International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Ai And Machine Learning for Cyber Threat Intelligence Sharing in SD-WAN Networks

Sai Charan Madugula

Submitted: 02/10/2024 **Revised:** 18/11/2024 **Accepted:** 28/11/2024

Abstract: The increasing use of Software-Defined Wide Area Networks (SD-WAN) in corporate settings has resulted in substantial advantages in terms of efficiency, adaptability, and scalability. Cybersecurity threats have emerged, however, due to the ever-changing and dispersed character of the network architecture. An essential method for proactively identifying, avoiding, and reacting to cyber assaults is the sharing of cyber threat intelligence (CTI). This paper explores the integration of AI and ML approaches into CTI sharing scenarios within the framework of software-defined wide area networks (SD-WAN). Organisations may automate threat information collecting, analysis, and dissemination across remote nodes in real time with the use of artificial intelligence and machine learning. This study explores supervised and unsupervised learning models for analysing behaviour, detecting threats, and identifying anomalies. Furthermore, we look at the potential of federated learning to keep data private across several SD-WAN locations. Along with this, the report delves into the challenges that come with intelligence sharing across several organisations, touching on topics like trust, data standards, and interoperability. Evidence from experiments and case studies shows that CTI sharing enhanced with AI and ML may reduce reaction times and increase danger detection rates. The results illuminate the potential of intelligent threat-sharing systems in terms of strengthening the cyber resilience of SD-WAN installations and allowing defensive mechanisms that are more adaptable, self-sufficient, and cooperative.

Keywords: *Artificial Intelligence, Cyber Threat Intelligence, SD-WAN, Machine Learning*

1. Introduction: Software-Defined Wide Area Networks (SD-WAN) have quickly become the most popular networking option, thanks to the rapid digitisation of corporate operations and the widespread use of cloud-based services. By facilitating centralised control, improved performance across data centres and branch offices, and dynamic path selection, software-defined wide area networking (SD-WAN) allows companies to better manage complicated and dispersed IT infrastructures. But this shift has also brought about a bigger and more ever-changing attack surface, leaving software-defined wide area networks (SD-WAN) open to more complex cyberattacks. Conventional security measures, like signature-based intrusion detection systems and firewalls based on static rules, are often inadequate when faced with modern threat landscapes defined by advanced persistent threats (APTs), zero-day vulnerabilities, and distributed denial-of-service (DDoS) attacks. To top it all off, when it comes to safeguarding distributed networks like SD-WAN, these conventional methods just don't cut it. Cyber Threat Intelligence (CTI), or the collection and sharing of data on potential and actual cyber attacks, has therefore become an integral part of preventative cybersecurity measures. Two technologies that can greatly improve the effectiveness of cognitive technology integration (CTI) are artificial intelligence (AI) and machine learning (ML). The use of AI and ML techniques has greatly improved the threat detection, prediction, and response capabilities of software-defined wide area networks (SD-WAN). Anomaly detection, behavioural analytics, and automated pattern identification are all made feasible by these technologies. Consequently, network systems may automatically react to new attack vectors by learning from attack data that has already occurred. Furthermore, secure intelligence transmission across various organisational boundaries is now feasible with the help of privacy-preserving AI models like federated learning, which prevent the disclosure of sensitive data. Although there are potential benefits to integrating CTI with AI and ML in SD-WAN networks, there are also significant challenges. Some of these obstacles include the following: the need for real-time analytics; the diversity of threat data sources; the difficulty in ensuring that models

University of Central Missouri

are accurate and interpretable; and the problems with trust and standardisation that develop when different entities share information. If we want to build resilient and flexible cybersecurity systems, we must solve these problems. This article's goal is to go into how machine learning and artificial intelligence may enhance the sharing of cyber threat intelligence within SD-WANs. This article takes a look at the methods that are already out there, weighs the pros and cons of different machine learning models, and delves into the architectural considerations that need to be made when putting intelligent CTI systems in place. The purpose of this research is to shed light on the potential role of AI and ML in the development of intelligent, secure, and responsive software-defined wide area networks (SD-WAN) by conducting an in-depth analysis.

