Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(3):98-104

Research Article ISSN: 2394 - 658X

Network Automation and Orchestration: AI-Driven Self-Healing Networks and Zero-Touch Provisioning

Ankita Sharma

Senior Specialist
HCL Technologies Ltd., Noida, UP, India
ankitash@hcl.com

ABSTRACT

This study analyzes the changing dynamics of network automation and orchestration, highlighting the contributions of Artificial Intelligence (AI) and Machine Learning (ML) in improving network stability, scalability, and efficiency. We examine the development of self-healing networks for autonomous fault identification and rectification, SD-WAN automation for hybrid cloud settings, and zero-touch provisioning for efficient network administration. This investigation underscores the role of AI and ML in advancing the next generation of network automation, paving the way for progressively autonomous network environments.

Keywords: Network Automation, Orchestration, Artificial Intelligence, Machine Learning, SD-WAN, Zero-Touch Provisioning, Self-Healing Networks

---

INTRODUCTION

In recent years, the demand for efficient, scalable, and resilient network infrastructure has significantly increased due to digital transformation across industries, the emergence of cloud computing, and the expansion of Internet of Things (IoT) devices. Organizations increasingly depend on networks to integrate diverse systems, facilitate essential applications, and provide uninterrupted communication across worldwide operations. Conventional networks, necessitating human configuration, monitoring, and troubleshooting, face challenges in fulfilling these requirements due to their complexity and restricted scalability. Furthermore, as network environments expand in complexity and scale, ensuring consistent performance, dependability, and security becomes ever more difficult, with human oversight susceptible to errors and inefficiencies.

Network automation and orchestration have become vital strategies to tackle these difficulties. Network automation entails employing software to autonomously install, manage, and test network equipment, therefore diminishing the necessity for manual intervention and facilitating the scalability and adaptability of networks in response to fluctuating demand. Orchestration entails the coordination of numerous automated actions to establish a unified, optimized workflow throughout the network, guaranteeing that each automated activity functions in harmony with the others. Collectively, these methodologies equip enterprises with the flexibility to dynamically manage intricate network infrastructures with minimal interruption.

Progress in Artificial Intelligence (AI) and Machine Learning (ML) has introduced a novel aspect to network automation and orchestration, allowing networks to not only react to changes but also to anticipate and proactively resolve issues. Artificial Intelligence and Machine Learning algorithms facilitate the instantaneous analysis of extensive network data, uncovering patterns that would be difficult, if not unfeasible, for human operators to discern. This intelligence layer improves automated networks' capacity to forecast demand, detect anomalies, optimize traffic flow, and automatically identify and rectify errors. AI and ML facilitate networks to function with enhanced efficiency, security, and dependability, simultaneously alleviating the workload on IT staff.

A significant use of AI-driven network automation is the self-healing network, a notion wherein networks autonomously identify and rectify errors without human involvement. Self-healing networks utilize artificial intelligence to incessantly assess the condition of network components, anticipate possible failures, and implement corrective measures prior to affecting end users. This self-sufficient defect detection and rectification system

minimizes downtime, promotes service reliability, and ultimately improves the user experience. Self-healing capabilities are especially advantageous in industries where network availability is essential, like healthcare, banking, and manufacturing, as they reduce interruptions that may result in operational or financial detriment.

A significant advancement in network automation is the Software-Defined Wide Area Network (SD-WAN), which offers adaptable, dependable, and effective communication across distant locations, cloud infrastructures, and data centers. SD-WAN technology enables enterprises to oversee and regulate their WAN connections using software, streamlining the configuration and management of network traffic. Through the integration of AI and automation, SD-WAN systems can adeptly route traffic, prioritize essential applications, and react to fluctuations in network conditions instantaneously. This automation is especially advantageous in hybrid cloud scenarios, where enterprises must seamlessly balance traffic between on-premises and cloud infrastructures. AI-augmented SD-WAN solutions empower enterprises to boost performance, minimize latency, and maintain reliable connectivity throughout their scattered networks.

