

SIMPLIFYING ENTERPRISE NETWORKS: SD-WAN AS A CATALYST FOR SCALABLE AND SECURE CONNECTIVITY

Kshitij Mahant

Sr Technical Manager in Marketing, Simplifying Enterprise Networks: SD-WAN as a
Catalyst for Scalable and Secure Connectivity

kmahant87@gmail.com

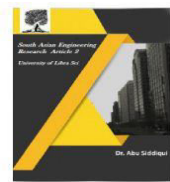
Abstract

In today's rapidly evolving digital landscape, enterprises require flexible, scalable, and secure network solutions to support cloud applications, remote workforces, and business growth. Traditional WANs, burdened with high costs and complex configurations, are increasingly inadequate for meeting these demands. Software-Defined Wide Area Networking (SD-WAN) offers a transformative approach by decoupling the control plane from the hardware layer, enabling centralized management, dynamic traffic routing, and enhanced performance. This paper explores how SD-WAN simplifies enterprise networks by improving scalability, reducing complexity, and ensuring secure, high-performance connectivity. It also highlights the integration of SD-WAN with cloud environments, its role in optimizing security through end-to-end encryption and threat intelligence, and its ability to lower operational costs. SD-WAN serves as a catalyst for next-generation network architecture, empowering organizations to stay agile while maintaining robust security.

Keywords: SD-WAN, enterprise networks, scalability, secure connectivity, and cloud integration.

1. Introduction

Comprising computational servers, data-storage systems interconnected with routers, and Internet-facing gateway devices, contemporary cloud data centres are built for business requirements, dispersed computations, and data-intensive applications. The most common security solutions in big Data Centre Networks (DCN) are often linked in series mode, which causes network congestion. These methods also become bottlenecks and only provide a limited level of protection in certain static network channels. Geographically dispersed around the world, computing resources—including networks and hardware/software—present difficulties for the linking network and its operations. Emerging paradigms like SDN/NFV are essential to meeting user requests in order to address this specific traffic orchestration and engineering problem. Features like programmability, flexible reconfigurations, dynamic policy enforcement, and global views are available in SDN-enabled networking topologies. Cloud service providers, data centre operators, and cyber-security professionals are very concerned about security and privacy. SDN may be a useful addition to traditional network environments, but it is now the most disruptive paradigm, reinventing network topologies, architectures, orchestration, and complicated policies [1] of cloud infrastructures, data centres, and huge applications. One of the quickly gaining paradigms in contemporary data centres is Network Function Virtualisation (NFV) [2], which provides virtualised networking services and functions as "Virtualised Network Functions (VNFs)". Advanced services with



different policy-processes are required by modern applications, therefore data centres must: "set up a series of NFs, various forms of state modifications by NFs: altering the contents of packets (e.g., Network Address Translation—NAT modifies ports and addresses), discarding packets (e.g., firewall), or absorbing packets and creating new ones (e.g., L7 load balancer ends the client's TCP connection and starts a new one with the right server). Because it lacks a complete view of the NF processing functionalities, which are either implemented as hardware chips in middlebox appliances or incorporated in monolithic kernels, the SDN controller in virtualised SDNFV data centres is unable to follow the packet streams and flow. Thus, issues with optimum NF service chaining and restrictions in SDN's global view of the network states of sessions remain unresolved. Community-driven cloud computing ecosystems like Eucalyptus, OpenStack, and OpenNebula provide a wide range of services, frameworks, and feature-rich user interfaces. Nevertheless, the majority of these solutions do not provide renters or hosted users with security or privacy guarantees. According to Verizon's latest analysis [603][604], insiders were engaged in 34% of assaults. By using techniques like port scanning, traffic sniffing, traffic spoofing, and more, inside attackers may take advantage of cloud networking flaws against other tenants. The cloud infrastructure providers use security measures such as firewall gateways, perimeter security, threat monitoring systems, and "Intrusion Prevention/Detection Systems (IDS)" in addition to installing anti-malware software and agents on tenant virtual machines and endpoint computers.

SDN and other virtualised network systems have just begun to be used by contemporary virtualised datacenters for comprehensive network orchestration and security services. A technique [3] known as "Switched Port Analyser (SPAN)" filter or rules can be configured to copy all/specific packets matching the criteria. The legacy approaches used the features of the routers and switches to mirror the traffic from one or more ports to a designed port on the same fabric. After receiving the packets, the system linked to the switch's SPAN port will check for malware or other threats and activate the network's reaction or mitigation mechanism. The software switch Open vSwitch[4] on a virtualised cloud network implements the SPAN function, mirroring the chosen packets. IDS software programs may be installed on one or more of the virtual machines (VMs) in the tenant network, and the OpenStack plugin "Tap-as-a-Service (TaaS)" [5] provides mirroring for the multi-hypervisor cloud environment.

Furthermore, SDNFV designs aid in introducing simple processes and solutions for these cyberthreats in order to address unresolved issues in cloud security [6] Through APIs, SDN provides a programmable paradigm for automating run-time traffic controls, dynamic security choices, service chaining, and provisioning. By separating the "packet forwarding (Data Plane) from the routing (Control plane)," SDN consolidates network information into a single component and offers a customisable interface for effective networking. The OpenFlow [7] protocol allows components on the control plane (the controllers) to interact with elements on the data plane. SDN is crucial for cloud virtualised data centres. "Software-Defined Networking (SDN)" is a term used in networking as in figure 1.

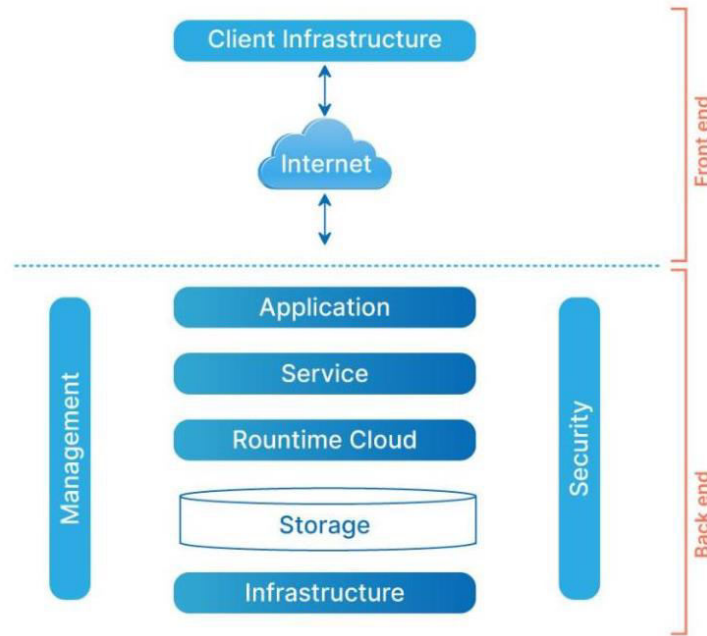


Figure 1: Framework of cloud model

1.1 Context

Here, we provide the background information on pertinent technologies needed to construct SDN-enabled cloud networks and associated projects. Cloud networks are very vulnerable to extensive attack surfaces and provide dependable

