Proceedings of the Third International Conference on Smart Electronics and Communication (ICOSEC 2022)
IEEE Xplore Part Number: CFP22V90-ART; ISBN: 978-1-6654-9764-0

A study of cloud-based VPN establishment using network function virtualization technique

Sankili Santhanamahalingam
Department of Computer Science and Engineering.
Kalasalingam Academy of Research and Education,
Anand Nagar, Krishnankoil,
Tamilnadu, India
sankili@gmail.com

Saravanan Alagarsamy
Department of Computer Science and Engineering.
Kalasalingam Academy of Research and Education,
Anand Nagar, Krishnankoil,
Tamilnadu, India
senthilsar@gmail.com

Karthikeyan Subramanian
Department of Mechanical Engineering.
Kalasalingam Academy of Research and Education,
Anand Nagar, Krishnankoil,
Tamilnadu, India
scorthik@gmail.com

2022 3rd International Conference on Smart Electronics and Communication (ICOSEC) | 978-1-6654-9764-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICOSEC54921.2022.9951894

Abstract— **Network Function Virtualization is the process of moving networking functions like Firewall, Load Balancing, Virtual Private networks (VPN), Gateway Antivirus, etc. away from proprietary hardware to the virtual server. This paper suggests enabling VPN security features to business customers by moving VPN features away from dedicated hardware and applying the feature by instantiating the corresponding VNF template from the virtual server. This paper aspires to develop a suitable architecture model with Software-Defined Network and Network Function Virtualization as its core techniques that can render a cloud design for VPN.**

The proposed model consists of three parts that include forwarding plane, signaling & control plane, and data plane. The forwarding plane contains a tunnel that can be accomplished with technologies such as VPN, VXLAN, etc., and policy information. The signaling & control plane contains entire topology information, Bgp-evpn protocols, SDN controller functions, and NFV Orchestrator functions. The Data plane contains an open flow protocol and underlay network components such as distributed switch or router to handle L2-L4 rules. The model is evaluated using a simulation on a testbed with order processing and order orchestration of the cloud VPN feature.

Keywords— Network Function Virtualization (NFV), Software Defined Networking (SDN), cloud-based Virtual Private Network (VPN), Network as a Solution Virtual Private Network (NaaS VPN).

I. INTRODUCTION

L3 VPN is used by telecommunication service providers to route traffic between branch offices and headquarters locations for enterprise customers. To provide VPN connectivity, the device at the customer premise is connected with the provider edge router (PE Router) of the service provider, and thereafter traffic will be exchanged between branch office and headquarters as part of routing with the help of provider routers (P Routers) that take care of transiting traffic within core network of telecom service provider (TSP). Telecommunication service providers use a Wide Area Network (WAN) topology to interconnect numerous Local Area Networks (LAN) of enterprise customers. An overlay network for VPN can be created as part of WAN on top of the underlay network to connect enterprise networks. In traditional networking, Multi-Protocol Label Switching (MPLS) technique is most widely used to exchange label binding information to support hop by hop traffic forwarding. In this technique, labels are used to route packet information instead of IP Addresses. Due to the high cost associated with the MPLS technique for the creation of VPN, service providers are moving towards a cloud-based approach to deliver VPN to business customers at low cost and to reduce higher build time. The SDN approach majorly implemented at Customer Premise Equipment (CPE) devices that are located at customer's premises and these devices could be of terminal/ modem/ adapter or any other device which can be owned by the customer or leased from telecommunication service provider. The cloud-based approach relies on Customer Premises Equipment devices rather relying on service provider's edge (PE) network. In contrast to cloud-based approach, MPLS majorly relies on Provider Edge (PE) devices of service provider's edge network.

Delivering new services to customers is often delayed by traditional network service models due to higher build time. The cloud-based offerings let telecommunication service providers instantaneously deliver networking services (like firewall, VPN, etc.) securely to thousands of user groups. The traditional network infrastructures are not scalable, not efficient, and non-resilient, and the network resources are considered on-premise resources. Hence the network can't be built and operated at varying demands.

The cloud-based infrastructures are highly scalable, efficient, and resilient. They enable networking space to be built and operated at any scale based on any peak demands. A proof of concept is implemented on a testbed for cloud-based VPN enablement with OpenStack as a cloud management platform. Results showcase that the strategy followed for cloud-based VPN enablement is an effective solution and they prove that services will be delivered with a shorter build time and peak demands can be provisioned 'just in time', which makes it possible to share networking resources across applications and thus drastically reduces cost.