Zero-Touch Provisioning (ZTP) streamlines network operations by automating the deployment and setup of network devices. In conventional networks, the configuration of new devices necessitates manual setup, frequently requiring on-site expert assistance and heightening the probability of configuration errors. Zero Touch Provisioning (ZTP) enables the automatic configuration and deployment of new devices upon their connection to the network, utilizing pre-defined templates and policies. This capacity optimizes network expansion and minimizes the time needed to deploy additional devices, rendering it an essential asset in extensive network settings, such as telecommunications and IoT, where numerous devices may require simultaneous management. Furthermore, ZTP bolsters security by guaranteeing that each device adheres to network policies upon connection, thereby mitigating the likelihood of vulnerabilities stemming from misconfigurations.

This study is to examine the multifaceted aspects of network automation and orchestration, particularly emphasizing the role of AI and ML in enhancing self-healing networks, SD-WAN automation, and zero-touch provisioning. We investigate the foundational technologies, evaluate practical applications, and assess the advantages and obstacles related to these methodologies. By comprehending the present landscape and future prospects of AI-driven network automation, organizations can strategically adopt these technologies, establishing networks that are resilient, efficient, and adept at addressing the requirements of a swiftly changing digital environment.

THE FUNCTION OF AI AND ML IN NETWORK AUTOMATION

The incorporation of Artificial Intelligence (AI) and Machine Learning (ML) into network automation signifies a substantial transition from static, rule-based frameworks to adaptive, intelligent networks capable of self-optimization utilizing real-time data. Conventional network automation depended significantly on pre-established scripts and human-operated operations. Although proficient for uncomplicated tasks, these strategies falter when confronted with the complexity, scale, and dynamic characteristics of contemporary network systems. In contrast, AI and ML empower networks to learn from historical experiences, adjust to unexpected problems, and perpetually enhance their operations. This section examines the influence of AI and ML on network efficiency, security, and performance, highlighting their transformational capabilities in contemporary networking.

A. Improving Network Efficiency using Artificial Intelligence and Machine Learning

In conventional networks, managers are required to manually configure each device and modify network settings, a labor-intensive procedure susceptible to human error. Artificial Intelligence and Machine Learning improve network efficiency through proactive management and real-time optimization, enabling network operators to manage larger, more complicated networks with reduced resources and minimal manual involvement.

• Predictive Analytics and Traffic Optimization

Predictive analytics driven by machine learning algorithms are essential for network efficiency, since they anticipate network demand using historical and real-time data. By consistently analyzing network traffic, AI can forecast peak usage times, enabling networks to deploy resources more effectively, prevent congestion, and minimize latency. In telecoms, AI-driven systems can forecast bandwidth demand across several regions and reallocate resources to ensure service quality, especially during peak hours or significant events.

Traffic optimization is a crucial domain in which AI excels. Through the analysis of consumption patterns, AI can dynamically change bandwidth, prioritize essential apps, and optimize traffic routing, so reducing latency and enhancing throughput. In workplace networks, an AI-driven system may prioritize video conferencing over file transfers during peak hours, so assuring optimal bandwidth allocation. This astute allocation mitigates network bottlenecks, improves user experience, and allows networks to function with increased efficiency and responsiveness.

• Resource Allocation and Load Distribution

The autonomous management of network resources by AI is crucial for load balancing, which entails the distribution of network traffic among various servers or connections to avert the risk of any single node becoming a bottleneck. AI can identify when a node nears its capacity through real-time monitoring and redistribute traffic to

ensure optimal performance. This dynamic load balancing is particularly advantageous in cloud situations, where workloads and network requirements can change swiftly.

Moreover, AI can anticipate the necessity for supplementary resources by analyzing observed trends and adjust accordingly to fluctuations in demand. In hybrid cloud networks, artificial intelligence may distribute workloads between on-premises and cloud infrastructure according to availability and cost, so assuring an equitable and economical utilization of resources. This capacity enhances network efficiency and allows enterprises to optimize their infrastructure investments.

