to the cloud network infrastructure including packet filtering, network virtualization, traffic and network isolation, increased security, high performance, better network management, energy efficient, inexpensive, load balancing, fault tolerance and logical centralized control.

 The deployment of the SDN into the cloud computing can increase the cloud computing security, network performance, and network management. Based on the results of the systematic literature review, I conclude that the implementation of SDN into the cloud computing is a possible well-suited solution.

8. Limitation and Future work

There are still various open issues with SDN. To address these issues, further research is required. Two future research questions are summarized as follows: 1. How significant is the security in the SDN environment? As technology develops, with new trends new security vulnerabilities also emerges. The security of the SDN has to be researched in order to understand that how significant is the security with the SDN. In order to conduct further research for evaluation of the SDN security, a combination of the systematic literature review and experimental research would be better. 2. Dynamic load balancing for multiple SDN-controllers: For load balancing and fault tolerance in the SDN environment, the use of multiple SDN-Controllers is suggested. How these multiple controllers communicate with the switches and how they dynamically balance their load has to be further investigated. Experimental research approach is suggested in order to solve the problem of dynamic load balancing between multiple controllers in the SDN environment. In the near future, SDN will be adopted and deployed by various businesses and IT companies due to the benefits of SDN. Various vendors of the network devices are implementing SDN and are producing SDN-enabled network devices. Some organizations such as Open Networking Foundation (ONF) are working for the development of protocols, which communicate between the controller and the SDN-enabled switches. These protocols will be alternatives to the OpenFlow.

References

1. Tuysuz, M. F., Ankarali, Z. K., & Gözüpek, D. (2016). A Survey on Energy Efþciency in Software Deþned Networks. *Computer Networks*. https://doi.org/10.1016/j.comnet.2016.12.012.
2. Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and Software-Defined Networking. *COMPUTER NETWORKS*, *81*, 308–319. https://doi.org/10.1016/j.comnet.2015.02.026 .
3. Watson, R. T., & Webster, J. (2002). Analysisng The Past to Prepare for The Future: Writing Literatur Review. *MIS Quarterly Vol. 26 No. 2, Pp. Xiii-xxiii/June 2002*, *26*(2). https://doi.org/10.1.1.104.6570.
4. Yan, Q., & Yu, F. R. (2015). Distributed Denial of Service Attacks in Software- Defined Networking with Cloud Computing, (April), 52–59.

5. Yan, Q., Yu, F. R., Member, S., Gong, Q., & Li, J. (2015). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments : A Survey , Some Research Issues , and Challenges, (c), 1–23. https://doi.org/10.1109/COMST.2015.2487361

6. Yang, B., Tan, F., & Dai, Y. S. (2013). Performance evaluation of cloud service considering fault recovery. In *Journal of Supercomputing* (Vol. 65, pp. 426–444). https://doi.org/10.1007/s11227-011-0551-2.

7. Yen, T. C., & Su, C. S. (2014). An SDN-based cloud computing architecture and its mathematical model. In *Proceedings - 2014 International Conference on Information Science, Electronics and Electrical Engineering, ISEEE 2014* (Vol. 3, pp. 1728–1731). https://doi.org/10.1109/InfoSEEE.2014.6946218.

8. Yigitbasi, N., Iosup, A., Epema, D., & Ostermann, S. (2009). C-Meter: A framework for performance analysis of computing clouds. In *2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGRID 2009* (pp. 472–477). https://doi.org/10.1109/CCGRID.2009.40.

9. Yoon, C., Park, T., Lee, S., Kang, H., Shin, S., & Zhang, Z. (2015). Enabling security functions with SDN : A feasibility study. *Computer Networks*. https://doi.org/10.1016/j.comnet.2015.05.005.

10. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18. https://doi.org/10.1007/s13174-010-0007-6 .

11. Zhang, Y., Cui, L., Wang, W., & Zhang, Y. (2018). A survey on software defined networking with multiple controllers. *Journal of Network and Computer Applications*. Elsevier Ltd. https://doi.org/10.1016/j.jnca.2017.11.015 .

12. Zhu, G., Yin, Y., Cai, R., & Li, K. (2017). Detecting Virtualization Specific Vulnerabilities in Cloud Computing Environment. In *IEEE International Conference on Cloud Computing, CLOUD* (Vol. 2017–June, pp. 743–748). https://doi.org/10.1109/CLOUD.2017.105.

13. Zissis, D., & Lekkas, D. (2010). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006