Software-Defined Networking in Cloud Computing

Mulumba Banza Gracia
Department of Information Technology
Tshwane University of Technology,
PRETORIA, Rep. of South Africa
Email: Mulumbagracia7 [AT] gmail.com

Lebogang Maaka
Department of Information Technology
Tshwane University of Technology,
PRETORIA, Rep. of South Africa
Email: maakalebogang [AT] gmail.com

Sphiwe Promise Ndlovu
Department of Information Technology
Tshwane University of Technology,
PRETORIA, Rep. of South Africa
Email: sphiwepromise96 [AT] gmail.com

Vusumuzi Malele
Department of Information Technology
Tshwane University of Technology,
PRETORIA, Rep. of South Africa
Email: malelev [AT] tut.ac.za

Abstract—**Through network programmability, we may simplify network management and bring innovation, cloud computing introduced some of its network concepts. One of the most prominent cloud models for minimizing maintenance obligations and simplifying network infrastructure administration is the SDN (Software Defined Network) architecture. SDN stands out because it provides separation of the control plane and programmability for developing network applications. As a result, SDN is expected to enable more efficient configuration, higher performance, and increased flexibility to support new network architectures. This article is aimed to demonstrates the importance of the SDN and the major role it plays in the organization and how SDNs can be profitable to many organizations that remain in the archaic or a traditional cloud environment and how SDN can restructure the cloud architecture with more security enhancement and also to investigate SDN related issues and challenges to provide insight into the obstacles that this revolutionary network paradigm will face in the future, from both a protocol and architecture standpoint. In this study, systematic literature was conducted and descriptive was used to analyze data. When it comes to SDN, the following challenges and issues stand out: All of these phrases are used to characterize the properties of a system: scalability, high availability, reliability, elasticity, security, performance, resilience, and dependability.**

Keywords-component: Software Defined-Networking(SDN), Cloud computing, systematic literature.

I. Introduction

SDN (Software Defined Network) is the latest trend in network architecture that brings a monumental revolution in the network paradigm. In the Old and traditional network architecture, the network was vertically integrated meaning the control plane (the engine allowed to determine how the network traffic should be managed) and the data plane (the engine allowed to send and forwarding traffic based on the control plane decision). Both were integrated inside the same device, which made the network less flexible, blocking the evolution of network infrastructure and made the network relying on the hardware. SDN is a novel technology that pushes conventional network topologies to their limits. To address the issue of network traffic that is vertically integrated, The control plane and the data plane mechanism are separated by SDN. The switch stays in a simple transporter with the control logic contained in the logically centralized controller when the control plane and data plane are separated.

The motivation behind this article is to demonstrate how SDN can be a solution to many organizations because of what it has offered and its benefits such as SDN does not rely on the hardware network device but rather a software-based network that opens up ways for innovation.

This article discusses how SDN enables a network to shift to a software-based controller rather of depending on a hardware network device. Built-in programs can also run on top of the network operating system thanks to SDN.

II. Literature Review

A. Software Defined Networking

The primary goal of Software DN is to facilitate a communication network, to transport data from a source location to a destination. Data travels across numerous nodes within the network, and the control given by network applications and services supports efficient and effective data transfer (forwarding) [1]. SDN is relatively new method that paves the way for on-demand virtualization of network resources. The applications in the upper layers benefit from a simplified version of the underlying network [2].

The SDN (Software Defined Network) simplify application deployment and enable flexible delivery by enabling organizations to increase network resources and save on both CapEx (Capital Expenditure) and OPEX (Operational Expenditure) to meet the needs of their applications and data. SDN has its own way to build, develop and manage networks, and decoupling network control (control plane) and transport procedures improves the user experience (data plane). With its concept of separating the data-forwarding hardware from the control plane, SDN has opened up new possibilities in networking, enabling the network to be dynamically programmable, customisable, and re-configurable [3]. This network segment has various benefits in terms of network flexibility and controllability. System virtualization and cloud computing can be combined to create centralized intelligence that will facilitate network management and maintenance and improve network control and responsiveness. Implementation, configuration, and troubleshooting of networks, as well as existing infrastructure, require advanced technical support from network and systems engineers, as well as the cost of provisioning and managing large-scale multi-vendor networks. Its maintenance costs as a result of the diversity and complexity of network components, especially when backup plans are not in place, in the event of frequent network failures, can reduce the reliability of the underlying infrastructure.