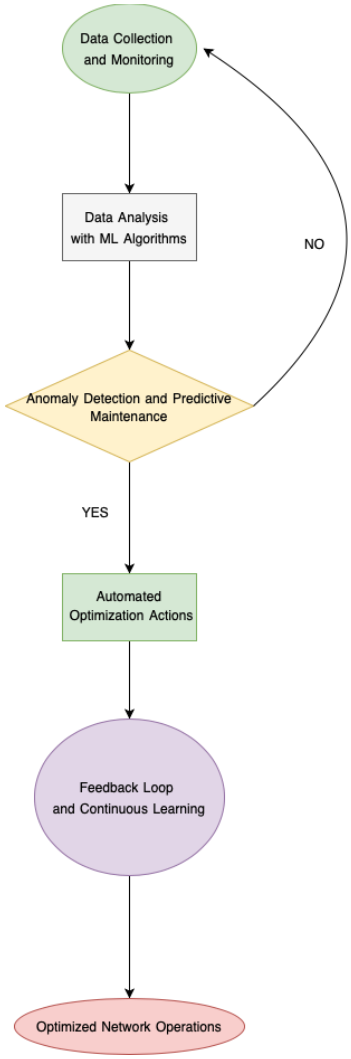

Figure 1: AI-Driven Network Efficiency Optimization Process

B. Artificial Intelligence-Driven Network Security

As networks increase in complexity, they concurrently become increasingly susceptible to advanced cyber assaults. Artificial Intelligence and Machine Learning have implemented advanced automation and intelligence in network security, enabling systems to identify, react to, and anticipate possible security incidents.

• Immediate Threat Identification and Mitigation

AI-driven security solutions augment network security by the constant surveillance of traffic patterns and the detection of anomalies that may signify hostile activity. In contrast to conventional rule-based systems that can solely address recognized dangers, AI systems has the capability to detect abnormalities in real time, thereby recognizing and autonomously responding to novel hazards. An AI system analyzing network traffic may detect an anomalous surge in data requests from a singular IP address, indicating a potential Distributed Denial of Service (DDoS) attack.

Upon detection of a possible threat, AI systems can autonomously respond by implementing defensive measures, like the isolation of impacted nodes or the blockage of suspect traffic. Automated responses expedite the resolution of security issues, thereby mitigating possible damage. This capacity is especially beneficial in extensive, distributed networks, such as those in financial institutions, where swift detection and response are essential to avert data breaches.

• Machine Learning for Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Conventional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) depend on static regulations, rendering them vulnerable to sophisticated, dynamic threats. ML-enhanced IDS and IPS continuously learn from network traffic data, enhancing their capacity to differentiate between regular and aberrant behaviors. By recognizing patterns linked to both innocuous and harmful activities, machine learning algorithms can more precisely identify possible intrusions and diminish false positives, a prevalent challenge in conventional intrusion detection and prevention systems.

Moreover, machine learning-based systems can adjust to new threats by recognizing prevalent patterns in assaults, such certain sequences of commands or requests that frequently precede harmful actions. They develop predictive models that foresee and avert attacks prior to their occurrence. This proactive security strategy fortifies networks against both identified and unidentified threats, rendering machine learning an indispensable component of contemporary network defense.

• Artificial Intelligence for Adaptive Security Policies

As network environments evolve, the maintenance of static security policies becomes unfeasible. Artificial intelligence facilitates adaptive security, permitting networks to modify security settings according on context and usage trends. An AI-driven system may implement more stringent access controls during peak traffic times or limit access to critical information upon detecting aberrant activity.

Adaptive security policies mitigate breach risks by ensuring that security measures develop in accordance with the network's requirements and circumstances. In corporate settings, this flexibility guarantees that security measures remain effective while not interfering with lawful traffic, thus harmonizing security with user experience.

C. AI-Enhanced Network Efficiency

Enhancing network efficiency necessitates continuous monitoring and adjustment, activities that AI and ML execute with exceptional speed and accuracy. Through the analysis of extensive data, AI systems may identify inefficiencies and bottlenecks, allowing networks to sustain optimal performance without necessitating manual interventions.

• Automated Quality of Service (QoS) Administration

Quality of Service (QoS) is essential in contexts where numerous applications vie for network resources. AI-driven QoS management systems autonomously prioritize traffic according to application specifications, user roles, and network circumstances. AI can prioritize voice-over-IP (VoIP) traffic over less urgent data, so maintaining superior audio quality during talks, even amid network congestion.

AI improves user experience and reduces latency in bandwidth-sensitive applications such as video conferencing and gaming by automating QoS management. This feature enables enterprises to provide dependable services while optimizing their network resources.

• Proactive Network Upkeep

Proactive maintenance constitutes an additional advantage of AI-optimized network performance. AI systems oversee the condition of network components, detecting indications of deterioration or performance decline prior to failures occurring. For example, by examining log data, an AI system may identify a gradual decline in a router's functionality and alert network managers to arrange maintenance or replacement.