The primary measure in service-level agreements (SLAs) is services. New assaults and tailored cyber-attack campaigns are appearing daily in the ever evolving security scene. As a result, the IT networks' detection and remediation plans must be updated on a regular basis. This causes a lot of equipment (hardware, software, and middlebox) inventory to change, and ultimately integrating the new solutions becomes difficult.

Virtualisation technologies make it easy and affordable to introduce new solutions and upgrade SDN/NFV-based procedures.

Centralised cloud network delivery: SDN provides centralised administration and a centralised network view. With its programmability and virtualisation, SDN offers predetermined planning and provisioning, a flexible architecture, and the ability to scale out dynamically to satisfy runtime requirements.

A comprehensive approach to enterprise management: SDN makes it possible for the cloud enterprise network, which has several applications in cloud services, to provide on-demand services and application provisioning. SDN makes it possible to test out different virtualised network topologies and introduce fresh ideas. Software upgrades for SDNFV-based techniques are very easy and reasonably priced.

Granular Security: It might be difficult to manage access control and granular security rules in contemporary virtualised datacenters. It is challenging to apply firewall and security

policies consistently in virtual networks since certain components are located in physical infrastructure. SDN offers a straightforward, adaptable, centralised application interface for threat control, security, and QoS policy management.

The most significant risk is control plane saturation, which occurs when SDN quickly replaces conventional networks in data centres, increasing the attack surface for further cyberattacks. Therefore, SDN-enabled cloud networks will have better security granularity outcomes if a dependable topology is designed.

SDN basically builds network abstractions to enable more adaptability and application-aware behaviours in cloud systems. The fast use of emerging paradigms like SDN, NFV, SD-WAN, and Software-Defined IoT in business data centres presents new potential to redefine security and defence systems, even if there are still unresolved issues in datacenters.

1.2 OpenStack Essentials

An open-source platform called OpenStack is used to create software-defined cloud computing environments that provide storage, network, and infrastructure as a service. It offers a comprehensive and effective set of APIs for creating and managing cloud platforms, as well as support for an ecosystem for cloud services [8]. A modular, stateless architecture of services is what OpenStack supports. Authorised OpenStack component services may access all configurations and important settings (such as users, credentials, and instances) stored in a central database. Strong interdependencies exist across the OpenStack software components (Figure 2), which offer REST APIs to facilitate communication with other components.

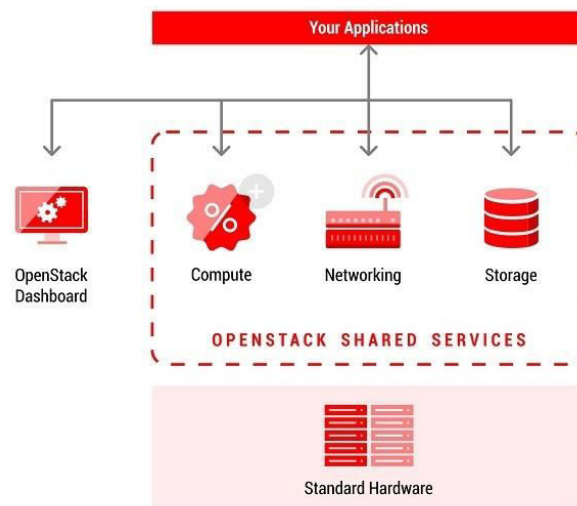


Figure 2: Services and Operations of OpenStack Components

1.3 OpenStack Integration with SDN/NFV

Networking services were recently moved from hardware appliances to softwarized NFV platforms using "VNFs (Virtualised Network Functions)" by cloud service providers and business datacenters [9].

Utilising the programmable and adaptable 202 SDN/NFV concepts, OpenStack, a cloud infrastructure technology, deploys contemporary applications like vIMS (Virtual IP Multimedia Subsystem) and vEPC (Virtual Evolved Packet Core) [10]. Opensource controller softwares like "ONOS (Open Network Operating System)" and "ODL (Open Day Light)" have been actively developed by the SDN community and provide potential answers to challenging network orchestration issues and virtual resource management. For inter-VM packet monitoring, cloud-based vEPC installations (Figure 3) use software TAPs implemented on the switching fabric, such as Open vSwitch.

