Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

AI-Driven Network Management: A Review of Machine Learning and Deep Learning Approaches

Kavitha S.

Professor, Department of Electronics and Communication Engineering, Hindusthan Institute of Technology, Coimbatore, India.

E-mail: dr.kavitha.s@hit.edu.in

Abstract

The AI-based network management has been recognized as an important facilitator for dealing with the increasing complexity, size, and dynamics of modern communication networks. The growth of data communication, heterogeneous networked devices, and stringent network services requires effective network management techniques to ensure the performance, reliability, and security of communication networks. Machine Learning (ML) and Deep Learning (DL) techniques are recognized as intelligent tools to support network management functions such as traffic prediction, resource management, anomaly detection, fault diagnosis, routing control, and security services. This review article discusses the state-of-the-art ML and DL techniques applied to network management, including the methodologies and paradigms of these techniques. The major developments in supervised, unsupervised, and reinforcement learning are discussed to support intelligent decision-making for network management. The review article also addresses the major research challenges of network management using ML and DL techniques. The research challenges are identified as the scarcity of network data, interpretability of ML models, computational complexity, real-time requirements, and security risks. Finally, future directions for scalable, explainable, and fully autonomous AI-driven network management systems are discussed.

Keywords: 5G/6G Networks, Network Automation, Traffic Prediction, Anomaly Detection, Intrusion Detection Systems, Software-Defined Networking (SDN), Network Function Virtualization (NFV).

DOI: https://doi.org/10.36548/jismac.2026.1.004
Received: 21.01.2026, received in revised form: 18.02.2026, accepted: 05.03.2026, published: 16.03.2026

1. Introduction

With the rapid growth of digital services, cloud computing, Internet of Things (IoT) devices, and 5G communications, modern networks have become more complex than ever before. Traditional methods for managing networks use a lot of manual configuration and rule-based systems and are not adequate to support the size, dynamic nature, and performance of modern infrastructures. Networks continue to grow and produce an enormous amount of traffic data; therefore, intelligent solutions that can automate network management are necessary to maintain reliability, security, and operational efficiency. AI (Artificial Intelligence), notably via ML (Machine Learning) and DL (Deep Learning), is transforming network management in modern networks. Network management based on AI uses data collected from routers, switches, servers and end-user devices to find patterns, predict failures, detect anomalies, and optimize resource allocation in real time. Both ML and DL can learn from historical data, adapt to dynamic network conditions, and continually enhance performance without requiring any reprogramming. traffic classification, congestion control, intrusion detection, and predictive maintenance are applications of machine learning techniques, like supervised learning, unsupervised learning, or reinforcement learning, combining with deep learning models, like convolutional neural network (CNN) and recurrent neural network (RNN), which offer more advanced features like complex pattern recognition, time series prediction, and automated fault diagnosis. machine learning techniques offer more network visibility, downtime reduction, and proactive decision-making. This review article attempts to offer a comprehensive discussion on machine learning and deep learning techniques that have been applied for the management of computer networks, along with various models, learning paradigms, application areas, and future directions.

2. Related Work

Vijay et al. (2023) proposed that AI is the development of techniques and technologies capable of acquiring knowledge and making decisions or predictions based on that knowledge. They introduced a novel approach to transforming network management by utilizing both AI-based Intrusion Detection Systems (IDS) and the BAT optimization strategy in conjunction with Deep Convolutional Neural Networks (DCNN). By leveraging the strengths of both deep learning and BAT, the aim is to enhance the performance of IDS within the context of network management through increased efficiency. This review supports the current studies in the area

of network security and improved network management systems [1]. Alaskar et al. (2021) reviewed that the rapid growth of Machine Learning and Deep Learning has led to many powerful applications across numerous disciplines, including image recognition, speech recognition, natural language processing, and has expanded into the world of healthcare. In this paper, they summarize all known techniques associated with Machine Learning and Deep learning, discussing the advantages and disadvantages of each, as well as recommendations for future use [2]. Javed et al. (2023) reviewed the two main categories of IoT that require security for user authentication, access control, and confidentiality of information: IoMT (Internet of Medical Things) and IoV (Internet of Vehicles) devices, which provide real-time tracking of healthcare and traffic to potentially save lives. Security breach incidents are on the rise as these devices become more widespread, creating a need for implementing an IPS (Intrusion Prevention System) in these technologies. This article also identifies challenging areas of IoT security, offers direction for future research in IoT, and provides possibilities for improving IoT device security. [3].