Predictive maintenance diminishes unanticipated downtime and curtails expenses related to emergency repairs. In data centers and enterprise networks, where network uptime is paramount, AI-enabled preventative maintenance results in substantial savings in time and money.

• Dynamic Network Configuration and Autonomous Optimization

Artificial intelligence facilitates networks to autonomously configure and optimize themselves, modifying settings according to real-time conditions. Self-optimization entails modifying factors like as bandwidth allotment, routing pathways, and access policies in accordance with network requirements. In wireless networks, AI may oversee signal strength and modify access points to enhance coverage and minimize interference, so maintaining reliable connectivity for users.

Dynamic configuration enables networks to adapt to unforeseen occurrences, such as abrupt traffic surges or equipment malfunctions. AI-driven networks sustain maximum performance by automatically modifying configurations, offering durability and adaptability that static networks lack, even in adverse settings.

SELF-HEALING NETWORKS: AUTONOMOUS FAULT IDENTIFICATION AND RECTIFICATION

The notion of self-healing networks, in which AI independently identifies and rectifies network malfunctions, is progressively materializing. Self-healing networks diminish the necessity for human intervention in addressing network problems, resulting in increased uptime and reliability.

A. Fault Detection and Diagnosis

Artificial Intelligence and Machine Learning are employed to continuously monitor network health, identifying anomalies that may signify possible issues. Methods such as anomaly detection and predictive analytics empower

networks to recognize and resolve problems, including packet loss or hardware malfunctions, prior to their escalation [4].

B. Automated Fault Rectification

Upon detection of an issue, AI algorithms commence corrective measures, such traffic rerouting or network configuration adjustments, to ensure optimal performance. In a self-healing network, corrective measures are executed automatically, minimizing downtime and enhancing service availability. Case studies in extensive enterprise networks indicate that self-healing functionalities result in a 30% decrease in downtime and related expenses [5].

AUTOMATION OF SD-WAN IN HYBRID CLOUD ENVIRONMENTS

Organizations are progressively using hybrid and multi-cloud architectures, necessitating adaptable, effective, and dependable Wide Area Network (WAN) solutions to accommodate fluctuating connectivity requirements across on-premises infrastructure, cloud services, and remote locations. Software-Defined Wide Area Network (SD-WAN) technology has become an essential instrument for addressing these requirements, including software-defined functionalities that facilitate centralized management, policy-driven routing, and traffic prioritization. Nonetheless, the manual administration of SD-WAN across diverse settings and applications can be intricate and labor-intensive. AI-driven automation for SD-WAN enhances agility, optimizes network performance, and facilitates intelligent, automatic reactions to network events.

Artificial Intelligence and Machine Learning converge with Software-Defined Wide Area Networking to establish a flexible and robust network infrastructure, particularly advantageous for hybrid cloud environments. SD-WAN automation boosts connectivity between cloud providers and company data centers, optimizes traffic prioritization, and dynamically allocates resources to adapt to real-time requirements. This section examines the impact of AI-driven SD-WAN automation on hybrid cloud settings through centralized control, better traffic routing, and improved security.

A. Artificial Intelligence and Machine Learning in Software-Defined Wide Area Network Automation

Artificial Intelligence and Machine Learning are integral to Software-Defined Wide Area Networking by delivering real-time analytics on network performance, detecting traffic patterns, and adaptively modifying network configurations to enhance connection. These technologies enable SD-WAN systems to be self-optimizing and self-managing, therefore considerably diminishing the necessity for manual intervention.

• Real-Time Traffic Assessment and Enhancement

A primary benefit of AI-driven SD-WAN is its capacity for ongoing, real-time traffic analysis. AI systems examine data streams to discern network utilization trends, recognize critical applications, and distribute bandwidth appropriately. In a business employing a hybrid cloud configuration, SD-WAN automation can prioritize essential applications—such as ERP or CRM systems—by allocating dedicated bandwidth, so ensuring uninterrupted functionality even during peak demand times.

AI empowers SD-WAN to make decisions based on real-time traffic demands instead of predetermined rules, resulting in a more agile and effective utilization of network resources. AI-driven SD-WAN dynamically optimizes bandwidth allocation, enhancing application performance across the network, improving user experience, and ensuring optimal connectivity to cloud resources, irrespective of the physical location of applications or users.