B. Securing networking environment with SDN

DDoS (Distributed Denial of service) is a form of widespread flooding attack which is one of the most common ways to disrupt cloud computing availability attacks. Availability is one of the most importance role in the cloud because the cloud is based on-demand services. Because of the SDN's features, such as software-based traffic analysis, logical centralized control, a network-wide perspective, and dynamic forwarding rule updating, identifying and responding to a DDos assault in the cloud is straightforward. [4].

In order to minimize security breaches or DDoS attacks, we need to devise an SDN security strategy that achieves the optimal balance of network speed and security features. A third layer, the security layer, is introduced in addition to the data layer. The security layer is responsible of transporting security-related data between the controller's third-party software module and the switch's third-party interface [5].

Similarly, in the cloud environment, as more personal and commercial data is outsourced, the recent advent of cloud enabled application has raised security concerns. In the past, single system and service security was given a lot of attention. Because a large number of services and systems coexist on one virtualization layer without knowing one other. Nowadays cloud systems and services necessitate a more intensive security implementation [6].

C. SDN in cloud computing

Nowadays it is very challenging to administer a network. Network administrators frequently struggle with low-level vendor-specific configurations when attempting to implement sophisticated high-level network policies, monitor and offer secure network connectivity. Recently, SDN has emerged as the networking industry's next big thing. SDN is a new network that enables network administrators to manage and control more network devices, traffic paths, and packet processing (quality of service) regulations using high-level languages and APIs. Gives you the ability to manage and customize your network. The role of SDN in cloud computing is to enable users to respond quickly to changes. SDN management creates network configurations more efficiently and enhances network performance and monitoring. In this review article, we explored the importance of SDNs, the key roles that organizations play in SDNs, and how SDNs can benefit many organizations.

The authors in [7] describes the various features of SDN, the best cloud computing networking solution. It also provides a way to detect SDN-based DDoS attacks in the clouds by taking advantage of the SDN properties. The method they propose detects DDoS attacks with very low communication and computing costs. In [8] proposes to use an SDN controller to detect attacks to generate a switch flow for each new incoming connection, so that the remaining received packets are sent to the destination without any additional processing. Therefore, every time the controller detects a packet it is considered a new packet.

The SDN architecture has been used in various security-related investigations to detect cloud network intrusions [9] adopts OpenFlow as a flow orchestration tool to monitor cloud traffic. The basic idea is to use OpenFlow to change the flow of packets and let the network intrusion detection system go through the deployed path [10, 11]. There is no need to transport or reinstall NIDS devices when implementing the SDN architecture. OpenFlow adds router and switches flow rules to handle packets passing through the path to the watchdog. Their research provides several strategies for discovering the shortest route to a safe route. These are categorized according to how long the controller takes to find them. OpenFlow allows researchers to do experiments on variety of switches consistently with high port density and line rate, without having to understand the internal design of the manufacturers switches [12].

The work by [13] describes a study on the improvement of wireless mobile network security. As wireless mobile networks become the primary means of accessing the Internet, it is important to maintain the growth rate of users. For example, the demand for network capacity for mobile data traffic has recently outpaced the current network supply. According to [14] The apparent absence of guarantees of the entire network of current solutions in terms of QoS is one of the key reasons for the slow adoption of wireless technology in industrial control applications. Algorithms for improving service quality in industrial wireless sensor networks. In their work [15] discussed network concerns in IaaS as well as federation challenges that are currently being handled using available technology. They also offer fresh software-defined networking approaches that alleviate some of the concerns and could be used in future deployments as efficient solutions.

The INMCS (Integrated Network Management and Control System) framework integrates SDN's end-to-end flow provisioning and control proposed by [16]. We believe that hybrid control is needed to gradually introduce SDN capabilities into today's networks. According to a survey by [17] despite the investigation of cloud computing SDN, there remains a hole that needs to be buried and investigated. Using taxonomy, the authors go over the advantages of SDN-enabled cloud computing. Exams using SDN in data center power efficiency, traffic engineering, network optimization, and virtualization were evaluated in detail, and cloud computing is emerging. It also describes the various simulation and experimental evaluation methods. As a final step, they identify research gaps and provide recommendations for future research efforts.