Sharifani et al. (2023) reviewed that the increase in the number of IoT devices has resulted in an increased likelihood of security breaches and attacks, creating a need for Intrusion Prevention Systems (IPS) within the ecosystem. Thus, the application of machine learning and deep learning methods will aid in establishing monitoring and protection mechanisms for the security of both IoMT and IoV devices. This article will analyze the current trends relating to security in our respective fields [4]. Janiesch et al. (2021) reviewed that AI-based decisions will have a high value in the present rapidly transitioning and extremely competitive environment, which has surged interest in the use of industrial machine learning (ML) technology. The demand for analytical experts exceeds the current capacity of this workforce. Solutions to this problem could include developing easy-to-use ML frameworks so that ML software can be used by individuals who are not experts in computer programming techniques. AutoML is a means to address this issue of expertise by providing users with a fully automated, off-the-shelf solution for selecting models and optimum hyperparameter settings. This article highlights the issues in human machine interaction and AI subscriptions [5]. Ahmad et al. (2021) conducted a study in which we will first explain what intrusion detection systems (IDS) are, and then create a classification of them based on the most popular machine learning (ML) and deep learning (DL) techniques used to create network-based IDS (NIDS). We will conduct an extensive review of all current NIDS articles, highlighting both

the advantages and disadvantages of their recommended solutions. After that, we will provide examples of current trends and advances in ML and DL-based NIDS, including the types of methods they are using to evaluate their solutions, the evaluation metrics they are using, and the datasets they are using. We have also identified some of the challenges associated with each of the previously discussed methods and provided examples of opportunities for future research into improving ML and DL-based NIDS [6].

Yang et al. (2023) researched that telecommunication networks (TNs) have become the primary infrastructure for data communications in the world. Operations and maintenance (O&M) are critical for ensuring the availability, functionality, and/or efficiency of TN communications. While O&M for information technology (IT) systems, such as the cloud, has characteristics of artificial intelligence for IT operations (AIOps), O&M for TNs presents three different fundamental challenges: (1) network components are topologically dependent, (2) the software used in TNs is highly diverse and heterogeneous, and (3) the amount of failure data for TNs is limited. TelOps is the first O&M framework used for TNs that is enhanced in a systematic way by focusing on artificial intelligence, data, and empirical evidence [18].

Table 1. Summary of Existing AI-Based Network Management Techniques

Ref.	Network Environment	Technique/ Algorithm used	Dataset/Platforms	Limitations
Jawad et al. [14]	Multimedia & Smart TV Networks	NFV & SDN	Mininet	Limited scalability under high traffic demand; dependency on centralized SDN controllers may introduce latency and single-point failure issues.
Jiang et al. [16]	5G Networks	DT, SVM, kNN	iPerf3	High implementation complexity and significant computational overhead; real-time deployment challenges in large-scale networks.
Ramesh et al. [7]	5G Network Reliability	Network Management Automation Algorithm (NMAA)	Computer Network Traffic	Performance depends heavily on predefined policies; limited adaptability to dynamic network conditions.

Hadi et al. [8]	Wireless Sensor Networks (WSNs)	Q-learning Algorithm	Bassam Kasasbeh	Resource-constrained sensor nodes restrict model execution; increased processing overhead affects energy efficiency.
Sattar et al. [9]	Water network management	Feed-Forward Artificial Neural Network	PRTools	Requires high-quality training data; limited robustness against noisy or incomplete real-world data.
Salman et al. [10]	Data Center Networks	RL	Mininet	Training complexity increases with topology size; lack of explainability in automated configuration decisions.
Bega et al. [13]	Cognitive Network Management	Deep Neural Network	Data analytics tool (SQL, Power BI)	High computational cost and scalability concerns; dependency on large datasets for effective learning.