• Automated Path Determination and Dynamic Routing

In conventional SD-WAN configurations, routing pathways are frequently pre-established, resulting in diminished performance at times of elevated demand or unforeseen network circumstances. Artificial Intelligence and Machine Learning revolutionize this process through automated path selection, enabling the system to dynamically determine the ideal route for each data packet according to real-time network conditions, including latency, congestion, and available capacity.

Dynamic routing is particularly advantageous in hybrid cloud situations, as data regularly transitions among on-premises infrastructure, private clouds, and public cloud providers. For instance, when a network connection to a particular cloud provider experiences congestion, AI-driven SD-WAN can autonomously redirect traffic to an alternate channel to preserve performance. This capacity to adjust instantaneously to network situations diminishes latency, averts bottlenecks, and guarantees that users encounter uniform performance throughout the network. Dynamic routing significantly reduces packet loss, a critical aspect in applications necessitating high reliability, such as VoIP and video conferencing.

• Proactive Load Distribution and Failover Administration

Managing traffic between diverse cloud services and data centers in multi-cloud and hybrid cloud settings can be intricate. AI-driven SD-WAN facilitates this process by proactively distributing loads across available network links, optimizing traffic allocation, and averting the overload of any singular link. The load balancing is governed by real-time data analytics, enabling SD-WAN systems to predict and alleviate potential problems prior to their impact on network performance.

AI improves SD-WAN's failover capabilities by promptly identifying link failures or performance deterioration and swiftly rerouting traffic to a backup path without interruption. For example, if a connection to a particular cloud provider break, the system instantly redirects traffic to an alternative channel, guaranteeing uninterrupted connectivity. Failover management is crucial for ensuring company continuity in sectors where uptime is vital, like financial services, healthcare, and manufacturing.

B. Benefits of Hybrid Cloud Networks

Hybrid cloud systems, integrating on-premises and cloud resources, necessitate SD-WAN solutions capable of managing the intricacies and fluctuations of multi-cloud operations. AI-driven SD-WAN automation fulfills these requirements by delivering uninterrupted connectivity, optimized application performance, and augmented security.

• Effortless Multi-Cloud Interconnectivity

Hybrid cloud designs may necessitate enterprises to interface with several cloud providers, resulting in difficulties with latency, cost, and data consistency. AI-powered SD-WAN solutions enable uninterrupted connectivity in these environments by dynamically modifying routes, capacity, and traffic priorities to maintain consistent performance across all cloud platforms.

AI-driven SD-WAN may optimize connections to various cloud providers, including AWS, Azure, and Google Cloud, by determining the most efficient path for each data transfer depending on latency and capacity. This capability guarantees that apps maintain a high-quality, uninterrupted connection to the cloud, irrespective of the provider or area utilized. This uninterrupted connectivity allows enterprises to utilize the advantages of many cloud providers, resulting in a more adaptable and robust network infrastructure.

• Improved Application Performance and Quality of Service (QoS) AI and ML-driven SD-WAN automation guarantees that essential apps constantly obtain necessary resources by prioritizing bandwidth according to application significance and performance criteria. In a hybrid cloud architecture that accommodates both standard and latency-sensitive apps, AI-driven SD-WAN can prioritize traffic for video conferencing or cloud-based ERP above less vital chores such as data backups.

AI automates and continually optimizes Quality of Service (QoS) management, guaranteeing optimal application performance despite varying network circumstances. This advanced QoS management mitigates performance deterioration during peak periods, minimizing delays, latency, and packet loss. Furthermore, it reduces downtime for applications dependent on high-performance connectivity, including those utilized in real-time analytics, customer support, and online collaboration.

• Cost Efficiency via Optimized Bandwidth Utilization

AI-driven SD-WAN enhances cost efficiency by optimizing bandwidth use across cloud services and WAN connections. Through the analysis of traffic patterns and the adjustment of resource distribution, AI optimizes the utilization of network resources, hence decreasing the necessity for expensive overprovisioning and mitigating cloud egress expenses.

During moments of diminished network demand, AI may decrease bandwidth allocation for non-essential applications, thereby liberating resources or minimizing expenses related to cloud utilization. Conversely, during periods of peak demand, AI might temporarily assign additional bandwidth to high-priority applications. This degree of resource optimization enhances performance and reduces operational costs related to hybrid cloud networking, rendering it a cost-efficient alternative for enterprises with intricate network requirements.