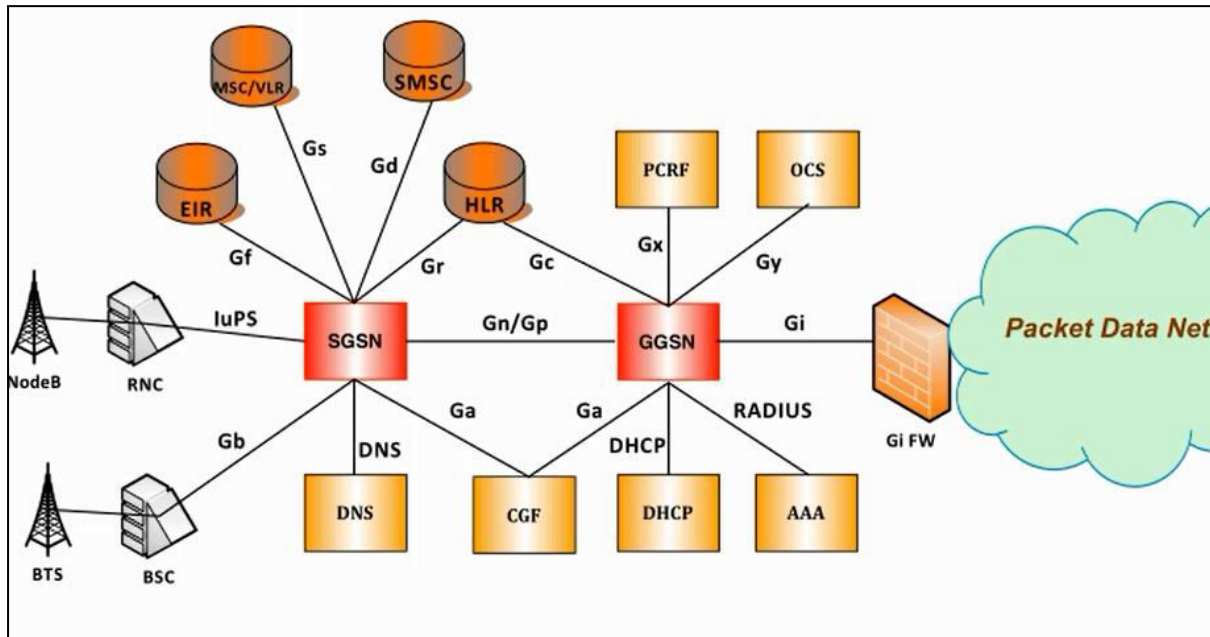


Figure 3: Virtual EPC Composition in modern data centers

1.4 OpenDayLight (ODL) SDN Controller

The OpenDayLight (ODL) [11] is a community-developed and maintained SDN Controller implementation that complies with OpenFlow specifications. In order to provide a dependable and secure cloud computing infrastructure, the OpenStack architecture may be expanded to include the SDN layer. The networking element of the OpenStack design, known as the neutron (Figure 4), makes sure that every virtual machine (VM) has a functional network.

The Neutron module facilitates the integration of OpenStack and SDN services. OpenStack network packets are transported to the ODL controller using the networking-ODL [12] plugin for OpenDaylight (ODL).

OpenStack Cloud and OpenDaylight SDN connect with one other using the public REST APIs. Since OpenStack's native Neutron lacks L3 routing capabilities and relies on the Linux kernel bridge, this architecture streamlines network traffic orchestration. As a result, the OpenStack networking architecture is neither secure or scalable enough to handle the explosive expansion of cloud services and multi-access internet connections.

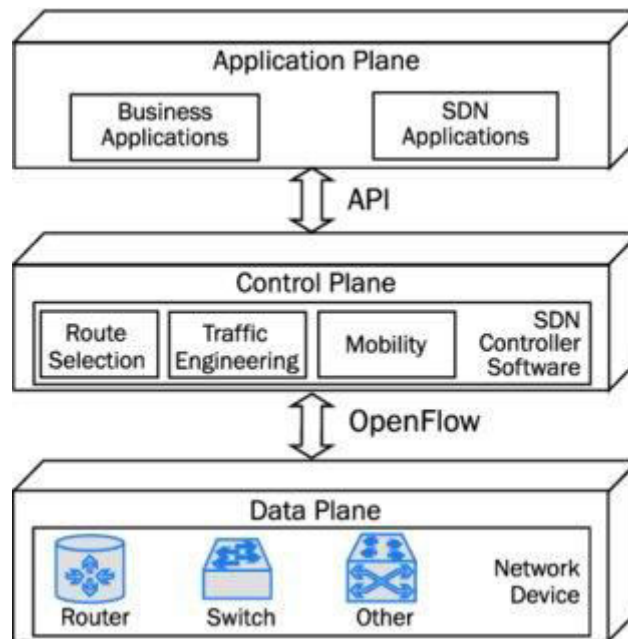


Figure 4: Neutron in OpenDaylight SDN Controller

2. Related works

An overview of important studies in pertinent fields is given in this section, with a focus on the OpenStack architecture's integration of SDN and NFV for cloud infrastructure. Finding the gaps that inspired this study project and taking inspiration from these initiatives are the objectives. The research has not thoroughly examined native SDN integration with cloud computing systems from a performance standpoint. Nonetheless, there are several solutions that use SDN to improve the cloud environment's network control capabilities, particularly in NFV deployment circumstances. "To use an external SDN controller and forcing it to control the SDN-enabled virtual switches used by Neutron, the OpenStack networking component, to implement its virtual network infrastructure" is a feasible and simple method [13]. With this method, the installed forwarding rules might be changed in accordance with a specific policy using the external SDN controller while Neutron manages the connection for the virtual instances via its regular operations. This is shown, for example, by earlier work that implemented Dynamic Service Function Chaining on OpenStack systems by using external SDN control [14]. This approach's main flaw is that it is very intrusive since it needs appropriate low-level setup and workarounds and is not a solution that Neutron natively supports. As a result, it is not a solution that is immediately applicable in production settings.

To interact with OpenStack, advanced SDN frameworks have started offering ad hoc solutions. Although these solutions were first created primarily to manage virtual switches using the Modular Layer 2 (ML2) Neutron architecture, they have now developed into far more comprehensive solutions that now include layer-3 (L3) 211 functionality. In fact, their strategy entails substituting their particular components for the whole OpenStack networking service.

3.The suggested architecture

We designed the CloudSDN framework, which incorporates SDN-managed security monitoring and response features in OpenStack cloud infrastructures, using the DTARS (Distributed Threat Analytics and Response System) that was previously established (Chapter 5). The framework uses many essential features, including: a) behavioural monitoring and profiling of every device in the data plane and control plane operation validation, b) sophisticated anomaly detection methods in the data plane c) A real-time threat analytics system in the control plane that discovers the topology for many data security layers and consumes various pieces of data with an updated malware/attack database d) Stateful-security-aware SDN stack-based mitigation techniques that are both scalable and flexible. (i) The monitoring mechanism vMon; (ii) the lightweight anomaly detection mechanism vIDS; (iii) the heavy-weight anomaly detection system NIDS (Monitor); and (iv) the mitigation and policy control applications (DTARS App) comprise the overall architecture (Figure 5). In accordance with the dynamic NFV principles—that is, software-based automated provisioning and remote configuration of network services—traffic monitoring and route manipulation modules are installed as VNFs inside the dataplaneOvS switches.

The SDN-enabled OpenStack security framework in a cloud architecture is shown in Figure 5.