3. Research Gaps

Although artificial intelligence has improved network management, several important research gaps still exist. Many current studies are tested only using simulated or publicly available datasets instead of real operational networks, which makes it difficult to apply these solutions in practical environments. Another major issue is the limited availability of high-quality network data due to privacy and security restrictions, which affects the accuracy and reliability of AI models. In addition, some of the machine learning and deep learning techniques demand high computational resources, which are also energy-intensive, making real-time execution difficult. Moreover, most AI systems are black boxes, meaning that network administrators are unable to trust the decisions made by these systems. Integrating AI systems with legacy network infrastructure has also been complex, mainly due to compatibility and standardization issues. Additionally, AI systems are at risk of various cyberattacks, such as adversarial attacks and data poisoning attacks. Furthermore, no evaluation criterion has been established to compare different AI systems, and most AI systems are not scalable enough to be used in environments like cloud and 5G/6G networks. Hence, the concept of autonomous

management of the network is still evolving, indicating the need for simple, trustworthy, and scalable AI systems for future intelligent networks.

4. AI Models Used in Network Management

AI enhances the intelligent decision-making capabilities of systems, allowing them to identify patterns, draw conclusions, and adapt continuously without requiring user involvement. The primary benefit of AI techniques in network management is to increase the level of automation, scalability, and efficiency provided by managing large quantities of data that can assist in performing activities such as predicting network usage patterns, identifying faults, allocating network resources, and monitoring security [15]. Within AI, one of the main subdivisions, Machine Learning (ML), is the most widely used method for managing a network. There are three primary types of ML: 1) Supervised Learning, which uses labelled data sets to complete classification or detection tasks; 2) Unsupervised Learning, which uses unlabelled data sets to discover new, hidden opportunities or patterns within data not previously identified; 3) Reinforcement Learning, which makes decisions based on previously learned information that will generate rewards.

An advanced area of machine learning, deep learning (DL), presents data to a multi-layered neural network and automatically advances through the extraction of complex features from the high dimensionality of the datasets available in the EMR. Architectures such as convolutional neural networks (CNNs) are well-suited for analyzing spatial patterns of traffic, recurrent neural networks (RNNs) and long short-term memory (LSTM) networks are well-suited for predicting traffic based on time series data, and graph neural networks (GNNs) are increasingly being used to model the networks' topologies and relationships between the nodes [16]. These technologies can be used in combination to create intelligent, adaptive, and autonomous network management systems.

The process of using machine learning and deep learning in network management involves a structured process with several stages (As shown in Table 2):

Table 2. Structured Workflow of Machine Learning–Based Network Management

Stage	Process	Description
1	Data Collection	Network monitoring systems gather data from routers, switches, base stations, and tools such as NetFlow, SNMP, and packet capture utilities. The collected data includes packet counts, flow duration, link utilization, latency, and protocol types.
2	Data Preprocessing	Raw network data is cleaned and converted into a structured format suitable for machine learning algorithms through normalization and transformation into feature vectors.
3	Feature Engineering	Relevant network features such as average packet size, flow duration, burst rate, and connection frequency are extracted to improve model performance.
4	Model Training	Machine learning models (e.g., SVM, Random Forest, k-NN) and deep learning models (e.g., CNN, LSTM) are trained to classify and analyze network traffic patterns.
5	Model Deployment	The trained models are integrated into network monitoring systems to analyze traffic and generate predictions in real time.
6	Decision and Automation	AI predictions enable automated network management tasks such as dynamic routing, bandwidth allocation, intrusion detection, and predictive maintenance.
7	Continuous Learning	Feedback from network performance is used to retrain and update models, allowing the system to adapt to evolving network conditions.

5. Machine Learning Applications in Network Operations

There are several advantages to using machine learning techniques in intelligent network management. For example, supervised learning algorithms such as support vector machines, decision trees, and random forests are used to classify network traffic and identify malicious activities in a network environment. These algorithms learn from labeled datasets that include normal and abnormal network behaviors and can effectively identify intrusion patterns and network anomalies [6]. Unsupervised learning algorithms such as clustering are used to identify unknown network anomalies and unseen network patterns. These algorithms group network flows based on statistical similarities and can identify abnormal behaviors that may indicate network faults, security issues, and performance degradation. In particular, reinforcement learning techniques have been used to solve various dynamic network optimization problems. For example, the use of Q-learning-based algorithms enables network

controllers to learn the best routing strategies by interacting with the network environment and receiving feedback in the form of reward signals. This enables adaptive bandwidth allocation, congestion handling, and intelligent resource management in large-scale networks [8], [11]. Overall, the use of machine learning techniques can greatly benefit network operation efficiency and reliability in terms of predictive analysis, fault detection, and resource optimization. In particular, as network infrastructures evolve to support new paradigms such as SDN, cloud-native networking, and 5G/6G communication systems, machine learning will play a critical role in assisting network operation in an autonomous and intelligent manner.