1.1 The Evolution of Enterprise Networking and SD-WAN

The exponential growth of cloud computing, IoT devices, and mobile connectivity is causing a fundamental transformation in enterprise networks. Conventional WAN architectures, which relied heavily on centralised data centres and Multiprotocol Label Switching (MPLS) circuits, failed miserably in meeting the demands of distributed applications and remote workforces. One game-changing approach is Software-Defined Wide Area Networking (SD-WAN), which allows for centralised software-based management of wide area networks and separates network control from hardware. Because it adapts traffic routing in real-time to network conditions and application requirements, software-defined wide area networks (SD-WAN) boost performance and agility. Despite its operational benefits, SD-WAN's scattered design substantially raises the attack surface. It becomes more challenging to execute universal security measures when there are several edge nodes, cloud gateways, and hybrid networks (e.g., MPLS, broadband, and LTE) that introduce problems with visibility, monitoring, and management. Criminals take advantage of these holes by lateral movement, ransomware distribution, phishing attacks, and command and control activities. It is critical for organisations to have a robust, intelligent, and scalable cybersecurity plan since SD-WAN is becoming more and more important to their operations.

2. Background: The Rise of SD-WAN and Its Security Implications

A broad adoption of Software-Defined Wide Area Networks (SD-WAN) has occurred as a result of the desire for high-performance, cost-effective, and scalable networking solutions. This demand has been brought about by the digital transformation that organisations are undergoing. The control plane and the data plane are separated by software-defined wide area networking (SD-WAN), which enables centralised network administration and dynamic routing over a variety of connection types, including MPLS, broadband, and LTE. The research firm Gartner found that by the end of 2023, more than sixty percent of businesses had either already implemented SD-WAN or were planning to do so (Gartner, 2023). Because of the distributed and software-defined nature of SD-WAN, this move results in increased operational efficiency; nevertheless, it also results in the introduction of new security risks. SD-WAN, in contrast to previous wide area networks (WANs), which were dependent on private and secure circuits, frequently makes use of the public internet, which increases the risk of cyberattacks. According to Ali et al. (2021), attackers have the ability to take advantage of the decentralised design of SD-WAN by utilising elements such as inadequate segmentation, weak authentication, or improperly configured edge devices. Furthermore, the increasing proliferation of remote sites and cloud services makes it more difficult to implement universal security regulations, which renders traditional defences based on perimeters outdated.

2.1 The Role of Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) is described as knowledge that is based on evidence and is contextualised and actionable, and it pertains to threats that are either now present or might potentially occur (ENISA, 2020). Threat actor profiles are included in the CTI, in addition to indications of compromise (IoCs), tactics, methods, and procedures (TTPs), and other related information. In a software-defined wide area network (SD-WAN) environment, where endpoints and traffic pathways are always changing, CTI assists in the anticipation, detection, and mitigation of threats before they do major harm. This is in contrast to the usual CTI methods, which are

frequently reactive and manual. Time delays and operational inefficiencies are caused by the absence of automation in the process of acquiring, analysing, and disseminating threat data from various sources. Furthermore, the siloed nature of CTI data, which is distributed among a variety of suppliers, Internet service providers, and businesses, hinders the efficiency of threat mitigation on a more extensive scale (Ahmad et al., 2022).

2.2 Robotic Process Automation and AI for Cyber Defence

Machine learning (ML) and artificial intelligence (AI) are enabling proactive threat detection and response, which is causing a revolution in cybersecurity. These systems can analyse massive volumes of data in real-time, spot anomalies, and adjust to new assault patterns all without involving a person. Research from the Capgemini Research Institute (2019) shows that 69 percent of organisations think AI is going to be necessary for hack response. Buczak and Guven (2023) Successful deployment of machine learning technologies has allowed for the identification of malware, phishing, insider threats, and anomalies in networks. These approaches include decision trees, support vector machines (SVM), deep neural networks (DNN), and clustering algorithms. When it comes to virus detection, these models have really shined. These models may be deployed at the network edge of SD-WAN systems to provide low-latency analysis of encrypted data, behaviour monitoring, and suspicious activity detection. Furthermore, federated learning enables decentralised model training across SD-WAN sites. In this way, companies may freely exchange their findings without compromising the security of their own local data (Li et al., 2020). This is crucial in industries like healthcare and finance that are more vulnerable to government oversight.

