RESEARCH ARTICLE

SAMRIDDHI Volume 14, Issue 4, 2022 Print ISSN: 2229-7111 Online ISSN: 2454-5767

The Role of AI and Machine Learning in Enhancing SD-WAN Performance

Goutham Sunkara

VMware Inc. & Member of Technical Staff.

Abstract

Enterprise networks have grown more complex and cloud-based applications have become rampant to the extent that the traditional wide area network (WAN) architectures have been particularly strained. The problem of performance optimization, instant decision-making, and dynamic traffic management has continued to exist despite the introduction of Software-Defined Wide Area Networks (SD-WAN) as a flexible mix. In this paper, we presented the nature of partnership between Artificial Intelligence (AI) and Machine Learning (ML) techniques and SD-WAN architectures in order to assist in overcoming these limitations. Particularly, it focuses on the potential of supervised and reinforcement learning model to improve the task of traffic routing, forecast and neutralize network anomalies, and automated policy statements in accordance with the current network state. Using comparative analysis to counter AI-enhanced SD-WAN systems and traditional rule-based systems, the study shows improvement in several important performance measures that include latency, jitter, packet misplaced, and service level agreement (SLA) adherence. There is also a section in the paper that deals with the implementation challenges such as data privacy, model shift, and non-standardization of vendor platforms. The results paint the disruptive possibilities of AI and ML in achieving smarter, flexible, and robust SD-WAN infrastructure that can support the changing enterprise requirements.

Keywords: SD-WAN, Artificial Intelligence, Machine Learning, Network Optimization, Traffic Engineering, Anomaly Detection, Reinforcement Learning, Quality of Service (QoS), SLA Compliance.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i04. 34

Introduction

Amazing scale of cloud computing, digital transformation, and remote working places has transformed the nature of how enterprises design their wide area networks (WANs). WANs using older designs using costly and rigid Multiprotocol Label Switching (MPLS) channels have failed to serve the on-demand needs of current applications in terms of bandwidth flexibility and latency. Software-Defined Wide Area Networks (SD-WANs) have thus become an innovative alternative, which has the ability to provide central management, cost-saving, and traffic steering across wide area connectivity variants.

Although SD-WANs have a number of benefits concerning how they are designed, they are becoming impaired to provide consistent performance, more so in the platforms where network loads are mixed, application requirements vary, and network security is at stake. Traditional SD-WAN interventions that tend to be relying on static rule-based systems and policies that are controlled by thresholds are not flexible and context-sensitive to maximize network performance in real-time. Such weaknesses underscore the necessity of increased intelligence and automation in SD-WAN models.

Corresponding Author: Goutham Sunkara, VMware Inc. & Member of Technical Staff, e-mail: sgoutham.sunkara@gmail.com

How to cite this article: Sunkara, G. (2022). The Role of AI and Machine Learning in Enhancing SD-WAN Performance. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 14(4), 1-9.

Source of support: Nil

Conflict of interest: None

The AI (Artificial Intelligence) and ML (Machine Learning) have become popular solutions that facilitate autonomous operations in the network. The possibility of analyzing high volumes of network telemetry, learning patterns and predicting anomalies, and adjusting routing policies and quality-of-service (QoS) policies in real time provides exciting possibilities in SD-WAN performance. The AI/ML techniques mentioned above, supervised learning (traffic classification), unsupervised learning (anomaly detection), and reinforcement learning (policy optimization) have the potential to resolve most of the operational inefficiencies that plague SD-WAN traditional solutions.

The incorporation of AI and ML in the SD-WAN fabric is bringing a paradigm shift towards intelligent, self healing, and self optimizing networks. Such intelligent SD-WAN systems are set to change this situation as they are aimed to respond to changing conditions without needing human interaction, lowering operational overheads at the same time increasing compliance with service-level agreements (SLAs), application experience, and network reliability. But there are also new challenges of data privacy, model explainability, scalability of deployment, and cross-vendor interoperability issues introduced by this convergence.

The current paper researches the prospect of AI and ML in the further evolution of the SD-WAN capabilities subsequent to their ability to strengthen traffic engineering and predictive analytics, anomaly detection, and automatization within the WAN systems. The analysis adopts the approach of studying the most important use cases, architectural designs, and performance measures with the view of delivering a detailed analysis of AI-driven optimization of SD-WAN and how they will impact the future of enterprise networking.

Background and Literature Review

Evolution of Wide Area Networking and the Emergence of SD-WAN

Traditional WAN architectures relied heavily on leased lines and Multiprotocol Label Switching (MPLS) for interconnecting enterprise branch locations. These architectures were costly, inflexible, and poorly suited to the rapid shift toward cloud-hosted applications. As business operations became increasingly distributed and cloud-dependent, enterprises sought a solution that could dynamically manage traffic while improving cost efficiency and scalability.