The table 3 below illustrates the suitability of different machine learning techniques for various network management tasks.

Table 3. Applicability of Machine Learning Techniques for Network Management Tasks

Machine Learning Technique	Traffic Classification	Traffic Prediction	Anomaly Detection	Intrusion Detection	Fault Detection	Routing / Resource Optimization
Support Vector Machine (SVM)	✓	✗	✓	✓	✓	✗
Decision Tree (DT)	✓	✗	✓	✓	✓	✗
Random Forest (RF)	✓	✓	✓	✓	✓	✗
k-Nearest Neighbor (kNN)	✓	✗	✓	✓	✗	✗
K-Means Clustering	✗	✗	✓	✓	✓	✗
Q-Learning (RL)	✗	✗	✗	✗	✗	✓

6. Deep Learning Architectures for Intelligent Networks

Deep Learning (DL) is now an integral part of AI-based network management due to its ability to automatically learn complex patterns from massive amounts of data in network

environments. Large-scale networks produce enormous amounts of data, including traffic flow, routing, user information, and network performance data from various sources such as routers, switches, and base stations Deep Learning techniques are used to analyze this data for intelligent network management functions such as traffic prediction, anomaly detection, fault diagnosis. Deep Learning is more powerful than traditional machine learning in terms of handling complex data from complex networks such as cloud computing environments, data centers, and 5G networks [6], [16]. Various DL architectures are used for various problems depending on the data type, such as spatial traffic data, temporal traffic data, or topology data.

The commonly used deep learning architectures in intelligent network management are summarized in Table 4.

Table 4. Deep Learning Architectures for Intelligent Network Management

Deep Learning Architecture	Key Characteristics	Networking Application	Advantages	Limitations	References
Deep Neural Networks (DNN)	Multi-layer neural networks capable of learning complex nonlinear relationships from high-dimensional datasets.	Network traffic classification, QoS prediction, performance monitoring.	High accuracy for complex classification tasks and ability to process large datasets.	Requires large training datasets and high computational resources.	[6], [13]
Convolutional Neural Networks (CNN)	Uses convolution filters to capture spatial patterns in structured data such as packet flows or traffic matrices.	Intrusion detection, traffic classification, anomaly detection in network traffic.	Effective for extracting spatial traffic features and detecting abnormal patterns.	Requires preprocessing to convert traffic data into structured feature matrices.	[1], [6], [13]

Recurrent Neural Networks (RNN)	Designed to process sequential or time-series data by maintaining internal memory of previous inputs.	Network traffic forecasting, workload prediction, and congestion detection.	Suitable for modeling temporal dependencies in network traffic flows.	Training instability and vanishing gradient problems in long sequences.	[6], [16]
Long Short-Term Memory (LSTM)	Improved RNN architecture with memory gates to capture long-term temporal dependencies.	Traffic load prediction, anomaly detection, predictive network maintenance.	High accuracy in time-series traffic forecasting and network performance analysis.	Computationally expensive and requires significant training time.	[6], [15]
Graph Neural Networks (GNN)	Models relationships between network nodes using graph structures representing network topology.	Routing optimization, topology-aware traffic prediction, and network failure analysis.	Captures structural dependencies between network devices and links.	Implementation complexity in large-scale networks.	[13], [16]
Generative Adversarial Networks (GAN)	Consists of a generator and discriminator network trained in an adversarial manner to produce realistic synthetic data.	Synthetic network traffic generation, intrusion detection dataset augmentation, anomaly simulation.	Helps overcome limited or imbalanced datasets by generating realistic training data.	Training instability and risk of generating low-quality samples.	[6], [3]

7. Emerging Trends In SDN, NFV And SON

The Software-Defined Networking (SDN) has impacted how new-age networks are deployed and managed. Unlike legacy networking models where control and data are highly coupled with networking devices, SDN separates control from data in the network architecture, allowing for centralized control through software-defined controllers. These attributes allow for greater network flexibility, programmability, and ease of operation. Additionally, recent advances in SDN are focused on integrating emerging technologies like artificial intelligence

and cloud computing to help automate networks more efficiently. Currently, organizations utilize SDN technology in their cloud data centers, enterprise networks, and 5G environments for dynamic traffic control, enhancing security monitoring and scalable network services.