Though cloud-based approach brings several advantages to the table, it also brings various complex technical issues, like: a) Selection of appropriate software controller according to the need and position it either as on-premises component or cloud component b) Selection of proper and distinct cloud architecture to orchestrate cloud resources such as: compute, storage, network, etc. as part of NFV orchestration c) Scalability and Reliability of entire architecture if number of components grow in size; and few others.

This paper targets to develop a distinct cloud architecture to move VPN function away from proprietary hardware and make it available as virtual function from cloud management platform. The traffic from Customer Premise Equipment

(CPE) will be steered programmatically and VPN function will be delivered from virtual server.

Precisely, this model triggers an order from Order Entry system and afterwards order fulfillment happens at Operation Support System (OSS) layer that does Order Management and Order Orchestration and triggers a notification to Cloud Management Platform that will orchestrate necessary cloud resources to create corresponding Virtual Machine (VM) with necessary components according to VNF template.

The paper is assembled as follows: Section II consists of the related works. Section III details about methodology being examined this paper and the problem statement. Section IV showcases simulations and simulation results. In the end, Section V extracts conclusions of proposed work covered in this paper.

II. Related Works

Telecom service providers (TSPs) build an enterprise's protected access networks to obtain private access from the public internet which is termed a virtual private network (VPN). There are multiple different types of VPN in accordance with OSI layer(L2/L3) in which it is implemented, for an instance, a VPN implemented in Layer 2 of the OSI layer is termed as L2 VPN, a VPN implemented in Layer 3 of OSI layer is termed as L3 VPN. Telecom service providers prefer to use either tunneling techniques or encryption techniques to safeguard connections through the unscreened network, for ex: public internet between customer edge network and provide edge network. In the telecommunication world, numerous techniques are used to achieve private connectivity for enterprise customers. Among them, VPN is one of the techniques that permit carrying out the traffic/data which is private to an enterprise by using public internet networks.

Numerous institutes have given definitions for VPN, among them these two definitions given by the National Institute of Standards and Technology (NIST) and Gartner are broadly popular. Gartner defined VPN as "a system that delivers enterprise-focused communication services on a shared public network infrastructure to provide customized operating characteristics uniformly and universally across an enterprise" [1]. NIST defined VPN as a virtual network that is built on top of existing physical networks to provide a secure communications mechanism for transmitted data and other information in between networks [2].

VPN connectivity is broadly divided into two types: Remote Access VPN & Site to site VPN [3]. Remote Access VPN is usually used by retail customers to connect them to the company's intranet from any remote place. Remote Access VPN uses VPN protocols like SSL, IPsec, PPTP, and L2TP to achieve remote access connectivity between the customer site and the company's site location [3]. SSL VPN: It is a secured socket layer VPN that uses the SSL encryption technique to deliver remote traffic access to retail customers [4]. IPsec VPN: It is an internet protocol security VPN that enables remote traffic access based on encrypting IP packets along with source packet authentication [4]. As opposed to Remote Access VPN, Site-to-Site VPN routes traffic between multiple intranet sites of an enterprise customer that span across multiple geographic locations. Site-to-Site VPN uses VPN tunneling protocols like IPsec, Multi-Protocol Label Switching (MPLS), and Generic Routing Encapsulation (GRE) to connect different locations of an enterprise customer [4].

Intranet VPN: It is basically used to provide network access for employees within an organization. It enables traffic connectivity between different sites of a single enterprise to provide network access to employees belonging to an organization [5]. Extranet VPN: It is basically used to provide access to users outside or users who do not belong to an enterprise (e.g., outside customers, partners, suppliers, etc.) [6]. It primarily provides connectivity between one enterprise's local area network (LAN) with another enterprise's local area network (LAN) in order to allocate the same environment to both enterprises in a controlled and secured manner [7].

A VPN tunnel is used to supply an encrypted line to secure data through a public internet network. VPN tunneling technologies (e.g., IPsec, L2TP, and PPTP) are used to create VPN tunnels [8]. Both open-source implementations and commercial products are used to implement tunnelling technologies [9]. An automation technique to establish dynamic VPN in the NFV context has been proposed latterly [10]. The motivation of this automation is to establish security and encryption to connect functions like firewalls, load balance service, intrusion detection, protection service, etc. of service function chaining (SFC) [10], but it does not cater to building cloud-oriented VPN. A proposal is made to clearly demonstrate the demand for distinct cloud architecture to establish cloud-oriented VPN [11] and it details numerous advantages of establishing VPN service via the cloud, but it does not specify a particular architecture for cloud-orientated VPN.