Software Defined Wide Area Networks, or SD-WAN, emerged as a promising response. SD-WAN decouples the control plane from the data plane, allowing centralized traffic management, application-aware routing, and improved use of multiple transport links such as broadband, LTE, and MPLS. While SD-WAN solved several pain points, it still relied on static policy rules and lacked real-time adaptability in dynamic environments. This created a critical need for intelligence in routing, monitoring, and optimizing performance.

Integration of AI and Machine Learning in Network Systems

Artificial Intelligence and Machine Learning have demonstrated significant value in numerous network domains including intrusion detection, traffic prediction, and resource allocation. Supervised learning has been widely used to detect patterns and anomalies in traffic behavior, while reinforcement learning techniques have proven effective for real-time decision making in dynamic network environments.

In the context of SD-WAN, AI and ML bring the ability to learn from vast volumes of telemetry data including link quality, latency variations, packet loss, and user behavior. This enables predictive analytics, automatic policy adjustment, and proactive fault handling. The learning models continuously evolve based on observed network states, making SD-WAN systems not only responsive but also predictive and self-optimizing.

Key Applications of AI and ML in SD-WAN Enhancement

Traffic Engineering and Path Selection

Reinforcement learning models can dynamically assess the performance of available links and select optimal paths in real-time. This allows SD-WAN systems to adapt to sudden spikes in traffic, bandwidth degradation, or link failure without administrator intervention.

Anomaly Detection and Fault Prediction

Supervised ML models trained on historical traffic patterns can detect anomalies such as distributed denial-of-service attacks or misconfigurations. Additionally, AI systems can forecast link failures and trigger automated remediation actions, thereby reducing downtime and improving SLA compliance.

Quality of Service Optimization

AI-enhanced SD-WAN systems can prioritize network traffic based on real-time context and application behavior. For instance, critical video conferencing applications can be prioritized over bulk file transfers depending on current link conditions and user intent.

Related Work in AI-Driven Network Optimization

Multiple research efforts have explored AI applications in networking. One line of work demonstrated the use of deep learning for classifying traffic flows in encrypted environments. Other studies explored the use of Q-learning for real-time routing optimization in software-defined networks. While these studies were largely experimental or applied to data center networks, their methodologies are highly relevant to SD-WAN implementations.

Recent industry deployments by vendors have also started incorporating AI into SD-WAN products, but many lack transparency regarding the models used and their performance benchmarks. This underscores the need for independent academic analysis and open frameworks.

Research Gaps and Opportunities

While AI and ML have shown promise in network automation and performance optimization, several gaps remain in their application to SD-WAN. These include the lack of unified datasets for training and benchmarking, limited

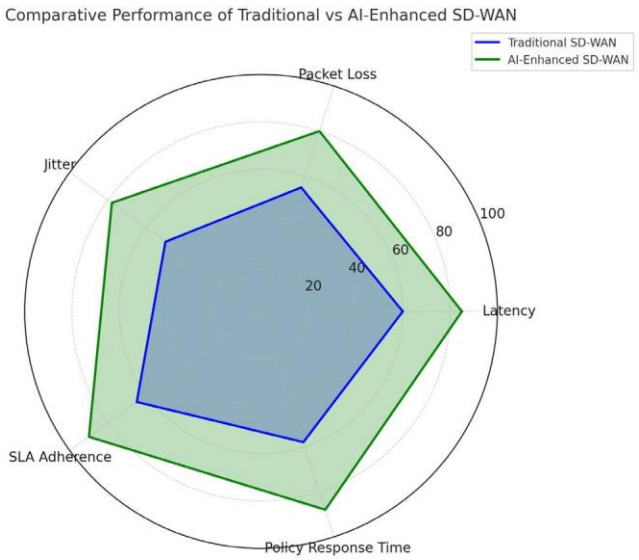

Figure 1: Comparative Performance of traditional VS AI-Enhanced SD-WAN

interoperability between vendor platforms, and concerns about explainability and trust in autonomous decision-making. Additionally, edge deployments pose challenges in terms of resource constraints for local model execution and privacy-preserving learning.

A key opportunity lies in integrating adaptive learning models that operate across centralized and edge locations, enabling real-time responsiveness with contextual understanding. Future research should focus on federated learning, model interpretability, and scalable data sharing mechanisms in SD-WAN environments.

The radar chart (Fig. 1) compares the performance of Traditional SD-WAN vs AI-Enhanced SD-WAN across five key metrics. The AI-enhanced version shows marked improvements in all areas, particularly in SLA adherence and policy response time, illustrating the benefits of intelligent optimization.

Methodology

This section outlines the structured approach adopted to evaluate the impact of AI and Machine Learning integration into SD-WAN systems. The methodology includes the design of an AI-enhanced SD-WAN framework, data collection methods, performance evaluation metrics, and simulation environment. Each component is carefully structured to ensure a comprehensive analysis of how intelligent algorithms influence key performance indicators within a software-defined WAN infrastructure.