Network Function Virtualization (NFV) refers to an approach to using virtualization technologies in place of physical, traditional network devices to deliver network-based functionality via software running on standardized computing platforms. With NFV, devices such as firewalls, load balancers and intrusion detection systems (IDS) are deployed as virtual machines or containers rather than on proprietary, specialized hardware products. Therefore, using NFV reduces the specialized hardware required for traditional network devices, thus lowering operational costs for network service providers (i.e. telecommunications companies) and giving them greater flexibility when delivering network services. As cloud computing and edge computing gain in popularity, the use of NFV for providing scalable and on-demand network services continues to grow rapidly. Additionally, the use of containerization and orchestration tools with NFV products has increased both the efficiency and speed of deployment of NFV solutions.

SON (Self-Organizing Networks) is designed to automate the management of complex wireless and cellular networks by allowing the network to automatically configure, optimize, and repair itself. With SON technology installed, there is less requirement for manual intervention from network management and improved overall performance of the network. SON is an important component of modern communication systems, such as 4G and 5G, as it helps manage various aspects of the network including power control, load balancing, and interference mitigation. SON systems can also apply artificial intelligence and machine-learning approaches to evaluate current network conditions in real-time and make intelligent changes to maintain the quality and reliability of service.

8. AI Applications in Network Operations (Routing, Traffic, Security, Fault Management)

Today, artificial intelligence is a revolutionary enabling factor in many of the operational functions of networks. By leveraging intelligence, adaptability, automation, and more as part of their management functions (e.g. routing, traffic control, security enforcement, fault management), many organizations are using AI for routing and traffic management as a

means of identifying and responding to potential network congestion before it occurs and optimizing routing paths for maximum network performance [13]. Using AI-based models that combine real-time and historical data from their networks to predict potential congestion events or route optimization opportunities and dynamically allocate available bandwidth accordingly, organizations are increasing their overall capacity to efficiently operate their networks while delivering superior QoS. AI machine learning and deep learning models are effective for traffic classification and forecasting which enables organizations to be proactive in responding to changing traffic patterns as opposed to responding to traffic using traditional static policies [14]. AI is also helping organizations to build intelligent intrusion detection and malware mitigation systems through behavior analysis and anomaly detection, enhancing traditional security measures that would fail to detect these types of threats by using static signature-based approaches. AI-enhanced security capabilities allow organizations to gain insight, identify, and respond to previously unknown and evolving types of threats.