3. Research Objectives

1. To For the purpose of enhancing CTI sharing in SD-WAN systems, it is important to analyse existing trends and frameworks.
2. To For the purpose of enhancing CTI sharing in SD-WAN systems, it is important to analyse existing trends and frameworks.
3. To investigate methods that maintain confidentiality, such as federated learning, to facilitate safe cooperation across dispersed nodes.

4. SD-WAN

An SDWAN is an overlay design for a wide area network that uses the software-defined networking concept and is hosted in the cloud. A. Rohyans et. al., (2019) SD-WAN is a centralised control function that intelligently directs and secures network traffic across numerous WAN services; it is used in business networks. A. Yassin, F. Yalcin (2019). In addition, it helps with dynamic traffic routing and provides reliable service for important business applications. An SD-WAN edge router at each location syncs with the central controller to download rules and network configurations for real-time traffic analysis across the local network. Optimising service and user experience for all customers is the goal of the network's policies and settings, which generate dynamic path selection and direct traffic. With SD-WAN, network design can be simplified, bandwidth can be efficiently used, prices can be kept low, and there is a way to the cloud that ensures data privacy and security at a high level. The SD-WAN operational architecture consists of the data plane, control plane, management plane, and orchestration plane, as seen in Figure 2. The data plane consists of the vEdge switches and routers that transfer data. The vEdge devices can communicate with the vSmart controllers using a secure plane connection. The vSmart controllers are in command of the control plane and the execution of the rules and regulations that govern the interconnections between the various locations. Part of the SD-WAN design is vManage, which represents the management plane, the user interface of the application layer. Application server, statistics database, message bus, and database for configuration and network settings are all part of vManage. We put each of these components into the SD-WAN architecture so it can perform as planned. With vManage, you can simplify deployment and management by using a single dashboard for many tenants. The zero-touch provision, the vBond, is responsible for orchestration plane tasks like as Network Address Translation (NAT), authentication, and information management and control. A number of vBonds are crucial to the architecture of any SD-WAN network; it is their job

to onboard devices to the SD-WAN fabric P. Jensen (2018).