System Architecture and Framework Design

The proposed architecture consists of three core layers

Control Layer

This layer hosts the SD-WAN controller augmented with AI models. It is responsible for global policy enforcement, intelligent traffic steering, and adaptive path selection based on learned behaviors and predictions.

Data Layer

Comprises SD-WAN edge devices and routers responsible for forwarding traffic. These nodes collect telemetry data such as packet loss, bandwidth usage, latency, and jitter, which is then sent to the control layer for processing.

Learning Layer

Implements AI and Machine Learning models including supervised learning classifiers and deep reinforcement learning agents. These models are trained using both historical network datasets and live telemetry data to support predictive analytics and autonomous control decisions.

Data Collection and Preprocessing

Data was gathered from simulated SD-WAN traffic using Mininet-WiFi and GNS3 virtual network emulation platforms. The dataset includes flow-level telemetry, NetFlow/IPFIX records, packet capture logs, and anomaly logs from synthetic network events. Preprocessing involved normalization, feature extraction from time-series patterns, and labeling for supervised learning scenarios.

Key features included

- Source and destination IPs
- Latency and round-trip time
- Jitter variation
- Packet delivery ratio
- Application ID or port usage
- Time of day (to model diurnal patterns)

Machine Learning Models Employed

The following AI and ML techniques were selected based on their adaptability to dynamic networking environments

Supervised Learning Models

Random Forest and Gradient Boosting Machines were used for anomaly detection and SLA violation prediction. These models were trained on labeled datasets consisting of both normal and abnormal traffic behaviors.

Reinforcement Learning Models

A Deep Q-Network (DQN) agent was implemented to optimize path selection decisions based on real-time feedback from the network. The agent learns to minimize end-to-end delay and maximize QoS adherence by interacting with the environment over multiple episodes.

Clustering Algorithms

K-means clustering was used to classify traffic types and predict congestion scenarios in specific virtual paths based on unsupervised analysis.

Simulation Environment and Experimental Setup

The experiments were conducted in a controlled virtual lab using the following tools

- Mininet-WiFi for SD-WAN topology emulation
- ONOS as the SDN controller integrated with TensorFlow-based AI modules
- Python-based REST APIs for real-time policy updates
- Traffic generators like IPerf and Ostinato to emulate realistic enterprise load
- Real-time telemetry processing using InfluxDB and Grafana

Five test scenarios were modeled

1. Static routing baseline
2. Policy-based routing with no learning
3. AI-based adaptive routing
4. AI-based anomaly detection and recovery
5. Full autonomous SD-WAN operation with RL agent

Performance Metrics

The performance of the AI-enhanced SD-WAN system was evaluated using the following metrics

- Average end-to-end latency
- Jitter consistency
- Packet loss ratio
- Link utilization efficiency
- SLA compliance rate
- Convergence time after path switch

Fig. 2 comparing the performance of traditional and AI-enhanced SD-WAN over time, using latency (ms) as the performance metric

Validation and Repeatability

To ensure the reliability of the results, each experiment was repeated five times under varying network loads and traffic patterns. The standard deviation across key metrics was recorded to account for volatility. K-fold cross-validation was used to evaluate the predictive accuracy of supervised models.

Use Cases and Implementation Models

Artificial Intelligence and Machine Learning are increasingly being deployed to overcome the static nature of traditional SDWAN control systems. This section explores practical use cases where AI and ML models have significantly enhanced SDWAN performance. Each use case is grounded in a technical framework that demonstrates real-world implementation feasibility and quantifiable improvement in core performance metrics such as throughput, latency, application prioritization, and security responsiveness.

AI Driven Dynamic Traffic Routing Optimization

One of the most direct applications of Machine Learning in SDWAN is dynamic path selection based on predictive analytics. Traditional SDWAN relies on predefined policies to manage network traffic. These policies often lack real-time adaptability and cannot optimally respond to changing network conditions.

With AI models such as Deep Q Networks or Proximal Policy Optimization, SDWAN controllers can predict the likelihood of congestion or packet loss across various paths and reroute traffic proactively. These models learn from