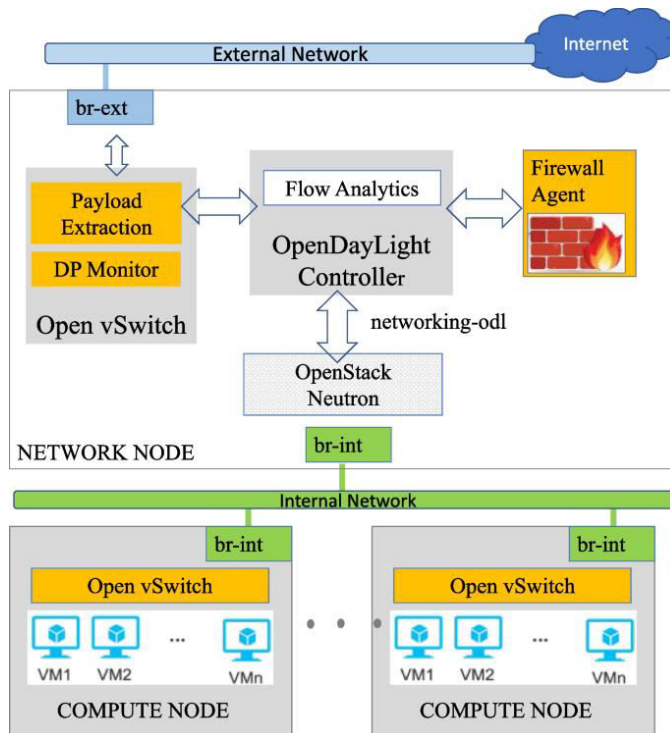
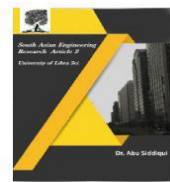


Figure 5: SDN-enabled OpenStack Architecture

3.1 Components of Monitoring and Anomaly Detection

These parts operate in the dataplane and are meant to keep an eye on the network and identify any unusual traffic patterns. Flow-based monitoring data, which are obtained from the OvS switches and are necessary for flow-based anomaly detection, are handled by the vMon



module. For further analysis, this module gathers flow data and exports it to the next module in-line vIDS on a regular basis. The necessary flow statistics may be gathered in a number of ways. Our design maintains a separation between the anomaly detection procedure and the monitoring data. Therefore, based on the capabilities of the upstream device from which we extract traffic monitoring data, any kind of flow statistics gathering technique may be used. We utilised OpenFlow examples that were exported from the OvS switches in our framework. The first level of anomaly detection is realised by the vIDS module, which uses a lightweight, coarse-grained anomaly detection algorithm to examine the collected information and look for unusual traffic patterns. The fine-grained heavyweight anomaly detection algorithm (second NIDS), which is operating on a dedicated virtual machine (Monitor), will be activated if this module notices unusual activity in order to categorise the assault. This module detects the attack victim as soon as it is identified and tells the relevant OvS switch to start mitigating the attack by propagating a static route for the victim's traffic. Such a modular design makes it possible to choose algorithms according to the network's traffic characteristics. Attack Mitigation: Using network monitoring data that is now exported by the OvS switch, the first function involves identifying malicious flows via packet asymmetry ratio examination. The third function is in charge of dumping the malicious traffic by instantiating the proper flow entries to the OvS switch and sending harmless packets back to their original destination, while the second function aggregates the malicious flows according to the originating IP address. To reduce malicious traffic, a VNF is activated on the OvS for on-demand traffic modification. To gain better scalability, we aggregate harmful flows into coarser flow entries.

It depends on the severity of the attack, system limitations (like the flow table capacity of OvS devices), and the operator's policy (for example, the attack may be low frequency or flooding, or the operator may wish to block all malicious sources or may be willing to leave some unblocked).

3.2 Cloud SDN Design

To provide a multi-plane cooperative DDoS security framework, the design approach suggests additions to the OpenStack Neutron layers and the current conventional SDN architecture. Figure 6 shows a high-level design of the suggested architecture. Attack sensors on the OvS switches keep an eye on the packet stream and flows that go through them as soon as CloudSDN is operational. The coarse-grained anomaly detection and trigger mechanisms included into the data plane switches, which serve as a security middlebox or proxy to the controller, identify malicious or anomalous flows (such as DoS assaults). on the event that no action-set matches, the ODL Controller receives sampled characteristics and synapses of suspect flows, which initiates a new, fine-grained attack detection and classification procedure on the control plane. Routing choices are the logical/optimal circumstances, and packets are sent over the dataplane. The main tactic in our proposal is to spend the majority of the transit time using switches for packet inspection and making local adjustments while enabling dynamic defence mechanisms and programmable security perimeters in the dataplane and tenant network.

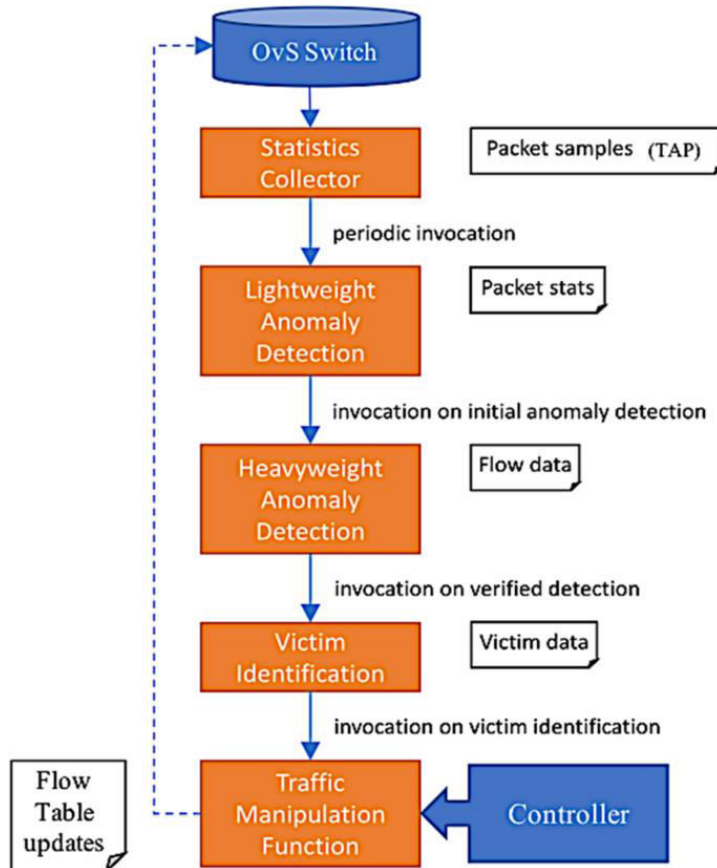


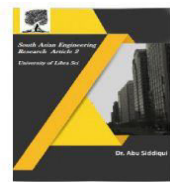
Figure 6: OpenStack Cloud Framework with SDN Integration

SDN Integrated Cloud Management Framework CloudSDN (Figure 6) includes threat analysis in the control plane and security monitoring in the data plane. Below, we provide the Framework's main elements:

Infrastructure: This layer includes cloud infrastructure devices (IoT, mobiles, modems, services, and apps), virtual computers, and physical hosts. The "OpenStack Nova" directly oversees this layer.