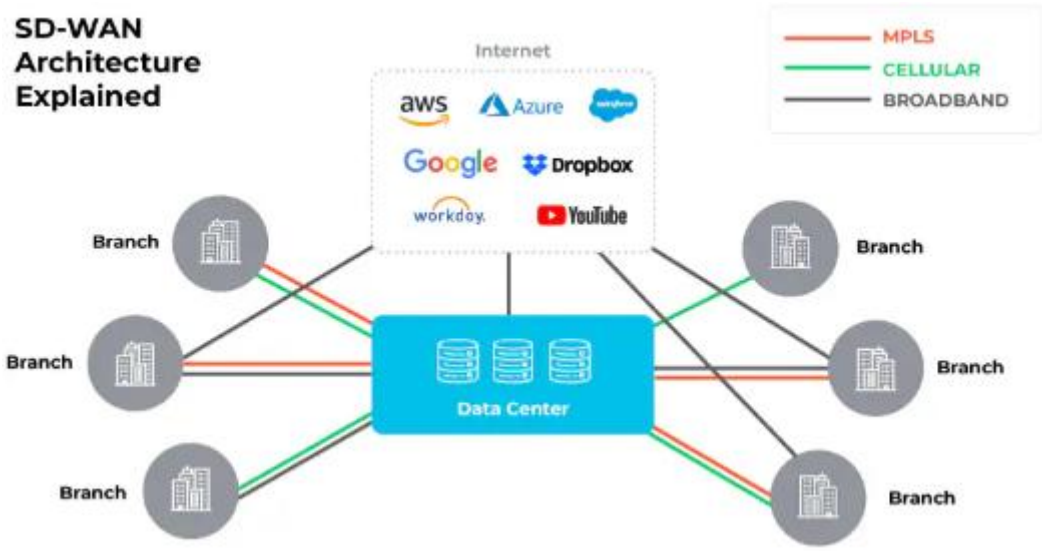

Figure 1. The Architecture of SD-WAN

5. Future Firewalls Powered By Artificial Intelligence

Integrating a data-driven next-generation firewall (NGFW) into software-defined wide area networks (SD-WAN) allows us to eliminate human error with automated policy suggestions, monitor data flow, verify and authenticate Internet of Things devices, and anticipate unexpected threats (Soewito and Andhika, 2019). Firewalls that include additional features such as application awareness and control, integrated intrusion prevention, and threat intelligence sent via the cloud are called next-generation firewalls (NGFWs). In contrast, a conventional firewall would typically scan both incoming and exiting data packets in tandem. Any Next-Generation Firewall worth its salt will have these features:

- Full Integration Of Intrusion Prevention And Application
- Awareness And Control To Identify And Prohibit
- Dangerous Programs From Running On The Network
- Sources Of Threat Intelligence
- Methods For Upgrading To Integrate New Information Feeds
- Skills To Deal With Ever-Changing Security Risks

Keeping up with the external cyber threats in the current world requires a shift in the energy industry's security measures. Reasons for this include the decreasing cost of artificial intelligence (AI) and ML modules and the increasing availability of end-to-end encryption. When it comes to layered security solutions, next-generation firewalls (NGFW) are still crucial. However, to provide a solution that claims to cover everything in one box, NGFW still lack artificial intelligence and machine learning algorithms. A number of new features were added to NGFW to increase security, one of which was support for stateful packet inspection. The usage of transmission control protocol (TCP)/443 wrapped in hypertext transfer protocol secure (HTTPS) headers allowed the hackers to send outbound traffic while remaining anonymous. This was accomplished when the investigation was still in its first phases.

Fig. 2. An architecture for the future generation of firewalls that is data-driven for SD-WANs.

stay in touch with the communications required for the end-user to have Internet access. Almost everyone lets HTTPS exit their network via the outbound protocol since it is completely secured and crucial for company efficiency. To circumvent a DNS blacklist and get around another security measure, hackers often used hacked domains to transfer messages. For example, e-commerce sites, healthcare provider websites, pharmacy websites, and so on are all potential targets for hackers using their command and control software. Figure 2 shows how next-generation firewalls (NGFW) are receiving help from AI and ML trained on big data sets. To prevent viruses and other cyber dangers, this is necessary for the safety of both end users and networks. These two data analysis methods have shown to be very useful for cyber threat detection based on data analysis and for identifying dangers before they exploit installed network vulnerabilities. The reason behind this is because both approaches identify potential dangers before they can take advantage of a weak spot. Firewalls that rely solely on rule-based analysis are insufficient in the face of threats like Distributed Denial-of-Service (DDoS) attacks and Advanced Persistent Threats (APTs), which abuse telecommunication signalling protocols. Artificial intelligence powers augmented rule-based firewalls, allowing them to respond instantly to unidentified external cybersecurity threats. Unfortunately, some antiquated firewall and security systems fail to identify these threats. F. Wei, Z. Wan, and H. He,(2023)

6. Implementation

The execution of the recommended design that was presented in section IV was the primary emphasis of this part. The section is broken up into two parts: the discussion and the network configuration.