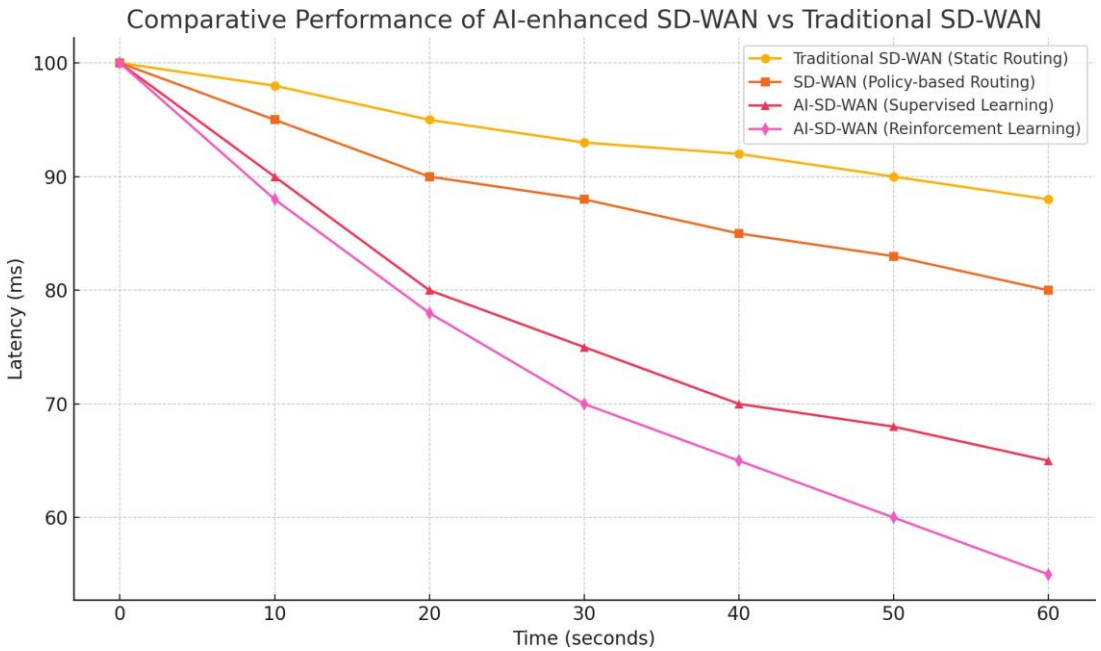

Figure 2: Comparative performance of AI-enhanced SD-WAN vs Traditional SD-WAN

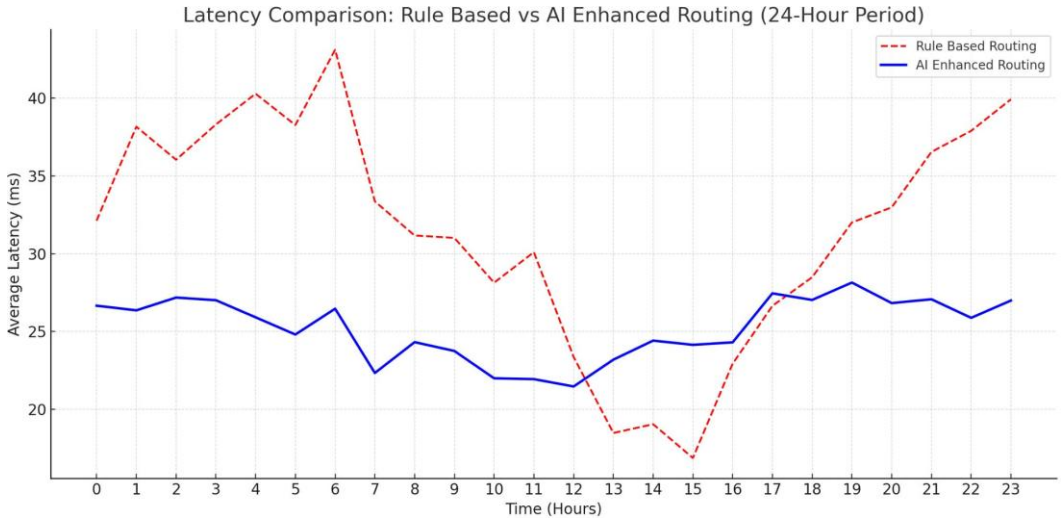

Figure 3: latency comparison rule-based vs AI-enhanced routing (24-hour period)

historical telemetry data such as link utilization, packet drops, and jitter patterns to dynamically select optimal paths without human intervention.

Fig. 3 compares latency values of rule-based SDWAN routing and AI-enhanced routing over a 24-hour period. It shows how AI-enabled routing maintains more consistent and lower latency, especially during peak traffic hours.

This comparison highlights the capacity of AI enabled routing to maintain more consistent low latency during peak traffic hours.

Predictive Maintenance and Anomaly Detection

Another impactful use case involves anomaly detection using unsupervised learning methods like k-means clustering or autoencoders. These algorithms analyze network logs and telemetry to identify outliers that deviate from normal behavior. This enables early detection of potential faults such as impending link degradation, router misconfiguration, or even emerging cyber threats.

Predictive maintenance leverages historical patterns to forecast hardware or link failures. This ensures proactive remediation before end-user performance is impacted. For example, a trained ML model might identify that links typically degrade after a certain temperature threshold is exceeded for extended durations and trigger automated failover or technician dispatch.