Switches: OpenFlow (OF) switches, Core switches, and hybrid OF-enabled Edge switches make up this layer. Through OF protocols for data switching, security monitoring, and policy enforcement, the Controller oversees this layer. Probes and sensors keep an eye on packet streams and flows; if they see any irregularities, they mark the flow as an assault. After that, the switch in question transmits an in-band message to the Trigger Core Switch or Controller that contains the flow-metadata, alerts, extracted feature-digest, and synopsis. Mitigator will carry out the matching defense-action & cleaning command (NF) on that particular Edge switch using actuators in the data plane.

Control Plane: This layer is made up of OpenDaylight's SDN Controller, which has been extended to include additional security monitoring, defence, and attack mitigation features. It uses feature digests, synopses, and uploaded in-band messages to categorise attack types.

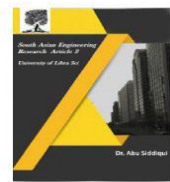


After that, it uses the defense-action to deliver instructions to the switch or switches that the malicious traffic is travelling upstream, encapsulating the -matching-action.

3.3 Data Plane for OpenvSwitch SDN

In order to gather counter values and traffic flows on switches, we created a lightweight monitor method. The controller creates "extended flow-table entries" on the dataplane switches in response to network alarms and synapses that the dataplane switches report to it after processing. Additionally, it pulls certain fields from the incoming packet stream according to the flow-rule that the controller implemented. The OpenFlow standard 1.5.1 with additional additions is used to extract the features in the switch hardware counter of action handlers. To identify irregularities in the flows and anticipate an upcoming attack campaign or an ongoing assault, the intelligent security Network Functions (NF) pipeline employs an attack forecasting algorithm. A turning-test NF further verifies the prediction by confirming the assault or triggering quick action based on the pre-built defence reaction ruleset. Those flows are flagged for fine-grained analysis at the control plane if the findings of the coarse-grained detection are uncertain. The standard forwarding procedure is used for the regular traffic, and the unflagged flows are regarded as benign. The whole procedure is coordinated by the switch manager.activities, such as the primary tasks carried out by the switch CPU. The Cloud SDNdataplane is a programmable switching platform that employs a unique strategy to satisfy the majority of application-aware and intent-based networking requirements. For example, it has a modular pipeline that executes autonomous, arbitrary, or custom logic, and every component of the switching architecture—not just NFs or flow tables—is programmable. The original OVS implemented as the network bridge interfaces (br-int/br-ex) in OpenStack is replaced by OVS-DPDK [15]. The OVS-DPDK polling mode device driver (PMD) uses ring buffers to accept packets that arrive at the OpenStack node's Ingress ports while avoiding interrupt handling overhead. OVS-DPDK offers settings for PMD, CPU affinity, and hugepages in both DPDK-compatible hardware NICs and virtual NICs in addition to maintaining the majority of the current capabilities and administration interfaces, including OpenFlow and Open vSwitch Database administration Protocol (OVSDB). The framework, which we created as an extension of Open vSwitch, preserves the well-known OpenFlow forwarding concept while smoothly integrating network functionality. For heavy-duty packet data-processing applications, the datapath supports both in-kernel for quick switching in transient connections and fully in-userspace, which binds to network interfaces directly (avoiding the kernel) using DPDK. It also makes it easier to create a flexible, programmable infrastructure for a variety of use cases, experiments, and open innovations.

In order to install the NFV platform with a series of network functions and services, modern networks need optimised infrastructure services. The naïve placement method would distribute the NFs evenly across the available NFV nodes. This results in increased overheads since packets must traverse the nodes several times, and performance would also suffer in lengthy NF chains that cover many nodes. For SFC, CloudSDN uses intelligent affinity-based placement, which exhibits reduced latencies than conventional placement techniques.



Complex and scale-out network service plans with many services (long and complex SFC pipelines) are implemented by sophisticated networks and datacenters. As we increase the number of discontinuous pathways in the chain and the number of NFs in the old configuration (NFs on VMs), the processing rate and throughput drop. Non-optimal I/O, packet copying across the stack and buffers, repeated context switching inside the node, and packets bouncing back and forth between the VMs over the switch as the number of NFs increases are the causes of this poor performance. All of the aforementioned overheads are avoided in CloudSDN architecture thanks to intelligent load-balancing across multi-node OpenStack deployments.

3.4 Common Effect

In this case, the variables RA and BA will have the common effect or the consequences on being maliciously targeted. It is believed that this causal topology will depend on the independent conditions, which will be the opposite of the independence property used for the causal chain and common cause topologies. This shows that the common effect will have the dependence property as Eq 6.8 rather than its independent property .

$$p(RA | BA, M) \neq p(RA | M)$$

The usage of dependence property claims that the consequences of the affected node is because of one of the protocol-based attacks. Also, if there is unavailability of evidences for any one of the attacks for instance, RA will there by increase the probability of another attack BA as the main cause. The dependence of the causal variables is shown as Eq 6.9

$$p(M | BA, RA) \neq p(M | BA)$$

The dependent and independent properties of the various causality topologies interpret the feasible probabilities of the protocol attack and its causal effect in the use case scenarios.

4. Analysis of BN vs SBN

In order to determine the causal consequences of a malevolent assault on a targeted node, the flooding attack analysis is first conducted using the concepts of the Bayes theorem [16,17]. By incorporating subjective judgements into the concepts of the Bayes theorem, intrinsic networking circumstances may be detected and reasoned more effectively and precisely. The research shows that, in comparison to the BN analysis, the protocol assaults have been carefully examined. Every protocol attack's involvement is examined separately. The computational analysis of BN and SBN is compared, as seen in Figure 7 (a)–(e).

(a) Malicious Attack detection time: The investigation reveals that the BN and SBN need about the same amount of time to identify the malicious activity of the compute nodes at first. As network scalability increases, time variations begin. This is due to the fact that although SBN analyses it separately, BN does it holistically throughout the network.