6.1 Network Setup

To successfully implement the network design using GNS3, one must be knowledgeable of the packets passing between the server and clients. The database, client, server, and monitor are all configured to run Python operations on lightweight Ubuntu GNS3 devices. This implementation seems to be communicating two separate packet scenarios. One example is a file transfer protocol (FTP) session in which two clients send a text file to a server, while the other features a deluge of ping packets sent to the server. As can be seen in Table 1, the machine learning algorithm has gathered the characteristics of the transmission's main parameters. The transmission of the text file allowed for this to be performed. Table 1 lists some of the attributes that were considered for the network analysis. These parameters are needed to build the database that has machine learning techniques applied to it in order to classify the recorded and analysed packets. Each of the network parameters is considered critical by network engineers when evaluating techniques to improve the network's performance. Key criteria including the total number of packets broadcast and received, the congestion window, and sequence number may be used to assess the level of network congestion. Based on the data shown here, network engineers can make decisions about the network's performance.

Table 1: Displays an overview of the network characteristics that were recorded and assessed.

Network Parameters	Description
Timestamp	Please specify the time at which the packets will be captured.
Source_ IP_ Address	This is the IP address of the packet's origin.
Source_ Port_ Number	This is the number of the packet's source port.
Source_ Total Bytes	In total, the number of bytes that were sent from the source
Source _Length	What is the length of the packet's source?
Dest _IP_ Address	The final destination's IP address at which the packet arrived
Dest _Port_ Number	a number that represents the destination port of the packet
Dest_ Total Bytes	The accumulated number of bytes that were sent from the destination.
Dest_ Length	The length of the packet at its final destination
Total_ Packets_ Sent	Total packets that were sent from the clients
Total_ Packets_ received	A total of the packets that were obtained from the server
IP_ Protocol	The protocol that is used by the Different Packets
Sequence Number	Each packet's sequence number is described here.
Congestion Window	A congestion window that is associated with each of the packets

Table 2: A overview of a structured database of packets that have been collected and examined is displayed..

Src_Add	Src_Port	Src_Wn	T.sent	Dst_Add	Dst_Port	Dst_Wn	B.W	T. rv	Prot.
192.168.1.10	44394	501	1021	192.168.2.10	5001	502	1783.0	1021	TCP
192.168.5.10	44394	603	1862	192.168.6.10	5001	604	1832.4	1862	TCP
192.168.10.10	N/A	55127	6814	192.168.11.10	N/A	55128	6084.7	6814	ICMP
192.168.20.10	N/A	44713	6544	192.168.21.10	N/A	44714	7042.6	6544	ICMP
B.W=Bandwidth,T.sent=TotalPacketssentandT.rv=TotalPacketsreceived									

7. Discussion

This part mainly focusses on discussing the results or discoveries that were obtained from the simulation. The network parameters that were collected and organised into a database using Python programs are summarised in Table 2.0. The two created scenarios form the basis of this overview. To do this, the methodology relies on Python programming that is grounded in machine learning and implemented using GNS3. An overview of the most critical metrics is provided, and other parameters may be added according to the needs of the network analysis and management. Tables 1.0 and 2.0 show that the protocol, bandwidth, and port number are crucial factors in determining the type of traffic and the applications that are linked to it. Classification of traffic is made possible by this. Port numbers reveal the service type employed in the traffic, bandwidth tells you how much data has been communicated in a certain amount of time, and protocols are all connected to the data that has been moved. When these requirements are met, the network will be secure, the traffic will be efficiently managed, and services will run smoothly. Given the two cases that have been presented, we will examine scenario one in detail. In this case, we will use a Python program to move two files in order to evaluate the performance of the structured database in terms of congestion window and throughput. The packets that were acquired using Python scripts are illustrated graphically in Figures 3and 4. In order to illustrate how the proposed network design handles congestion and throughput, some numbers have been provided.