A migration technique to migrate IT services to cloud-based services is brought forward [12]. In this technique, two options are chosen to protect IT resource access. One option is related to an open-source software option (pfSense) and another option is outsourced to an external body to provide VPN as a service to enterprise customers [12]. A SaaS model is brought forward by (Gupta, P. & Verma, A) to establish VPN as a service that is fully devoted to small and mid-size enterprises. The model proposed is to reveal the elastic VPN concept, but it requires improvements with respect to topology design [13].

III. METHODOLOGY AND PROBLEM STATEMENT

In traditional network service model [14], a typical router/ switch has both data plane and control plane coupled together and hence these elements are considered as tightly coupled elements. In general, data plane is responsible for packet forwarding and control plane is responsible for controlling the traffic that includes features like creation and maintenance of Virtual Routing and Forwarding (VRF) table, create an entry for each traffic/ route path, attach import and export Route Target (RT) details to each and every route created in VRF table, assign Route Distinguisher (RD) to routes maintained in VRF table, etc and coupling between these two elements make a router/ switch as vendor dependent device. Due to such restriction, it is hard to extend a router/ switch to accommodate new functions. The cloud-based architecture decouples data plane and control plane elements, facilitates service provider to move functions such as VPN, firewall, load balancing, intrusion detection and prevention, etc. to the cloud as part of virtualization and

allows service provider to program the network and implement routing features or control logic from a centralized controller and hence it simplifies network's control and allows service provider to switch traffic to less congestion route during network congestion. The centralized controller is a Software Defined Networking (SDN) controller that decouples control and data planes and hence Software Defined Networking (SDN) has become synonyms with decoupling the control and data planes [15].

The problem statement of cloud-based VPN establishment using network function virtualization technique is the following: With specific number of CPEs and internet/ broadband connections, the goal of this technique is to orchestrate compute, storage and network resources instantly in cloud management platform to create and manage VM for vRouter VPN service to minimize build and operation time associated with traditional MPLS technique and to provision VPN services as and when needed to serve peak demands via scaling up corresponding cloud resources and scale down them when demand goes down. Additionally, a scaling factor might have to be considered to achieve better optimization of dynamically changing system [16] and to achieve high availability of the system which brings uninterruptable service, elastic resource provisioning of cloud resources in cloud management platform is highly recommended [17].

To be specific, this work aims to develop a cloud-based VPN model to connect two CPEs, one at enterprise's branch office and another one at headquarters office, via two internet/ broadband connections and traffic will be interchanged between branch office and headquarters office via a communication channel that interconnects these two CPEs.

IV. SIMULATIONS AND RESULTS

A cloud-based VPN prototype was simulated as proof of concept. The simulation employs open-source software tools, such as OpenStack [18] as a cloud management platform and JBOSS Business Process Management tool (jBPM) [19] as Order Management and Order Orchestrator component. OpenStack is the most widely deployed cloud computing platform and it is used in this work to create, orchestrate and share compute, storage, and network space and OpenStack acts as an NFV Orchestrator (NFVO), VNF Manager & NFV-MANO Virtualized Infrastructure Manager (VIM). Also, simulation employs JBoss Business Process Management (jBPM) as Order Management and Order Orchestrator tool that lies in Operation Support System (OSS) vertical which is widely used open-source toolkit to automate business processes and decisions. The cloud-based VPN prototype's core implementation is done in Java and Spring Boot and these components are interfaced with jBPM according to JBOSS interface standards. The prototype receives order requests from the Order Entry system as input and uses a REST API interface which was implemented in spring boot to receive the request and to process the request, various workflow stages are defined in jBPM system to logically fulfill cloud VPN order. The business process management flow defined jBPM system does contain both automatic and manual tasks and manual tasks need user intervention to complete them which will mandate user to provide necessary parameters to fulfill cloud VPN order. The VNF template for vRouter VPN service is maintained and managed under the VNF catalog portion of OpenStack.

The VM for the VPN service is created by instantiating the corresponding VNF template which is stored under the VNF catalog. The cloud-based VPN Architecture Hierarchical view is depicted in Fig.1.