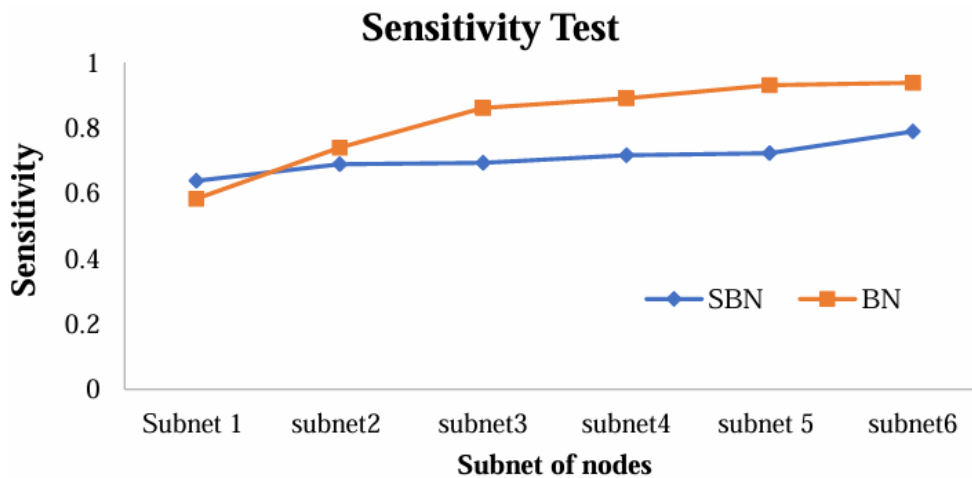
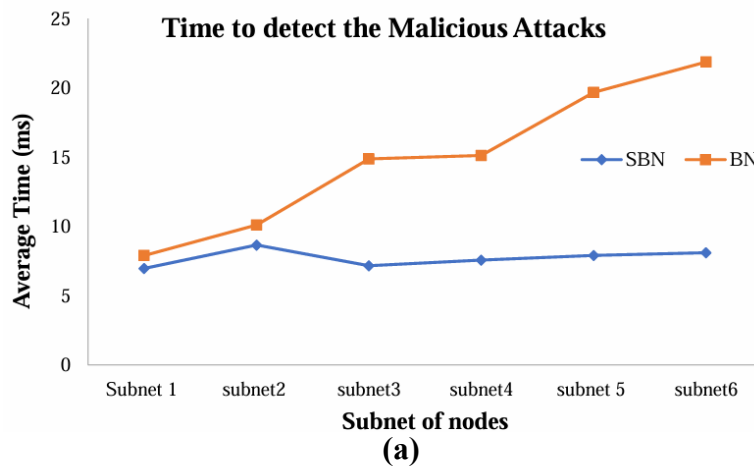
(b) Sensitivity Test: The SBN has a higher true positive rate of accurately identifying the nodes that are being attacked maliciously. This is because of the views that were included and the second level of analysis that was carried out to identify the uncertainty.

(c) Conditional Relevance: The SBN analysis will have stronger evidence to support the arguments over the participating variables since it incorporates subjective views with conditional probability [18].

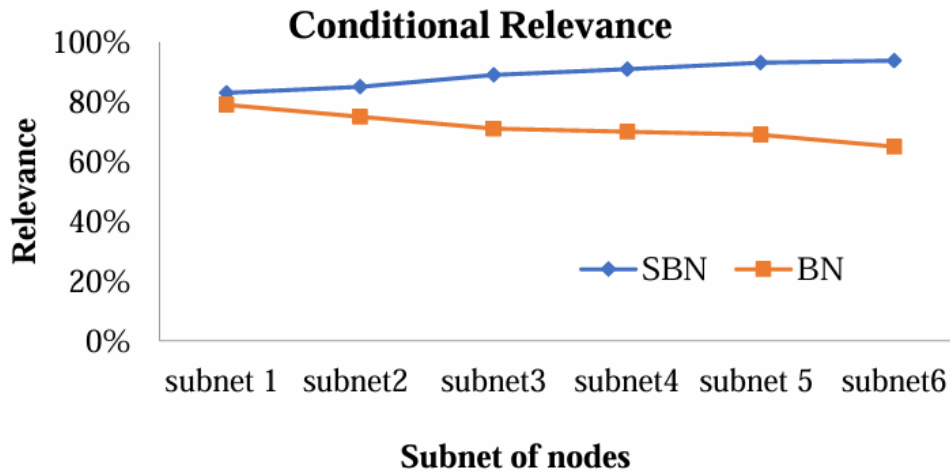
(d) Dependence: Depending on the networking scenario parameters, the SBN manages both dependent and independent variables. But in SBN as opposed to BN, the independent conditional attribute predominates [19].

(e) Detection Rate: Because the SBN can identify all of the variables, including their underlying hidden components and linked agents, it can detect at a much greater rate. However, since BN only relies on the probabilities of the variables involved, its detection rate is far slower, and if it does not meet the aforementioned likely requirements, it may sometimes go unreported as well.

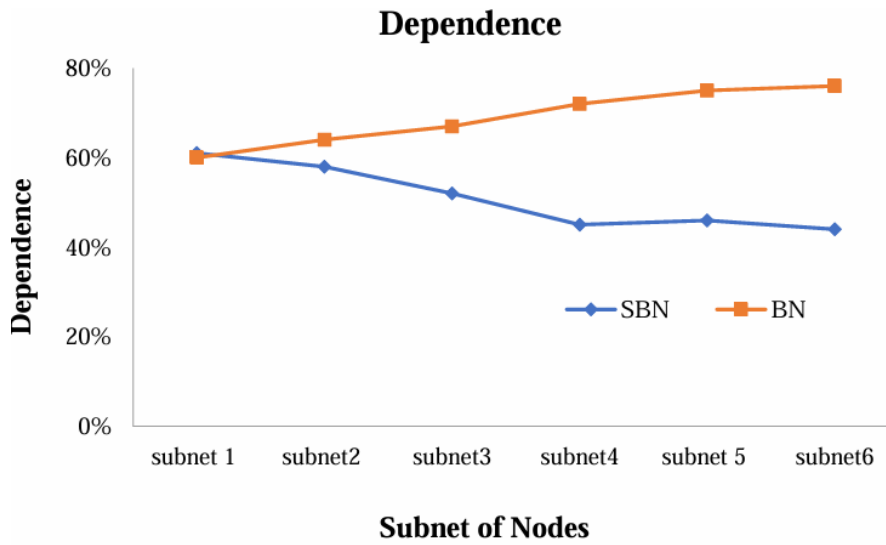
(f) Trust Computational cost: For a smaller network, the SBN will have a larger trust computational cost than the BN. This is due to the fact that it entails analysing every variable involved in the transmission. The computational cost of the trust diminishes as the network expands and ramps up at various architectural levels [20].