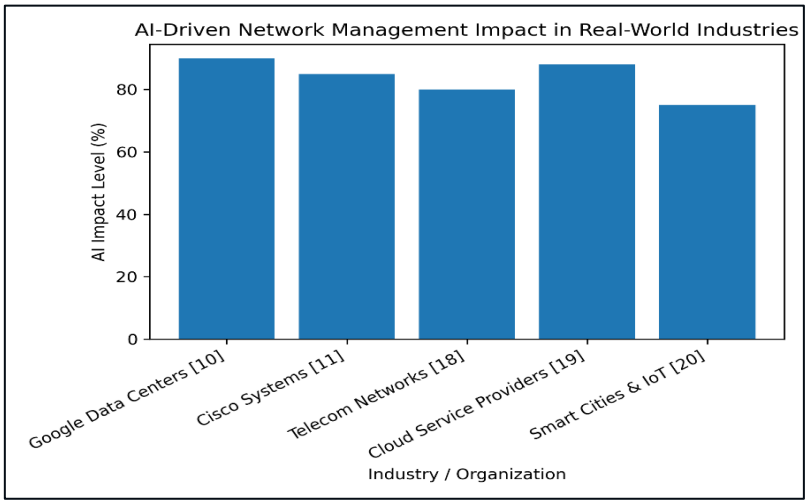

Figure 1. AI-Driven Network Management Impact in Real-World Industries

Figure 1 illustrates the impact level of AI-driven network management across real-world industries, expressed as a percentage. It indicates that Google Data Centers have the maximum AI impact, which is approximately 90%. This is because AI is used extensively in data centers for traffic optimization, energy efficiency, and predictive fault management. Similarly, Cloud Service Providers have the second-highest AI impact, which is approximately 88%. This indicates that AI has a critical role to play in managing cloud infrastructures. Furthermore, Cisco Systems have a high AI Impact, which is approximately 85%. This indicates that AI has widespread adoption in the industry for intelligent routing, network

automation, and security analytics. Similarly, Telecom Networks have a moderate AI Impact, which is approximately 80%. This indicates that AI has moderate adoption in the industry for traffic forecasting, optimization, and proactive fault detection. Moreover, Smart Cities and IoT have the lowest AI Impact, which is approximately 75%. This indicates that AI has the lowest adoption in the industry. Additionally, the graph indicates that AI has a significant and increasing impact on various industries. For instance, AI has the maximum adoption in data centers and cloud-based industries. Table 5 illustrates the adoption of AI/ML techniques in modern network management: industrial case studies.

Table 5. Adoption of AI/ML Techniques in Modern Network Management: Industrial Case Studies

Refs	Industry / Company	AI/ML Application	Key Benefits & Use Case	Issues	AI-Based Solutions	Performance evaluation (Accuracy)
[10]	Google Data Centers	Deep learning–based traffic and resource optimization	Reduced latency, improved throughput, lower energy consumption	Traffic congestion, inefficient resource utilization	Deep reinforcement learning for adaptive traffic routing and load balancing	RL - 0.95%
[16]	Telecom Operators (5G: SK Telecom, AT&T, Verizon)	AI-driven 5G network slicing and traffic prediction	Dynamic bandwidth allocation, improved QoS/QoE, SLA compliance	Highly dynamic traffic, spectrum scarcity	ML/DL-based traffic forecasting and self-organizing networks (SON)	kNN - 96.3%
[11]	Enterprise Networks (Cisco DNA Center)	AI automation & intent-based networking (IBN)	Automated configuration, monitoring, and policy enforcement	Manual errors, slow fault diagnosis	ML-based telemetry analysis, anomaly detection, closed-loop automation	LSTM - 97.3%

[18]	Telecom Vendors (Nokia)	Cognitive network performance optimization	Real-time anomaly prediction and performance enhancement	Service degradation, delayed fault resolution	Cognitive AI engines for proactive optimization and healing	CNN - 94.5%
[12]	Enterprise Cybersecurity	AI-based intrusion and anomaly detection	Real-time detection of cyber threats and zero-day attacks	Evolving attack patterns, high false positives	ML/DL-driven behavioral analysis and automated mitigation	LSTM - 95.8%
[6]	Telecom Infrastructure (General)	Predictive maintenance and self-optimizing networks	Reduced downtime, proactive maintenance	Unexpected hardware failures	ML-based failure prediction and self-healing mechanisms	CNN - 92.8%

Table 6. Comparison of Classification Accuracy and Network Performance Metrics in Existing research

Refs.	**Evaluation Metrics**	**Classifiers**	**Metrics**
Jiang et al. [16]	Classification Accuracy	DT, SVM, kNN	95.4%, 95.8%, and 96.3%,
Ramesh et al. [7]	Accuracy	Remote, Global, Urban, and Local Network Administration Models	91.82%, 95.25%, 96.59%, 95.07%
Hadi et al. [8]	Network Performance	Packet Delivery Ratio (PDR), Latency Reduction	96.38%, 24ms
Sattar et al. [9]	Regression-Based Model	R^2, RMSE, E_{sn}, D, PC time (s)	0.46, 0.17, 0.51, 0.85, 0.001 s

Arzo et al. [15]	Classification Accuracy	K-NN, Decision Tree, SVM, Naïve Bayes	98.798%, 99.504%, 94.746%, 88.262%
Zhao et al. [17]	Detection Accuracy	SVM	99.90%