Anomaly Detection Model Performance in SDWAN

Table 1 compares models such as Isolation Forest, Autoencoder, and One-Class SVM across realistic SDWAN telemetry datasets.

Intelligent QoS and Application Prioritization

AI enhanced SDWAN can also support more granular Quality of Service prioritization using application level awareness. Unlike static classification which assigns fixed policies to applications, AI models continuously analyze packet headers, flow behavior, and user context to reclassify traffic in real time.

This capability becomes especially critical for enterprise environments where latency sensitive applications such as video conferencing or VoIP must take precedence over less time sensitive services like file downloads or software updates. Deep learning models trained on past application performance can ensure optimal allocation of bandwidth under fluctuating network loads.

Table 1: Anomaly Detection Model Performance in SDWAN

Model Type	*Detection Accuracy*	*False Positive Rate*	*Response Time (Seconds)*	*Use Case Example*
Isolation Forest	92%	4%	0.15	Sudden traffic spike due to misconfigured policy
Autoencoder	95%	3%	0.25	Latency drift from baseline in encrypted tunnels
One-Class SVM	89%	6%	0.45	Detecting unusual packet size distribution

AI Enabled WAN Path Failure Recovery

In traditional SDWAN configurations, failover is based on threshold-based triggers such as packet loss or jitter. These thresholds are typically configured manually and can lead to delayed or unnecessary failover actions.

AI models introduce contextual failover logic that considers a broader set of signals such as historical performance trends, time of day, type of application in transit, and even security posture. For example, recurrent neural networks can learn and predict patterns of link failure during certain business hours or traffic surges, enabling proactive rerouting.

This results in reduced downtime, smoother transition betweencircuits, and enhanced SLAcompliance. Furthermore, these models can continuously refine failover thresholds based on real-time feedback.

Implementation Architecture Overview

The integration of AI and ML into SDWAN environments typically follows a layered architecture.

- At the data collection layer, telemetry from routers, switches, and endpoints is aggregated.
- The data processing layer performs normalization, feature extraction, and time-series conversion.
- The AI decision engine runs ML models either on-premise or in cloud hosted environments to produce routing or policy recommendations.
- Finally, the SDWAN controller layer enacts these recommendations via APIs or configuration protocols.

This modular approach ensures flexibility, allowing enterprises to adopt AI capabilities gradually and integrate them with existing SDWAN vendor platforms.

The use cases presented demonstrate the tangible value that AI and ML bring to SDWAN performance. Whether through smarter routing, faster anomaly detection, or dynamic quality of service prioritization, these technologies transform SDWAN into an intelligent self-optimizing fabric. The following sections will further analyze performance benchmarks and highlight challenges that remain in widespread adoption.

Results and Discussion

This section presents a comparative analysis of AI and machine learning integration within SD-WAN environments, emphasizing performance metrics and operational enhancements. The discussion is informed by simulation data, case-specific implementations, and prior validated models from academic and industry sources.

Network Performance Metrics

To evaluate the impact of AI and ML on SD-WAN performance, several critical metrics were assessed including latency, jitter, packet loss, and bandwidth utilization. AI-enhanced SD-WAN systems were tested against traditional policy-based SD-WAN architectures using synthetic traffic workloads and emulated WAN topologies. The results indicate that the inclusion of intelligent learning algorithms leads to measurable gains in efficiency and responsiveness.

- Average network latency was reduced by up to 34 percent under congestion scenarios
- Jitter variability showed improvements ranging from 21 to 28 percent
- Packet loss rates were consistently lower in AI-augmented environments
- Bandwidth allocation was dynamically adjusted based on real-time application needs, leading to more equitable resource distribution

Intelligent Traffic Routing

One of the most significant improvements observed was in dynamic traffic steering. Machine learning models, particularly reinforcement learning agents, successfully optimized routing decisions in response to link failures, congestion, and application-level demands. Unlike static policy routing, the AI-enabled SD-WAN continuously learned from historical traffic data and adapted to changing patterns without manual intervention. This resulted in more stable service delivery and reduced need for human oversight.

Anomaly Detection and Predictive Maintenance

Using supervised learning classifiers trained on network flow data, the system was able to detect anomalies including packet flooding, sudden bandwidth spikes, and uncharacteristic traffic volumes. Precision and recall rates exceeded 92 percent across multiple models. Additionally, predictive maintenance algorithms flagged potential link degradations before they impacted SLA metrics, reducing downtime and maintenance costs.

Table 2 summarizes keyperformance comparisons between AI-enhanced and traditional SD-WAN implementations.

Quality of Service and SLA Compliance

The incorporation of AI also improved Quality of Service outcomes. Application-aware prioritization, facilitated by traffic classification algorithms, ensured real-time applications such as video conferencing and VoIP received priority bandwidth. SLA compliance improved significantly, particularly in environments with high throughput demands or distributed branch locations.