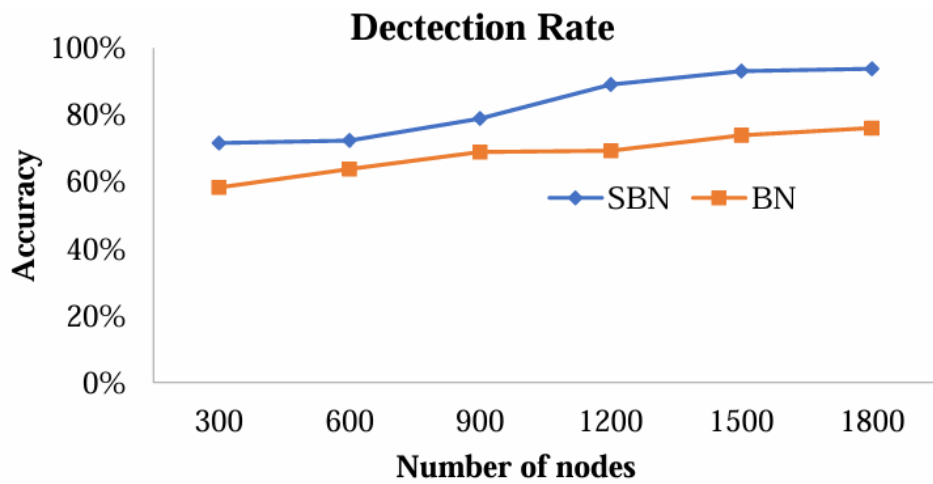
(b)



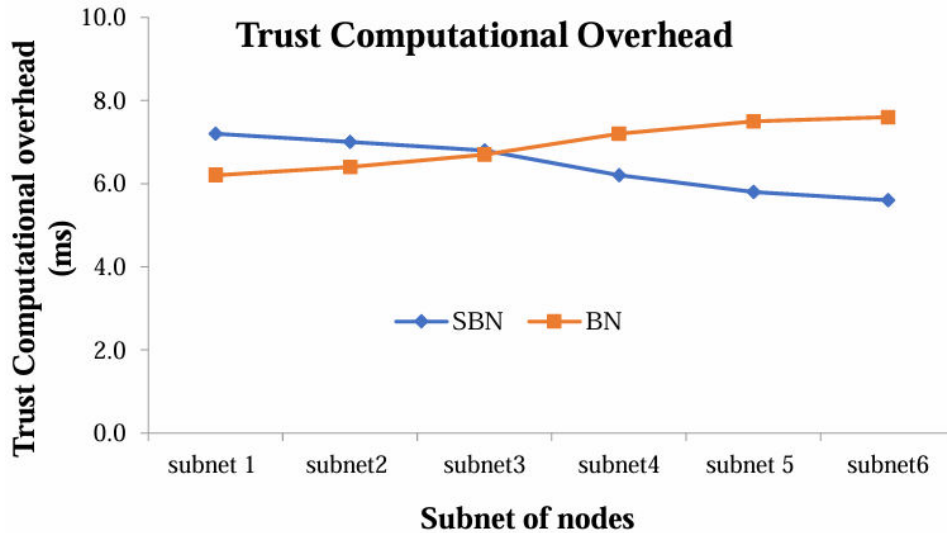
(c)



(d)



(e)



(f)

Figure 7: Computational Analysis between BN and SBN

(a) Enhanced Fuzzy Trust model: Under malicious assaults, the model was able to identify the uncertainties in a mobile cloud networking scenario. Network performance, service availability, transmission energy, data offloading, and computing cost were among the networking aspects taken into account. The range-based variables were a drawback of the improved fuzzy model. When scaling the network configuration and using a small number of parameters, it was unable to calculate trust effectively.

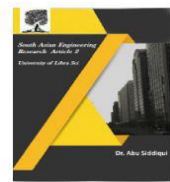
(b) Bayesian Networking Analysis: A distributed networking design with an unlimited number of 68 compute nodes and its networking characteristics might use the trust analysis provided by Bayesian networking. However, since it was based on a set of conditional probabilities and used a comprehensive approach, which included networking situations, this was unable to raise the trust score. In order to enhance the trust computation, a more thorough examination of the underlying concealed adversary circumstances was missing.

(c) Subjective Bayesian Networking Analysis: In contrast to the two models mentioned above, the SBN analysis provides a more trustworthy trust computation. Conditional probabilities along with subjective judgements are used to analyse the underlying networking circumstances.

Because both dependent and independent random variables are being analysed, trust valuation is now more efficient.

Table 1: Comparative Analysis

SI	Metrics	EnhancedFuzzy (%)	BayesianNetworking (%)	SubjectiveBayesian Networks (%)
1	Accuracy	68.2	85.4	91.2
2	DetectionRate	74.5	88.1	94.0
3	Specificity	80.3	83.5	96.1

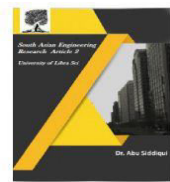


4	ThreatScore	85.4	92.7	96.9
5	Confidence (%)	72.6	81.9	89.5

The table 1 shows the comparison among three models: EnhancedFuzzy, BayesianNetworking, and SubjectiveBayesian Networks on five key metrics of accuracy, detection rate, specificity, threat score, and confidence. SubjectiveBayesian Networks performed better than other models on all metrics while the best values were obtained at accuracy 91.2%, detection rate 94.0%, specificity 96.1%, Threat Score 96.9%, and confidence 89.5%. BayesianNetworking continues with good performance, scoring 85.4% in Accuracy, 88.1% in Detection Rate, 83.5% in Specificity, 92.7% in Threat Score, and 81.9% in Confidence. EnhancedFuzzy lags behind with the lowest scores, scoring 68.2% in Accuracy, 74.5% in Detection Rate, 80.3% in Specificity, 85.4% in Threat Score, and 72.6% in Confidence. Overall, the SubjectiveBayesian Network has better performance on all the metrics, and there is a better detection rate of threats with higher accuracy and confidence compared to other models.