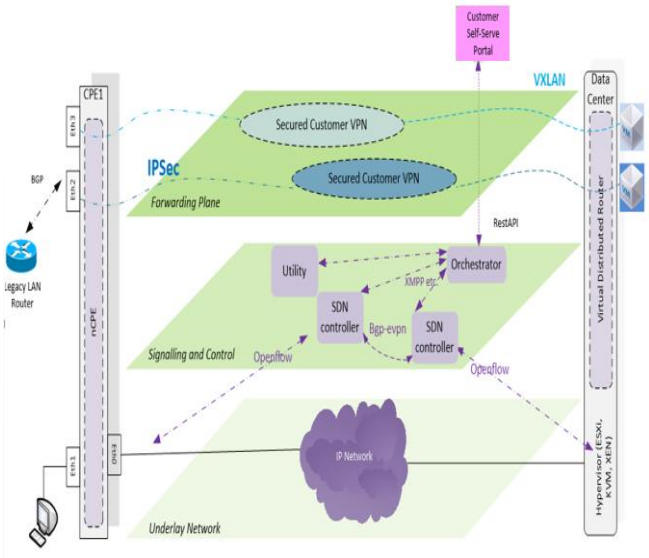

Fig.1.Cloud-based VPN Architecture Hierarchical View

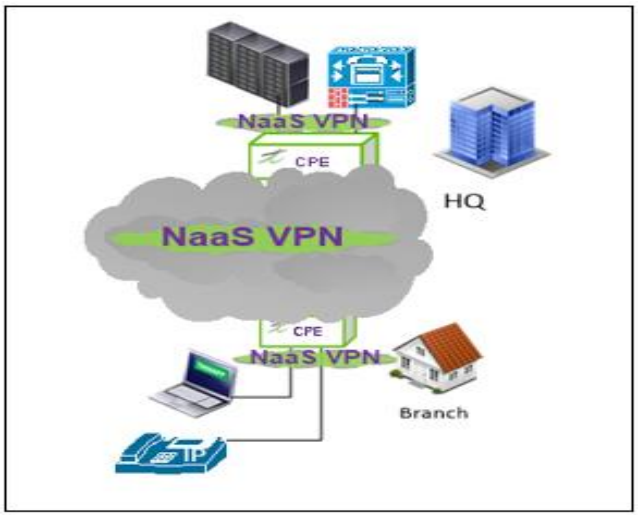

Fig.2.NaaS Enterprise VPN connectivity between branch office and headquarters office

The holistic view of cloud-based VPN connectivity between a branch office and headquarters is depicted in Fig.2. The diagram in Fig.3. details about high-level design of the cloud-based VPN Product Model with respect to L3VPN/ Managed VPN Product Order and Cloud Network Product Order. Also, it demonstrates the decomposition of L3VPN/ Managed VPN Product Order into L3VPN Customer Facing Service (CFS) order and the decomposition of Cloud Network Product Order into Cloud Network Customer Facing Service (CFS) Order.

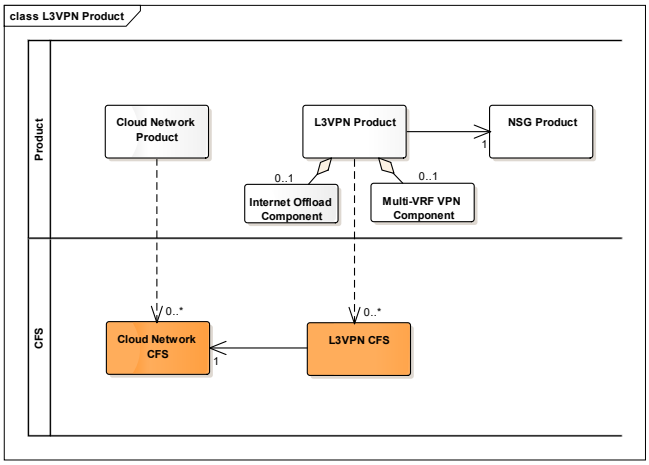

Fig.3. Cloud based VPN product model

A Sales Order of type Network as a Service – VPN with encryption will be submitted from Order Entry to initiate processing of Cloud VPN service. A new L3VPN/ Managed VPN Product Order and a new Cloud Network Product Orders will get created when Sales Order entered into bpm system as per catalog configuration and bpm flow will link newly created L3VPN/ Managed VPN Product Order with NSG product order and hence it provides the ability to create network services and bind a port on that NSG device to the newly created Cloud Network CFS. The link created between L3VPN/ Managed VPN Product Order and NSG product order provides NSG with the ability to create n number of connections based on the 'Number of Allowed Connections' parameter. Cloud Network CFS is an entity that is an instantiation/ realization of VPN cloud object. It is only created during configuration step either manually by the customer or automatically when there is no Network as a Service (NaaS) specific Cloud Network CFS.