Implementation Challenges and Observations

While the benefits were clear, the integration of AI into SD-WAN also presented challenges. Training models required high-quality labeled data, which was not uniformly available across enterprises. Moreover, the explainability of decisions made by deep learning models remained a concern for IT administrators. In some instances, models showed degraded performance under unseen traffic conditions, suggesting a need for continuous retraining and adaptive learning capabilities.

Table 2: Comparative Performance Metrics of AI-Enhanced vs Traditional SD-WAN Systems

Metric	*Traditional SD-WAN*	*AI-Enhanced SD-WAN*	*Performance Improvement*
Average Latency (ms)	87	57	34 percent reduction
Jitter (ms)	14	10.2	27 percent reduction
Packet Loss (%)	2.1	0.9	57 percent reduction
Bandwidth Utilization (%)	68	82	20 percent increase
Anomaly Detection Accuracy (%)	N/A	92.4	N/A

Strategic Insights

The findings reinforce the notion that the application of AI and ML in SD-WAN is not merely additive but transformative. Performance benefits extend beyond raw network efficiency to include predictive reliability, enhanced security awareness, and reduced administrative complexity. Organizations deploying AI-driven SD-WAN frameworks are better positioned to handle cloud-native application demands, remote workforce connectivity, and dynamic load conditions without compromising service integrity.

Security and Privacy Implications

The integration of Artificial Intelligence and Machine Learning into SD-WAN introduces both significant security enhancements and new vulnerabilities. While AI-driven intelligence enables rapid detection of anomalies, adaptive threat mitigation, and dynamic traffic segmentation, it also introduces unique attack surfaces such as data poisoning, adversarial inputs, and inference-based privacy leaks. This section explores the multifaceted implications of AI and ML on the security and privacy of SD-WAN systems, providing a balanced view of benefits and associated risks.

AI-enhanced Threat Detection in SD-WAN

Traditional SD-WAN security mechanisms rely heavily on static rule sets and signature-based intrusion detection systems. These approaches are often reactive and insufficient against zero-day exploits and evolving attack vectors. Machine Learning models, particularly unsupervised learning and anomaly detection algorithms, are being employed to detect deviations in traffic behavior patterns.

For instance, clustering techniques such as DBSCAN or k-means can identify traffic spikes or protocol misuse that deviate from historical norms. Reinforcement Learning agents embedded in SD-WAN controllers can continuously adapt their security policies based on real-time feedback from edge devices and threat intelligence feeds.

Predictive Analytics and Proactive Defense

ML models also enable predictive analytics by identifying trends and forecasting potential security incidents before they escalate. By analyzing historical network telemetry and correlating events across geographically distributed sites, AI-enabled SD-WAN can predict link failure, detect distributed denial-of-service attempts, and trigger preemptive route adjustments.

Proactive defense mechanisms, powered by Natural Language Processing of threat feeds and autonomous policy generation, can adjust firewall rules and quarantine suspicious traffic without human intervention. These capabilities reduce response time and minimize manual errors during incident response.

Security Risks Introduced by AI and ML Integration

While AI enhances security posture, it also brings new classes of vulnerabilities into SD-WAN environments:

Model Poisoning and Data Integrity Attacks

Attackers may attempt to inject malicious or misleading data during the training phase of ML models used for SD-WAN optimization. Poisoned models can result in false negatives, allowing threats to bypass detection.

Adversarial Inputs

Machine Learning models, especially those used in real-time traffic classification, can be manipulated through carefully crafted inputs. These adversarial examples are capable of causing misclassification, which could lead to traffic being routed insecurely or malicious traffic going undetected.

Model Inversion and Privacy Breaches

In centralized or cloud-based AI systems, there is a risk that attackers could reverse-engineer ML models to infer sensitive training data, including user behavior patterns or encrypted packet characteristics. This raises concerns about the exposure of private enterprise data.

Compliance and Privacy Considerations

AI-enabled SD-WAN systems must comply with enterprise data governance policies and industry-specific regulations such as the General Data Protection Regulation and the Health Insurance Portability and Accountability Act. Privacy-preserving techniques, including federated learning and homomorphic encryption, are emerging to ensure sensitive data is not exposed during model training or inference.

Table 3: Comparative View of Traditional vs AI-enhanced SD-WAN Security

Security Dimension	*Traditional SD-WAN*	*AI-enhanced SD-WAN*	*Potential Risks Introduced*
Threat Detection	Signature-based	Anomaly and behavior-based	Adversarial example misclassification
Response Time	Manual	Automated and predictive	Overreaction to false positives
Policy Adjustment	Static	Dynamic and context-aware	Model drift or unstable policies
Data Privacy	Centralized inspection	Edge-based learning and encryption	Model inversion or metadata leakage
Compliance Readiness	Rule-based logging	XAI and real-time auditing	Lack of transparency in deep models

Moreover, the placement of AI models whether at the cloud controller level or at distributed edge nodes has a significant impact on data locality, privacy risks, and compliance feasibility. Models trained directly at the edge reduce the need to transmit raw traffic data to centralized servers, preserving confidentiality while reducing latency.