5. Conclusion

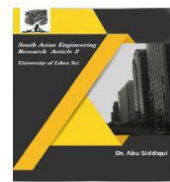
We developed a CloudSDN security framework via this study that can be used with OpenStack Cloud infrastructures that are governed by SDN. The suggested approach enhances performance in packet-level inter-VM traffic monitoring and offers users centralised security policy and access control administration. At the distributed virtualised edge network, the security policies and access control definitions are converted into OpenFlow standard rules and implemented. It is preferable in cloud systems to monitor worldwide security events and react quickly to threats or assaults. If this capability could be programmed and used in larger, geographically dispersed cloud networks, it would be even more ideal. This goal was accomplished by our investigation. We have addressed several network attack scenarios and DDoS/botnet attack attempts, as well as integrating SDN with cloud computing. Through a large-scale cloud computing application, our suggested SDFV-based security architecture integrates threat analytics, multi-plane security monitoring, and attack detection/prevention. Our research indicates that SDN has the potential to realise one of its paradigm objectives, which is to provide a programmable capacity for a global view of security events and quick response times, particularly in large geographically dispersed cloud networks. To address some of the unresolved reliability and security challenges, we have also made significant contributions to the OpenStack/SDN-based Cloud platform in the form of extensions and plugins, particularly to the network architecture. We have introduced a productive multi-phase anomaly detection method for network-wide traffic in cloud infrastructures that is based on outliers. In these areas, we outperformed the cutting-edge works: We implemented the OvSdata plane stack using the "Data Plane Development Kit (DPDK)" which includes Network Interface Card (NIC) drivers, libraries, and APIs for high-speed packet processing. i) We implemented a stateful/security-aware SDN dataplane, so some lightweight detection/computation functions are offloaded to the switches for in-line processing. The switch's flow-analysis pipeline processing throughput is much greater as a



result of fastpath kernel processing and DPDK acceleration. iii) The two aforementioned enhancements free up the controller's processing power and network port throughput for additional uses. Our framework is among the first to integrate NFV and SDN-enabled Cloud platforms, NF service chaining inside the SDN data plane, which improves cloud networks' speed, agility, and security awareness. Any big cloud application in IoT, 5G, or Industry 4.0 may use CloudSDN's platform-neutral architecture, which can be expanded to heterogeneous network models.

Reference

1. Ansari, S.A., Agrawal, A.P., Wajid, M.A. et al. MetaV: A Pioneer in feature Augmented Meta-Learning Based Vision Transformer for Medical Image Classification. *Interdiscip Sci Comput Life Sci* (2024). <https://doi.org/10.1007/s12539-024-00630-1>
2. Ansari, S. A., & Zafar, A. (2023). Multi video summarization using query based deep optimization algorithm. *International Journal of Machine Learning and Cybernetics*, 1-16.
3. Ansari, S. A., & Zafar, A. (2022). A fusion of dolphin swarm optimization and improved sine cosine algorithm for automatic detection and classification of objects from surveillance videos. *Measurement*, 192, 110921.
4. Ansari, S. A., & Zafar, A. (2020). A review on video analytics its challenges and applications. *Advances in Bioinformatics, Multimedia, and Electronics Circuits and Signals: Proceedings of GUCON 2019*, 169-182.
5. Dell Technologies. (2021). *Transforming Enterprise Networks with SD-WAN*. Dell Technologies Whitepaper.
6. Palo Alto Networks. (2019). *The Role of SD-WAN in Network Security*. Palo Alto Networks Whitepaper.
7. Zhang, X., & Zhao, X. (2020). SD-WAN Deployment and its Impact on Enterprise Network Security. *International Journal of Computer Applications*, 175(12), 54-62.
8. F5 Networks. (2019). *Securing SD-WAN for the Modern Enterprise*. F5 Networks Whitepaper.
9. Juniper Networks. (2021). *The Future of SD-WAN in Enterprise Networking*. Juniper Networks Whitepaper. Discusses the future prospects of SD-WAN technology and how it will drive the next generation of enterprise network architectures.
10. Forrester Research. (2020). *The Total Economic Impact of SD-WAN: A Study of SD-WAN Benefits for Enterprises*. Forrester Research. An analysis of the economic impact of SD-WAN adoption, focusing on cost savings, improved efficiency, and scalability for enterprises.
11. Huawei Technologies. (2021). *Building a Secure and Scalable Network with SD-WAN*. Huawei Whitepaper. Huawei's perspective on how SD-WAN enhances both security and scalability in enterprise networks, especially in hybrid cloud environments.
12. Zhang, P., & Li, D. (2020). SD-WAN: Enabling Scalable and Secure Network Architecture for Enterprises. *IEEE Access*, 8, 105150-105160. This article provides a detailed analysis of SD-WAN's role in enabling scalable and secure enterprise network architectures.



13. Ansari, S. A., & Zafar, A. (2023, March). A Comprehensive Study on Video Captioning Techniques, Benchmark Datasets and QoS Metrics. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1598-1603). IEEE.
14. SDxCentral. (2020). How SD-WAN Helps Enterprises Achieve Scalability and Security. SDxCentral Blog Post. An industry blog that explores how SD-WAN addresses key pain points in network scalability and security for modern enterprises.
15. Verizon. (2020). SD-WAN for the Enterprise: Simplifying Connectivity with Security and Scalability. Verizon Business Whitepaper. Focuses on the advantages of SD-WAN in simplifying enterprise networking while ensuring security and scalability.
16. Suresh, K., Reddy, P. P., & Preethi, P. (2019). A novel key exchange algorithm for security in internet of things. *Indones. J. Electr. Eng. Comput. Sci*, 16(3), 1515-1520.
17. Bharathy, S. S. P. D., Preethi, P., Karthick, K., & Sangeetha, S. (2017). Hand Gesture Recognition for Physical Impairment Peoples. *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)*, 6-10.
18. Sujithra, M., Velvadivu, P., Rathika, J., Priyadharshini, R., & Preethi, P. (2022, October). A Study On Psychological Stress Of Working Women In Educational Institution Using Machine Learning. In 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
19. Arista Networks. (2020). Scaling Secure Enterprise Networks with SD-WAN. Arista Networks Whitepaper. Explores how SD-WAN can help organizations scale their networks securely and efficiently in increasingly complex IT environments.
20. Ansari, S. A., & Zafar, A. (2018, December). A Review on Multisource Data Analysis using soft computing Techniques. In 2018 4th International Conference on Computing Communication and Automation (ICCCA) (pp. 1-6). IEEE."