They look at the security challenges that new technologies encounter in the context of the new communications paradigm in their study [18]. To address these issues and safeguard the 5G software-defined mobile network, they therefore provide multi-tier component-based security plan that manages security at multiple levels to protect the network and its users (SDMN). To increase security in the control and data planes of SDMNs, the presented approach includes components for encrypted communication, policy-based communication, sensitive information and event management, security defined tracking, and deep packet inspection.

The authors in [19] present examples of how SDN may help with a variety of big data issues, such as cloud data center big data processing, data delivery, joint optimization, scientific big data architectures, and scheduling concerns. They demonstrate how, by appropriately regulating the network, SDN may improve the performance of huge data applications. They also discuss how big data may assist SDN in areas such as traffic engineering, cross-layer design, cyber risk mitigation, and SDN-based inter and intra data center networks. There were also a number of unresolved concerns that needed to be addressed before big data and SDN could be used in future experiments.

D. General observation from the reviewed works

Along with the spread of flexible appliances such as intrusion detection systems and firewalls, policy enforcement, and topologically dependent complexity, where applications are migrated from on-premises servers to cloud services [20].

As well as guaranteed performance issues. SDN` Unique and dynamic network design allows you to transform your existing network backbone into a rich service delivery platform.SDN-based design eliminates the basic infrastructure for applications that use it by separating network control and data plane. It can be programmed and managed. Network architecture at any time.

III. METHODOLOGY

A. Techniques used in the literature review

The following techniques are used for literature review:

- Searching several databases and information sources for qualifying research, including grey literature sources, with no language constraints.
- To avoid random or systematic errors in the process, more than two separate reviewers select papers, extract data, and assess risk of bias in a duplicate fashion.
- Using quantitative and qualitative tools to analyze data.
- Figures with summary of findings are used to present the findings.
- Making sense of the data and reaching conclusions.

B. The approach used in data collection.

The literature was searched against recognized and validated publications and databases for both information systems and information science research.

List the units for each quantity used in the equation. The databases and journals that were used include:

- Google Scholar (https://scholar.google.com/).
- Scielo (http://www.scielo.org.za/).
- Semantic Scholar (https://www.semanticscholar.org/).
- Science.gov (https://www.science.gov/).

The method selected was to scan the most important information from published journals obtained by conducting a search using the required keywords. After scanning the abstracts and determining whether they were relevant.

To construct a piece of robust information, will need to gather critical data and we will summarize all of that through steps.

- The first step in collecting and constructing data is observation; Observation is a method of obtaining information by observing people, events, or physical characteristics in their natural environment. Observational data collection strategies have the advantages of direct access to research phenomena, a high level of adaptability in terms of application and the creation of permanent records of occurrences that can be returned later. Time constraints and observer bias are also issues of observation strategy, as well as the observer's influence on the core data.

- The second step is the Research topic area. When conducting research, a researcher's research topic is a subject or issue that piques their interest. The foundation of any successful research effort is a well-defined study topic. Researchers examine, define, and polish their ideas while deciding on a topic.
- The third step is to build a hypothesis meaning a research hypothesis is a distinct, explicit, and testable proposition or prediction regarding a scientific research study's likely outcome.
- The fourth step is to test with experiment if the hypothesis made prior will be confirmed, testing will tell us how much information or expertise we've gained. We may also utilize testing as a significant step in the overall process to see if goals are being accomplished.
- An evaluation of facts using statistical or logical techniques will be carried out in the fourth step, which is data analysis. Assuring data integrity requires detailed and proper analysis of study findings.
- The last step where we provide a summative report and a brief conclusion.

C. Existing network cloud-based models

NaaS is one of several cloud-based technologies for improving network capabilities and enabling network management of the underlying infrastructure. For example, you can support NaaS, boost speed, and obtain global visibility of your network using the OpenFlow-based SDN paradigm. Users can use various trusted applications to take advantage of the extended network capabilities. Some of the most important challenges and issues in the SDN environment are: Scalability, High Availability, Reliability, Resilience, Security, Performance, Resilience, Reliability are terms used to describe the characteristics of any system. Other cloud-based approaches include the network virtualization paradigm and the evolutionary model. To enable scalability in VLANs, the network virtualization concept can be used for SDN. Using this technique, multiple virtual network instances can be created in a single physical infrastructure. In joint-tenant circumstances, this architecture was designed to address issues like subnet mobility and isolation. Quality of service, fault tolerance, and configuration management are all provided by the evolutionary model, which separates the network into virtual segments.