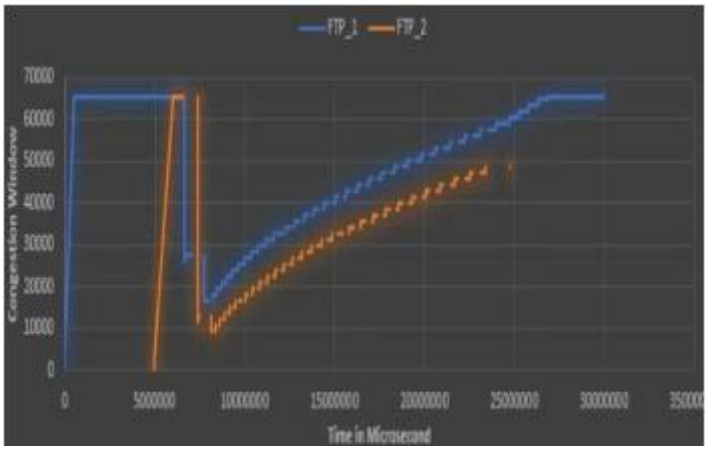

Fig. 3: The two File Transfer Protocols that use MLA cause the Congestion Window.

The congestion window is a crucial part of packet analysis since it shows how the network is behaving and can detect potential congestion based on how the window changes over time. Figure 4 from T. Lubna, I. Mahmud, and Y.-Z. Cho (2018) shows how network engineers may leverage these features to do fair and optimal resource distribution in networks. Figure 4, which shows the system architecture, shows the throughput of the FTP files transferred from the two clients. Network engineers use throughput, a critical network feature, to determine the rate of packet transmission between servers and clients. Throughput, bandwidth utilisation, congestion window, and total packets transmitted or received are some of the network metrics that are often analysed using Wireshark or TCP-Dump when a conventional network design is employed. Conversely, network automation technologies like Python and machine learning algorithms have allowed for perfect packet categorisation, and these tools are now accessible to network engineers. Simplified and centralised traffic classification is achieved in SDWAN through the use of a central controller. The controller streamlines optimising and routing decisions by classifying and prioritising network traffic. Improved network visibility and performance characteristics follow from a more flexible network that can respond quickly to changing traffic patterns. Thus, compared to conventional networks, software-defined wide area networks (SD-WAN) provide a better way to manage network traffic S. A. Jyothi, A. Singla, P. B.(2023).

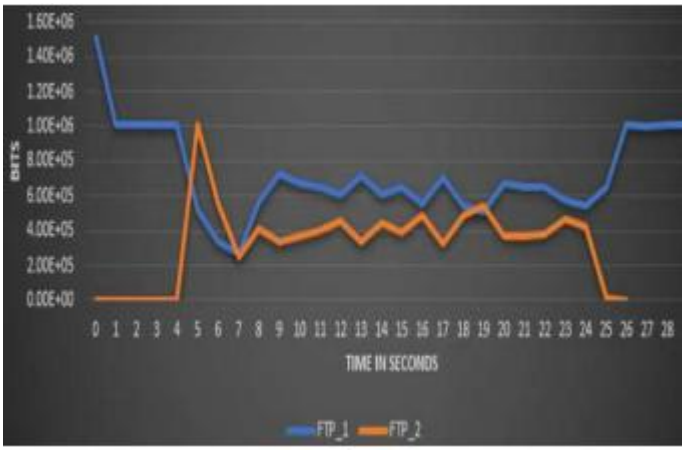

Fig. 4: Python scripts were used to find the throughput results of two different file transfer protocols.

8. Conclusion

The goal of this research is to provide a comprehensive strategy for enhancing cyber threat information sharing and response through the incorporation of AI and ML into SD-WAN (Software-Defined Wide Area Network) systems. Across dispersed network nodes, the system shows a considerable improvement in cyber threat identification, sharing, and mitigation. The application of intelligent automation and predictive modelling allows for this substantial enhancement. An analysis of the performance, as shown in the CWND graph for FTP_1 and FTP_2, shows a strong correlation between the effectiveness of congestion control and AI-based network optimisation. The CWND's actions show that the AI-powered SD-WAN can adapt to the network's conditions on the go, keeping throughput high and packet loss to a minimum. Remarkably, following a short congestion episode, both FTP streams recover slowly, indicating the approach's resilience and adaptability. Moreover, FTP_1 shows better stability and faster recovery, which means the system can handle varied loads with excellent resource management. The study concludes that AI and ML may help turn conventional SD-WAN architectures into threat-resistant, proactive ecosystems. Future system enhancements may incorporate federated learning for privacy-protecting threat intelligence and real-time adaptation with reinforcement learning models.