9. Discussion

The analysis of the issues presented in this review article emphasizes the importance of artificial intelligence technology in modern network management. As communication networks expand and change over time, traditional rule-based network management techniques are not sufficient to deal with network issues such as traffic fluctuation, security risks, and resource management. Machine learning and deep learning techniques are being used to analyze network operation information and assist in network decision-making processes. The comparative analysis of the issues presented in Table 1 shows that different AI techniques are being applied to manage various network environments such as wireless sensor networks, 5G networks, data center networks, and cognitive network management. Supervised learning techniques such as support vector machines, decision trees, and random forests are being used to manage network operations such as traffic classification, intrusion detection, and fault diagnosis. Unsupervised learning techniques are being used to address network issues such as abnormal network behavior, and reinforcement learning techniques are being applied to manage network operations such as routing and resource management. The various deep learning architectures discussed in Table 4 improve network management by providing analysis for large-scale and high-dimensional data. These include convolutional neural networks and long short-term memory networks for anomaly detection and traffic prediction. Another is graph neural networks, which are applicable for relationship analysis between nodes in a network. Various industrial case studies on AI-based network management are discussed in Table 5. These include applications in cloud services, telecommunication networks, enterprise networks, and cybersecurity. These demonstrate improvements in terms of network efficiency, traffic optimization, and predictive fault detection. Various metrics for evaluating network performance are discussed in Table 6. These show high classification accuracy and improvements in various network performance metrics such as packet delivery ratio and latency.

The overall findings of this research suggest that artificial intelligence has the potential to significantly improve network management systems. However, more research needs to be done to address the challenges of scalability, availability, interpretability, and security to support the development of autonomous networks using AI.

10. Future Scope

The future of AI-based network management will focus on more intelligent, transparent, and fully autonomous systems that can accommodate the increasing complexities of future network generations. Another research direction in this area will be the development of more transparent and trustworthy AI models that can improve the effectiveness of network management. In the future, network generations will include 6G and beyond. In this regard, AI-native network architectures will play a vital role in providing ultra-low latency communication, massive connectivity, and efficient spectrum and resource management. Another promising research direction in AI-based network management will be focused on the integration of AI with digital twin technology. In the future, privacy-preserving techniques such as federated and distributed learning will also play a more critical role in network management. Network generations will use collaborative learning techniques without compromising user privacy. In the future, network management will also require the development of lightweight and energy-efficient AI models to accommodate the complexities of IoT and edge network environments. Future network generations will also utilize zero-touch network management frameworks that can provide self-configuration, self-healing, and self-optimization. Furthermore, strong and trustworthy AI models, as well as cross-layer optimization techniques and adherence to industry standards, are essential for the successful deployment of AI-driven network management solutions at scale.

11. Conclusion

This review looked at how AI is changing how networks are managed; using traditional methods to create Intelligent, Adaptive, and Autonomous Networks. We examined various forms of machine learning (ML), deep learning (DL), and reinforcement learning (RL) to show that data-driven models are being used effectively within the core functions of a network (e.g., optimizing traffic, routing, enforcing security, managing faults). ML methods can be used to classify, predict, and detect anomalies, while DL allows for complex spatial, temporal, and

topological patterns to be extracted from very large-scale data sets. Finally, RL extends the ability to make autonomous decisions in dynamic, time-varying networked environments. The emphasis placed on Artificial Intelligence-enabled network management solutions will be increasingly important in new networking paradigms such as Software Defined Networking, Network Function Virtualization, the Internet of Things, and 5G and beyond due to the need for highly scalable, low-latency, and reliable implementations. In addition to providing support for scalable, low latency, and reliable implementations, there are several notable challenges that must be addressed before there can be widespread adoption of AI-based networking solutions; these include data availability, model interpretability, deployment constraints associated with real-time processing of network events, and security and privacy. If these challenges are not mitigated, practical implementation of Artificial Intelligence-enabled solutions cannot occur. Overall, the continued development of new networking solutions enabled by Artificial Intelligence is a very promising direction for the creation of self-optimizing, self-healing, and zero-touch networks, and future research will play an important role in shaping future communication infrastructures.