As part of traditional networking, routers and switches employ integrated hardware and software to route traffic between them. To virtualize the network,Separation of the control and data planes is required. Data centers are equipped with a smart controller that runs specialized software and a series of switches that forward packets. Virtualizing a network has its advantages, as well as drawbacks. Dynamically spinning up and down networks is possible. Specific applications can benefit from their utilization, and security policies can be installed on each network. As the market for SDN matures, it is expanding beyond the data center. Wide Area Networks (WANs) employ SDN to govern how organizations connect to their branch office locations. It combines multiple types of network connections, such as broadband, MPLS, or wireless, with software to provide powerful and cost-effective connections. One such application is SDN-WAN. SDN security is based on micro-segmentation. Certain networks can carry sensitive data and be secure. If a hacker gains access to a public-facing web server, he or she is restricted to the server part of the network, rather than the entire network. Other components such as the secured data center network are not accessible by hackers.

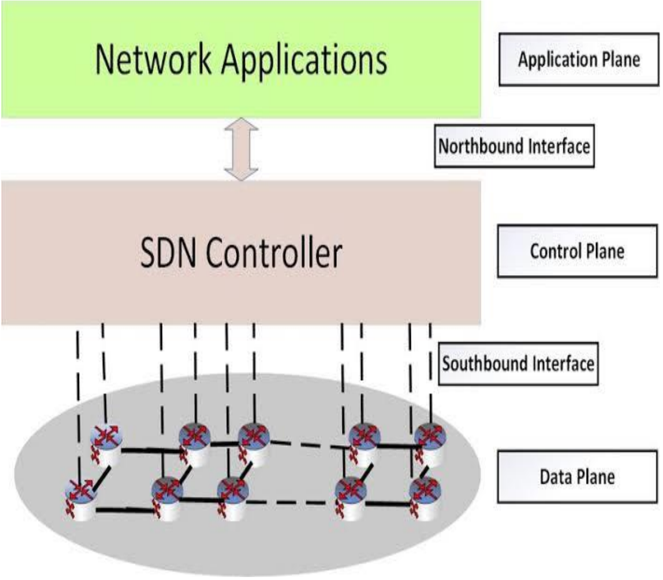

Figure 1. SDN block diagram (Source: adapted from [9])

IV. Results and Discussion

Since 2011, the demand and need for research on SDN, as well as its problems and impacts, has increased, according to the review. After finding no relevant articles in 2010 and one relevant item in 2011, the first increase occurred in 2012, with seven relevant articles. In 2013, 22 articles dealt with the challenges and implications of SDN, while 14 articles dealt with the topic again in the first half of 2014. SDN is becoming more relevant over time, as evidenced by the temporal analysis, with more study and analytical methodologies predicted in the next years.

The problems and implications of SDN are represented in Figure 1. The majority of publications emphasize the difficulty of implementation. This category contains the most debated and investigated factors, such as vendor lock-in effects and the high risk of changing established network topologies. The category of demand receives the secondhighest amount of attention. Security challenges coming from software-defined networking, as well as the end-constant user's high demand and anxiety of changing traditional networks, are all included in this category. The third group covers software-defined networking know-how. This category included the administration and control of software-defined networks with current workers, as well as the overload that resulted.

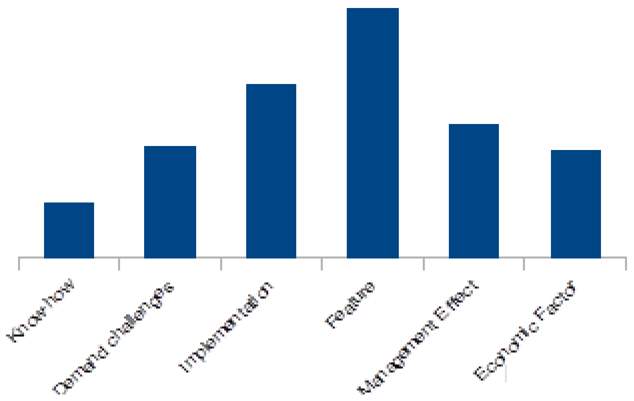

Figure 2. Classification of SDN in several publications.