Further L3VPN/ Managed VPN CFS and Cloud Network CFS are decomposed into multiple RFSes during order provisioning of L3VPN/ Managed VPN Product orders. The following list of RFSes will get created during the decomposition of L3VPN/ Managed VPN CFS: 1) Subnet RFS 2) Vport Bridge RFS 3) Interface Bridge RFS 4) Static Ip Binding RFS. The following list of RFSes will get created during the decomposition of Cloud Network CFS: 1) NSG RFS 2) Domain RFS 3) Zone RFS 4) QoE Policy RFS 5) Ingress ACL RFS 6) Egress ACL RFS 7) Forwarding ACL RFS 8) Ingress ACL Entry RFS 9) Egress ACL Entry RFS 10) Forwarding ACL Entry RFS 11) DNS Server RFS

A Heat template is created to instantiate vRouter VPN and it is made available under VNF Catalog. During the activation phase of L3VPN/ Managed VPN CFS and Cloud Network CFS, an initialization (or) activation request will be sent to OpenStack from the business process management (bpm) system and this will trigger the instantiation of vRouter VPN at OpenStack end. Heat Orchestration from OpenStack is used as NFV Orchestrator. Upon receiving the request from the bpm system, the orchestrator will look for the corresponding VNF template under VNF catalog, it will instantiate vRouter VPN template to create an instance or Virtual Machine (VM) for vRouter VPN and it will reserve and consume resources in accordance with the HEAT template defined for vRouter VPN.

The simulation was executed in OpenStack and VM which is instantiated under stacks section will consume following resources as per VNF template configuration - a Nova server instance as part of computing space, four Neutron resources (two ports for nsg/ vCPE, one internet port and one other port for management purpose) as part of network space, and a cinder volume as part of storage space and these resources are reserved and occupied per-site basis. After the creation of all necessary resources, the status of VM will get transformed from 'Create In-progress' to 'Create Complete' and a response will be shared to the bpm system to intimate completion of VM creation for vRouter VPN and the status of L3VPN/ Managed VPN product order in bpm system will get changed to Active. The status change of VM to Active indicates that virtual resources for vRouter VPN are orchestrated and occupied successfully for the service that is requested from bpm system.

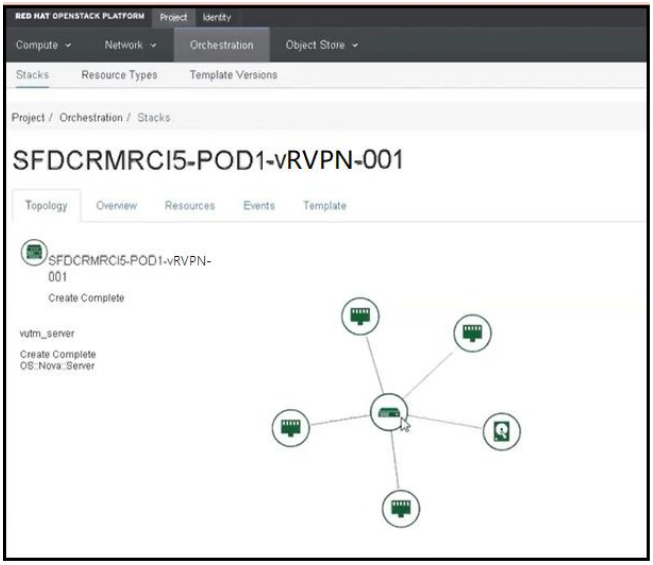

Fig.4. Instantiation of vRouter VPN in OpenStack cloud management platform

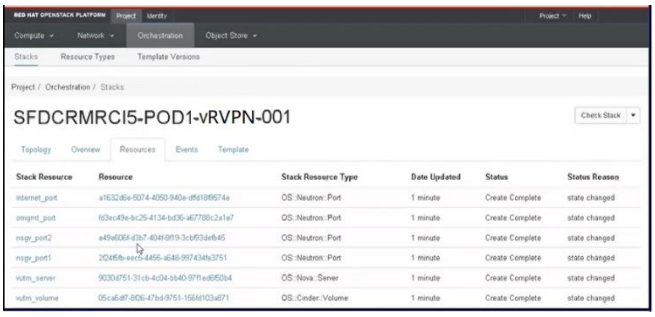

Fig. 5. Cloud Resources orchestrated for vRouter VPN in OpenStack cloud management platform

The diagram in Fig.4. shows spinning of a Virtual Machine (VM) for vRouter VPN when activation request is received in OpenStack cloud management platform and also it depicts status of VM created under Stacks section of OpenStack.
The diagram in Fig.5. shows cloud resources orchestrated and reserved upon creation of Virtual Machine (VM) for vRouter VPN in OpenStack cloud management platform.