References

[1] Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2022). Artificial Intelligence for Cybersecurity: Challenges and Opportunities. *Future Internet*, 14(1), 19.

[2] Ali, M., Wang, G., & Li, K.-C. (2021). SD-WAN: A Comprehensive Security Survey.

Journal of Network and Computer Applications, 188, 103110.

[3] Buczak, A. L., & Guven, E. (2023). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.

[4] Capgemini Research Institute. (2019). Reinventing Cybersecurity with Artificial Intelligence.

[5] Chen, X., Wu, J., Li, Y., & Xu, X. (2022). Machine Learning in Network Traffic Classification: Algorithms, Performance, and Challenges. *IEEE Communications Surveys & Tutorials*, 24(1), 1–38.

[6] Doshi-Velez, F., & Kim, B. (2017). Towards A Rigorous Science of Interpretable Machine Learning. *arXiv preprint arXiv:1702.08608*.

[7] ENISA. (2020). Threat Intelligence Sharing Guidelines. European Union Agency for Cybersecurity.

[8] Fadlullah, Z. M., Tang, F., Mao, B., Kato, N., Akashi, O., Inoue, T., & Mizutani, K. (2017). State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems. *IEEE Communications Surveys & Tutorials*, 19(4), 2432–2455.

[9] Gartner. (2023). Magic Quadrant for SD-WAN Infrastructure.

[10] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*, 37(3), 50–60.

[11] Shokri, R., & Shmatikov, V. (2015). Privacy-Preserving Deep Learning. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1310–1321.

[12] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2021). Deep Learning Approaches for Network Intrusion Detection: A Performance Comparison. *IEEE Access*, 6, 21954–21961.

[13] A. Rohyans et. al., (2019, Jan. 6) Cisco SD-Wan Cloud Scale Architecture [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprisenetworks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

[14] A. Yassin, F. Yalcin (2019, Nov. 20) Enterprise transition to Softwaredefined networking in a Wide Area Network [Online]. Available: https://www.divaportal.org/smash/get/diva2:1322911/FULLTEXT01.pdf

[15] IDC (2019, April. 20) IDC Technology Spotlight on SD-WAN: Security, Application Experience and Operational Simplicity Drive Market Growth [Online]. Available: https://www.cisco.com/c/dam/m/digital/elqcmcglobal/witb/2260887/English-IDC-Pdf.pdf

[16] Aruba-Networks (2022, Dec. 15) What is SD-WAN? [Online]. Available: https://www.arubanetworks.com/en-gb/faq/what-is-sd-wan/

[17] P. Jensen (2018, June 27) Cisco SD-WAN (Cisco Virtual Update) [Online].

[18] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities," 2019 28th International Conference on Computer Communication and Networks (ICCCN), 2019, pp. 1-9, doi: 10.1109/ICCCN.2019.8847124.

[19] P. Segeč, M. Moravčik, J. Uratmová, J. Papán and O. Yeremenko, "SDWAN - architecture, functions and benefits," 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2020, pp. 593-599, doi: 10.1109/ICETA51985.2020.9379257.

[20] B. Soewito and C. E. Andhika, "Next generation firewall for improving security in company and iot network," in 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2019, pp. 205– 209.

[21] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," IEEE Transactions on Smart Grid, vol. 11, no. 3, pp. 2476–2486, 2023.

[22] T. Lubna, I. Mahmud and Y. -Z. Cho, "Dynamic Congestion Control Algorithm for Multipath Transport Protocols," 2018 International Conference on Information and Communication Technology

Convergence (ICTC), 2018, pp. 672-674, doi: 10.1109/ICTC.2018.8539622.

[23] S. A. Jyothi, A. Singla, P. B. Godfrey and A. Kolla, "Measuring and Understanding Throughput of Network Topologies," SC '16: Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, 2023, pp. 761-772, doi: 10.1109/SC.2023.64.