Figure 2 also demonstrates that in the publications examined, the distinctive aspects of software-defined networking are discussed the most. Separating hardware and software, in addition to a broad overview of the complete network architecture, fall under this category. When describing the consequences of software-defined networks against traditional networks, the second category – management – is crucial. This main area includes easier policy implementation, network programmability, and network maintenance. Finally, there are economic issues to consider, such as cost efficiency and cost reductions for specialized and skilled personnel. These tendencies indicate that current research is mostly concerned with technical and scientific issues.

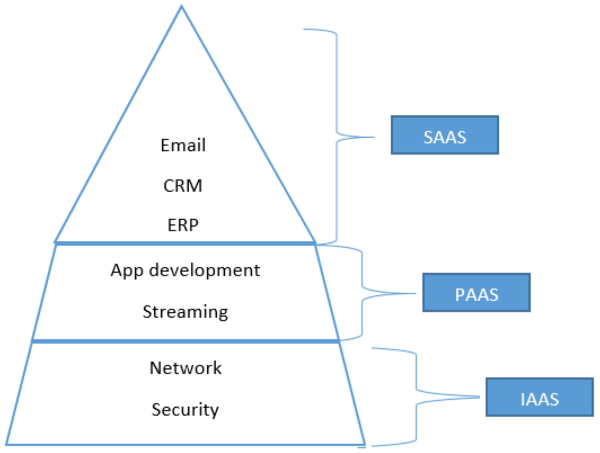

Figure 3. A summary of several publications addressing the issues and impacts of SDN.

To show the incredible amount of work that has already been done in this area, we will focus on cloud security rather than network security in this paper. Information on individuals and enterprises is increasingly being stored in the cloud because it allows capacity (bandwidth, storage, processing power) to be dynamically expanded or added without the need for new infrastructure.

This raises questions regarding the security of such an ecosystem. As a result, significant work was placed into three major aspects of cloud which are illustrated in the Figure 3.

- Software as service: SaaS can be broken down into several different security concerns. The purpose of this paper is to give a high-level summary without going into too much detail. In this delivery paradigm, network security is frequently supplied using well-known SSL encryption endpoints that are dependent on the cloud provider.
- Platform as Service: aims to give a client more control over the platforms on which they build and develop apps. As a result, the provider must be aware of security concerns below the application level.
- Infrastructure as Service: Customers who use IaaS must be aware of all potential security risks with their systems, except for a security flaw in the environment's hypervisor. Since the increasing virtualization of everything in the information society, data control, regardless of its physical location, has piqued people's curiosity

Security in cloud providers' networks differs from that in traditional networks since their networks are far more dynamic than traditional networks. To change the network's behavior in traditional networks, an administrator or a small group of administrators would have to modify a specific routing table item or access control list. The traffic flow or access to appropriate resources cannot be maintained in highly dynamic networks, such as cloud environments, where virtual machines and processing power are assigned and removed in short periods without user intervention. Unprotected machines, for example, can provide access to a previously specified target running within the same cloud environment, which is another security weakness in cloud setups.

To avoid such security risks in a cloud environment, access and security policies must be implemented soon after a system is set up and revised after each system modification. A proposal must be known of all available services and risks in a cloud-based system. This will be guaranteed through a necessity for a beginning input amid the setup handle of a modern system, which includes important system information, but it needs to be overhauled persistently.

V. Conclusion

SDN (Software Defined Network) is a revolutionary network design that claims to simplify network administration, increase network resource usage, and accelerate network growth and innovation. By separating network functionality from data forwarding devices into conceptually centralized distributed controllers, SDN enables the abstraction and centralized management of lower-level network capabilities. For each gap, we identified future research directions that must be taken to fill them. The construction of a policy language suitable for hybrid SDN networks, as well as the development of automated protocols for network management and upgrading, are the two primary future research topics. Because of these issues, future study is restricted. For SDN networks, it's also critical to establish good measuring techniques and modeling tools.

References

[1] S. Sezer, S. Scott-Hayward, P.K. Chouhan, B. Fraser, D. Lake, J. Finnegan, and N. Viljoen, "Are we ready for SDN? Implementation challenges for software-defined networks", IEEE Communications Magazine,vol.51,2013,pp.36 - 43,Accessed on September. 10,2021. [Online]. Available doi: 10.1109/MCOM.2013.6553676

[2] K. Govindaraj, K.C. Meng and H. Ong, "A literature review on software defined networking (SDN) research topics, challenges and solutions", 2013 fifth International conference on advanced computing(ICoAC), 293-299.