V. Conclusion

In this work, an architecture for cloud-based VPN is proposed to orchestrate corresponding components both at the cloud NFV platform and OSS platform. This architecture ensures effective implementation of cloud-based VPN to provide communication links and reduces complexity, overhead, and cost associated with traditional VPN networking solutions. The proof of concept allows the conclusion that the proposed model delivers VPN with a shorter build time and serves peak demands as and when needed since cloud resources are reserved and occupied on demand basis. Future work in this area would be to protect vRouter VPN VM from complex attacks by applying a firewall at VM level rather than applying a firewall at the packet level and accomplish above said functionality with the help of Service Chaining to steer traffic programmatically to deliver additional functions like firewall, load balancing, etc. along with VPN function and bind those functions to provide end to end services should also be investigated.

References

[1] Gartner, "Virtual Private Network (VPN)," n.d.. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/vpn-virtual-private-network

[2] Frankel, S. et al., "Guide to SSL VPNs," National Institute of Standards and Technology (NIST), 2008.

[3] AM Gamundani, JN Nambili, M Bere., "A VPN Security Solution for Connectivity over Insecure Network Channels: A novel study," Int. Journal of Computer Science and Engineering (SSRGIJCSE), vol. 1, no. 7, pp. 3, September 2014.

[4] Y Bhaiji., Network Security Technologies and Solutions, Indianapolis: Cisco Press, 2008, pp. 505-618.

[5] Jeff Tyson. et a., "How a VPN (Virtual Private Network) Works" n.d.. [Online]. Available: <https://computer.howstuffworks.com/vpn.htm> [Accessed 8 November 2021]

[6] JM Stewart., Network Security, Firewalls, and VPNs, Second ed., Burlington: Jones & Bartlett Learning, 2014, pp. 402.

[7] P Rajamohan ., "An overview of remote access VPNs: Architecture and efficient installation," vol. 2, no. 11, pp. 3, November 2014.

[8] J Gokulakrishnan & VT Thulasi bai ., "A survey report on VPN security & its technologies," Indian Journal of Computer Science and Engineering (IJCSE), vol. 5, no. 4, pp. 3-5, 2014.

[9] T Berger., "Analysis of Current VPN Technologies," IEEE Computer Society, pp. 1, 2006.

[10] H. Gunleifsen, T. Kemmerich, and V. Gkioulos, “Dynamic setup of ipsec vpns in service function chaining,” Computer Networks, vol. 160, pp. 77 – 91, 2019.

[11] A. Z. Bhat, D. K. A. Shuaibi and A. V. Singh, "Virtual private network as a service — A need for discrete cloud architecture," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2016, pp. 526-532.

[12] F. A. Arshad, G. Modelo-Howard and S. Bagchi, "To cloud or not to cloud: A study of trade-offs between in-house and outsourced virtual private network," 2012 20th IEEE International Conference on Network Protocols (ICNP), 2012, pp. 1-6.

[13] Gupta,P. & Verma,A., "Concept of VPN on Cloud Computing for Elasticity by Simple Load Balancing Technique," Int. Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 5, pp. 1-5, May 2012.

[14] S. Troia, F. Sapienza, L. Varé and G. Maier, "On Deep Reinforcement Learning for Traffic Engineering in SD-WAN," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 7, pp. 2198-2212, July 2021.

[15] D. Saif, F. Arsiwala and I. Khanna, "Software Defined Networking in Next Generation Mobile Backhauls: A Survey," 2018 IEEE 5G World Forum (5GWF), 2018, pp. 106-111.

[16] W Haoxiang, S Smys. "Overview of configuring adaptive activation functions for deep neural networks-a comparative study." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 3, no. 01 (2021): 10-22.

[17] MD Pandian., "Survey on virtual load balancing architectures in mobile cloud." iro Journal on Sustainable Wireless Systems 1, no. 3 (2019): 161-175.

[18] Openstack Web: https://www.openstack.org/

[19] jBPM Web: https://www.jbpm.org/