• Enhanced Security and Compliance

Security is paramount for enterprises utilizing hybrid and multi-cloud environments, as data frequently traverses diverse infrastructures with differing security mandates. AI-driven SD-WAN automation improves network security by analyzing traffic for irregularities, identifying threats, and uniformly applying security policies throughout the network.

AI enables SD-WAN to autonomously detect anomalous patterns, such as atypical traffic surges or data transmissions to illegal destinations, and to activate security measures accordingly. Furthermore, AI facilitates automated adherence to organizational policies and regulatory mandates by guaranteeing that all traffic complies with established security standards. This functionality is crucial in regulated sectors, where enterprises must comply with stringent data protection regulations, such as GDPR or HIPAA, when managing sensitive information in both cloud and on-premises settings.

• Scalability and Adaptability

Hybrid cloud infrastructures are frequently dynamic, with resources and network demands varying according to business requirements. AI-driven SD-WAN facilitates enhanced scalability and flexibility by autonomously modifying network resources and settings to meet fluctuations in demand. As new apps or services are implemented, SD-WAN may dynamically adjust to provide requisite connectivity and performance, without necessitating extensive manual configuration.

For example, if a business expands its cloud services to facilitate growth, AI-driven SD-WAN may autonomously modify routing and bandwidth to manage the increased traffic. This scalability enables enterprises to broaden their

operations without being hindered by network limitations, facilitating company expansion while guaranteeing uninterrupted access to both cloud and on-premises resources.

Table 1: Benefits of ai-driven sd-wan automation in hybrid cloud environments

Benefits	Description	Example in Use
Seamless Multi-Cloud Connectivity	Enables dynamic routing and traffic adjustments across multiple cloud providers to maintain consistent connectivity.	Connections between AWS, Azure, and on-premises systems.
Enhanced Application Performance and QoS	Prioritizes critical applications by allocating bandwidth based on real-time network conditions, ensuring optimized Quality of Service (QoS).	Video conferencing and cloud-based ERP systems.
Cost Efficiency	Optimizes bandwidth usage to reduce cloud egress fees and avoid overprovisioning, lowering operational costs.	Adjusting resources for non-critical applications during low demand.
Improved Security and Compliance	Monitors traffic for anomalies, enforces security protocols, and ensures compliance with policies and regulatory standards.	Data protection for HIPAA-compliant networks.
Scalability and Flexibility	Adapts network resources and configurations based on fluctuating demand, supporting network growth without extensive manual configuration.	Scaling connectivity for expanding cloud services.

ZERO-TOUCH PROVISIONING AND ITS APPLICATIONS IN NETWORK ADMINISTRATION

Zero-touch provisioning (ZTP) is an automation method that facilitates the automatic configuration and deployment of new devices upon their connection to the network, thereby obviating the necessity for manual configuration. This method streamlines network expansion and improves the efficacy of network administration.

A. ZTP Workflow and Execution

ZTP operates by utilizing pre-configured templates or policies that are implemented on new devices upon their connection. Upon deployment of a new router or switch, it autonomously retrieves its configuration files and updates firmware as required. This procedure significantly lowers the time needed for device provisioning, especially in extensive networks where manual configuration would be onerous [8].

B. Applications and Advantages

ZTP is advantageous for sectors necessitating the regular deployment of new devices, including telecommunications and IoT. Through the automation of device configuration, Zero Touch Provisioning (ZTP) mitigates human errors, expedites deployment durations, and enhances uniformity throughout the network. Furthermore, ZTP bolsters security by guaranteeing that all devices comply with network policies upon their introduction [9].

CONCLUSION

Network automation and orchestration, driven by AI and ML, represent a paradigm shift in network management. AI and ML enable proactive maintenance, dynamic adjustments, and real-time security enhancements, paving the way for autonomous, self-healing networks. SD-WAN automation and zero-touch provisioning further streamline network management, allowing networks to scale seamlessly while maintaining high levels of reliability and security. Future advancements in AI are expected to drive even more sophisticated automation capabilities, ultimately leading to networks that are fully self-managing and resilient.

REFERENCES

[1]. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.
[2]. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68–73.
[3]. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[4]. K. Elissa, “Title of paper if known,” unpublished.
[5]. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
[6]. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7]. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.