[3] K Benzekki, A El Fergougui and A.E. Elalaoui, "Software-defined /networking (SDN): a survey", Laboratory of Computer Networks and Systems, Department of Mathematics and Computer Science, 9.

[4] Q. Yan, F.R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE Communications Surveys & Tutorials, 2015, 18, pp. 602-622. Accessed on September. 10, 2021. [Online]. Available doi:10.1109/COMST.2015.2487361.

[5] A Hussein, Imad H. Elhajj, A Chehab, A Kayssi,"SDN Security Plane: An Architecture for Resilient Security Services", 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), 2016, Accessed on September. 10,2021. [Online]. Available doi: 10.1109/IC2EW.2016.15

[6] S Seeber, G.D. Rodosek, "Improving network security through SDN in cloud scenarios",10th International Conference on Network and Service Management (CNSM) and Workshop, 2014. Accessed on: September. 10, 2021. [Online]. Available doi:10.1109/CNSM.2014.7014198

[7] K. Bhushan and BB Gupta " Detecting DDoS attack using software-defined network(SDN) in cloud computing environment", 5th international conference on signal processing and integrated networks (SPIN), 2018

[8] S.M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers", International Conference on Computing, Networking and Communications, Communications and Information Security Symposium, 2015.

[9] G. Gu and S. Shin, "cloud watcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: how to provide security monitoring as a service in clouds?), "20th IEEE International conference on network protocols, pp. 1-6, 2012,

[10] J. Medved, R. Varga, A. Tkacik, and K. Gray, "OpenDaylight: Towards a Model-Driven SDN Controller architecture", Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2014. Available online doi: 10.1109/WoWMoM.2014.6918985

[11] R Amin, M Reisslein, N Shah,"Hybrid SDN Networks: A Survey of Existing Approaches", IEEE Communications Surveys & Tutorials, 20(4), pp.3259-3306.

[12] S. Vissicchio, L. Vanbever, and O. Bonaventure, "Opportunities and research challenges of hybrid software-defined networks," ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 2, pp. 70–75.

[13] A.Y. Ding, J. Crowcrofy, S. Tarkoma, and H. Flinck, "Software-Defined Networking for security enhancement in wireless mobile networks", computer networks, 2014, 66, pp. 94-101.

[14] M. Kumar, R.F. Tripathi, and L. Xu, Design & test of radio communication and control system for aquaculture. Sensors & Transducers, 2013, 21(5), pp. 8-14. Available from http://0-search.proquest.com.tkplib01.tut.ac.za/docview/1508499119?accountid=42821. [Accessed 11-08-2018]

[15] A. Alshamrani "A defense system for defeating DDoS Attack in SDN based Networks", Proceedings of the 15th ACM international symposium on mobility Management and Wireless Access – MobiWac'17, 2017.

[16] P. Sharma, S. Banerjee, S. Tandel, R. Aquiar, and R.A. David, "Enhancing network management frameworks ith SDN-like control", IFIP international Symposium on integrated Network Management, 2013.

[17] J. Son, and R. Buyya, "A taxonomy of software-defined networking (SDN)-enabled cloud computing", ACM computing surveys (CSUR), 2018, 51(3), pp.1-36.

[18] M Liyanage, I Ahmed, J Okwuibe, M Ylianttila, H Kabir, J.L. Santos, "Enhancing Security of Software Defined Mobile Networks", IEEE Access, 2017, 5, pp. 9422-9438. Accessed on September. 10,2021. [Online]. Available doi:10.1109/ACCESS.2017.2701416

[19] L. Cui, F. Richard Yu, and Q. Yan, "When big data meets software-defined networking: SDN for big data and big data for SDN", IEEE Network, 2016, 30, pp.58 - 65. Accessed on September. 10,2021. [Online]. Available doi: 10.1109/MNET.2016.7389832.

[20] S.A.P. Wieder and R. Yahyapour, "Cloud computing networking: challenges and opportunities for innovation", 15th international conference on transparent optical networks (ICTON), 2013, pp. 1-4.