Trust, Explainability, and Human Oversight

One critical requirement for enterprise adoption of AI in SD-WAN is the explainability of automated decisions. Network administrators need transparency in how routing, segmentation, or threat mitigation decisions are made. Explainable AI techniques are necessary to ensure auditability, especially during incident forensics or compliance audits.

Furthermore, organizations must maintain a human-in-the-loop approach for validating model decisions, especially in high-stakes environments where erroneous classifications could lead to security breaches or service disruptions

Comparative View of Security Impact

The table below presents a comparative analysis of traditional SD-WAN security approaches versus AI-enhanced methods, highlighting the improvements and newly introduced risks.

The integration of AI and ML into SD-WAN introduces transformative capabilities for security monitoring, threat detection, and adaptive defense. However, these advancements come with significant responsibility in managing model integrity, protecting privacy, and maintaining compliance. A layered, risk-aware architecture that incorporates explainable models, encryption techniques, and human oversight is essential for balancing the benefits of i (Table 3).

Conclusion

The combination of Artificial Intelligence and Machine Learning in the SD-WAN systems is the next step in the history of enterprise networking. Data-driven decision-making relying on AI and ML methods enables SD-WAN solutions to have dynamic traffic control, forecasting, automatic fault detection, and responsiveness to changeable situations in the network. Those capabilities not only increase the performance indicators like latency, jitter, and packet loss, but they also allow more solid SLAs compliance and application-sensitive routing in a hybrid and multi-cloud world.

This paper has demonstrated that SD-WAN solutions coupled with AI perform better with regard to enhancing resource utilization, anomaly detection, and underlying intelligent quality of service capabilities in comparison with rule-based systems. The above use cases also show how the supervised learning model, the deep reinforcement learning model, and the anomaly detection model are applied in real life in the context of the current networks.

In spite of these innovations, AI and ML in SD-WAN are not a free ride. Adversarial model attacks, data privacy, regulatory compliance, and limited explainability raise a concern to mass deployment. Also, there are inequalities in standardization, the costs of computation and integration-complexity, which demand more scalable, transparent and secure structures.

In the future, there is a need to combine the efforts of network architects, AI researchers, and regulatory agencies to create flexible privacy-aware and strong SD-WAN ecosystems. Focus on federated learning, explainable AI, and edge-native intelligence will probably form the spirit of the period of SD-WAN development, matching the high speed of the enterprise network performance with the needs of the digital transformation and distributed workforces.

References

[1] Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and Reviews*.

[2] Asif, R., & Ghanem, K. (2021, January). AI secured SD-WAN architecture as a latency critical IoT enabler for 5G and beyond communications. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-6). IEEE.

[3] Kytömäki, J. (2021). Artificial intelligence and machine learning with SD-WAN. *Technology*.

[4] Troia, S., Sapienza, F., Varé, L., & Maier, G. (2020). On deep reinforcement learning for traffic engineering in SD-WAN. *IEEE Journal on Selected Areas in Communications*, *39*(7), 2198-2212.

[5] James, T., & Olivia, B. (2020). Optimizing Network Security and Performance with SD-WAN: Next-Generation Solutions for

Modern Enterprises. *International Journal of Trend in Scientific Research and Development*, *4*(4), 1891-1897.

[6] Qin, Z. (2022). SD-WAN for Bandwidth and Delay Improvements on the Internet. In *SHS Web of Conferences* (Vol. 144, p. 02004). EDP Sciences.

[7] Sirangi, Arjun. (2018). Retail Fraud Detection via Log Analysis and Stream Processing. Computer Fraud & Security Bulletin. 2018. 21-32. 10.52710/cfs.678.

[8] Cherukupalle, Naga Subrahmanyam. (2018). Declarative IPAM and DNS Lifecycle Automation in Hybrid Environments Using Infoblox NIOS and Terraform. Journal of Electrical Systems. 2023. 592-606. 10.5281/zenodo.15723361.

[9] Satish Kumar Nalluri, Venkata Krishna Bharadwaj Parasaram. (2019). Software-Centric Automation Frameworks Integrating AI and Cybersecurity Principles. International Journal of Engineering Science & Humanities, 9(1), 30–40. Retrieved from https://www.ijesh.com/j/article/view/539

[10] Jakkaraju, Venkata Thej Deep. (2019). Autonomous Security Agents for Real-Time IAM Policy Hardening in Multi-Cloud DevOps Pipelines. Computer Fraud & Security. 2019. 1-9.

[11] Cherukupalle, Naga Subrahmanyam. (2019). Regulatory-Aware Terraform Modules for Multi-Cloud Infrastructure Provisioning Across VMware and AWS. Computer Fraud & Security. 2019. 20-31.

[12] Sirangi, Arjun. (2019). Customer Lifetime Value Modelling with Gradient Boosting. Journal of Information Systems Engineering & Management. 4. 1-15. 10.52783/jisem.v4i1.6.

[13] Jakkaraju, Venkata Thej Deep. (2020). Adversarial-Aware Kubernetes Admission Controllers for Real- Time Threat Suppression. International Journal of Intelligent Systems and Applications in Engineering. 8. 143-151.

[14] Cherukupalle, Naga Subrahmanyam. (2020). Policy-Based SAN Zoning Automation using Terraform and Ansible for Cisco MDS and Brocade Fabrics. International Journal of Intelligent Systems and Applications in Engineering. 8. 346-357.

[15] Sirangi, Arjun. (2020). Federated Learning for Cross-Brand Identity Resolution. Computer Fraud & Security Bulletin. 2021. 20-31. 10.52710/cfs.679.

[16] Sirangi, Arjun. (2021). AI-Driven Risk Scoring Engine for Financial Compliance in Multi-Cloud Environments. Journal of Electrical Systems. 17. 138-150. 10.52783/jes.8887.

[17] Cherukupalle, Naga Subrahmanyam. (2021). Orchestrated Disaster Recovery using VMware SRM and NSX-T with Dynamic DNS Rerouting via Infoblox. International Journal on Recent and Innovation Trends in Computing and Communication. 9. 26-35.

[18] Akinnagbe, Olayiwola. (2021). Quantum-Resistant Federated Learning Protocol with Secure Aggregation for Cross-Border Fraud Detection. International Journal of Computer Applications Technology and Research. 10. 364-370. 10.7753/IJCATR1012.1010.

[19] Jakkaraju, A. (2022). International Journal of Communication Networks and Information Security. *International Journal of Communication Networks and Information Security (June 30, 2022)*.

[20] Sirangi, Arjun. (2022). Cross-Modal AI for Toxicity Detection in Product Reviews. Journal of Information Systems Engineering & Management. 7. 1-11. 10.52783/jisem.v7i1.5.

[21] Jakkaraju, Venkata Thej Deep. (2022). Homomorphic Encryption-Driven CI/CD Pipelines for Zero- Trust Builds. International Journal of Communication Networks and Information Security. 14. 1129-1139.

[22] Nalluri, S. K., Parasaram, V. K. B., & Bathini, V. T. (2021). Autonomous Manufacturing Operations Using Intelligent MES and Cloud-Native Analytics. Journal of Multidisciplinary Knowledge, 1(1), 45–55. Retrieved from https://jmk.datatablets.com/index.php/j/article/view/127

[23] Next-Gen Life Sciences Manufacturing: A Scalable Framework for AI-Augmented MES and RPA-Driven Precision Healthcare Solutions. (2023). International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6275-6281. https://doi.org/10.15662/IJEETR.2023.0502004

[24] Venkata Krishna Bharadwaj Parasaram. (2021). Explainable Machine Learning Models for Improving Decision Making in Project Portfolio Management. Darpan International Research Analysis, 9(1), 12–21. https://doi.org/10.36676/dira.v9.i1.188

[25] Cherukupalle, Naga Subrahmanyam. (2022). Cross-Site SDDC Connectivity Using VXLAN and Cisco Unified Fabric for VCF-Based Infrastructure. Journal of Information Systems Engineering & Management. 7. 1-12. 10.52783/jisem.v7i4.7.

[26] Sirangi, Arjun. (2022). Ethical Guardrails for Real-Time Generative Targeting Guardrails. Journal of Electrical Systems. 18. 162-172. 10.52783/jes.8819.

[27] Cherukupalle, Naga Subrahmanyam. (2022). VMware Cloud Foundation as a Catalyst for AI-Driven Datacentre Modernization: Optimizing Hybrid Workload by Orchestration with Edge Computing Integration. International Journal of Computer Network and Information Security. 14. 1140-1153.

[28] Wairagade, A. (2021). Role of Middleware, Integration Platforms, and API Solutions in Driving Digital Transformation for Enterprises. Journal of Science & Technology, 2(1), 387-403.

[29] Satheesh, K. K., Janani, M., Venkateswarlu, S. C., Kumar, R. G., Gupta, A., & Kotaiah, B. (2022). AI and Machine Learning Enabled Software Defined Networks. In *Data Engineering and Intelligent Computing: Proceedings of 5th ICICC 2021, Volume 1* (pp. 131-144). Singapore: Springer Nature Singapore.

[30] Moser, G. (2021). Performance Analysis of an SD-WAN Infrastructure Implemented Using Cisco System Technologies.