References

[1] Vijay, G. S., Meenakshi Sharma, and Roma Khanna. "Revolutionizing Network Management with an AI-Driven Intrusion Detection System." Multidisciplinary Science Journal 5 (2023): 2023ss0313.

[2] Alaskar, Hind, and TanzilaSaba Saba. "Machine Learning and Deep Learning: A Comparative Review." Proceedings of Integrated Intelligence Enable Networks and Computing: IIENC 2020 (2021): 143-150.

[3] Javed, Abqa, Muhammad Awais, Muhammad Shoaib, Khaldoon S. Khurshid, and Mahmoud Othman. "Machine Learning and Deep Learning Approaches in IoT." PeerJ Computer Science 9 (2023): e1204.

[4] Sharifani, Koosha, and Mahyar Amini. "Machine Learning and Deep Learning: A Review of Methods and Applications." World Information Technology and Engineering Journal 10, no. 07 (2023): 3897-3904.

[5] Janiesch, Christian, Patrick Zschech, and Kai Heinrich. "Machine Learning and Deep Learning: C. Janiesch et al." Electronic markets 31, no. 3 (2021): 685-695.

[6] Ahmad, Zeeshan, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, and Farhan Ahmad. "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches." Transactions on Emerging Telecommunications Technologies 32, no. 1 (2021): e4150.

[7] Ramesh, G., J. Logeshwaran, and Avvaru Praveen Kumar. "The Smart Network Management Automation Algorithm for Administration of Reliable 5G communication Networks." Wireless Communications and Mobile Computing 2023, no. 1 (2023): 7626803.

[8] Hadi, AL-Shukrawi Ali Abbas, Aeizaal Azman Bin Abdul Wahab, Firdaus Mohamad Hamzah, and B. S. Veena. "AI-Driven Energy Management Techniques for Enhancing Network Longevity in Wireless Sensor Networks." Journal of Robotics and Control (JRC) 6, no. 1 (2025): 246-261.

[9] Sattar, Ahmed MA, Ömer Faruk Ertuğrul, Bahram Gharabaghi, Edward A. McBean, and Jiuwen Cao. "Extreme Learning Machine Model for Water Network Management." Neural Computing and Applications 31, no. 1 (2019): 157-169.

[10] Salman, Saim, Christopher Streiffer, Huan Chen, Theophilus Benson, and Asim Kadav. "DeepConf: Automating Data Center Network Topologies Management with Machine Learning." In Proceedings of the 2018 Workshop on Network Meets AI & ML,2018, 8-14.

[11] Manda, Jeevan Kumar. "AI And Machine Learning in Network Automation: Harnessing AI and Machine Learning Technologies to Automate Network Management Tasks and Enhance Operational Efficiency in Telecom, Based on Your Proficiency in AI-Driven Automation Initiatives." Educational Research (IJMCER) 1, no. 4 (2019): 48-58.

[12] Antwi, Isaac Kwame, Eric Akwei, Olanrewaju Ogundojutimi, and Nicholas Donkor. "AI-Driven Infrastructure Protection Framework for Resilient Enterprise Networks." International Journal of Innovative Science and Research Technology 10, no. 5 (2025): 4566-4578.

[13] Bega, Dario, Marco Gramaglia, Marco Fiore, Albert Banchs, and Xavier Costa-Perez. "DeepCog: Cognitive Network Management in Sliced 5G networks with Deep Learning." In IEEE INFOCOM 2019-IEEE conference on computer communications, IEEE, 2019, 280-288.

[14] Jawad, Nawar, Mukhald Salih, Kareem Ali, Benjamin Meunier, Yue Zhang, Xun Zhang, Rudolf Zetik et al. "Smart Television Services Using NFV/SDN Network Management." IEEE Transactions on Broadcasting 65, no. 2 (2019): 404-413.

[15] Arzo, Sisay Tadesse, Zeinab Akhavan, Mona Esmaeili, Michael Devetsikiotis, and Fabrizio Granelli. "Multi-Agent-Based Traffic Prediction and Traffic Classification for Autonomic Network Management Systems for Future Networks." Future Internet 14, no. 8 (2022): 230.

[16] Jiang, Wei, Mathias Strufe, and Hans D. Schotten. "Intelligent Network Management for 5G Systems: The SELFNET Approach." In 2017 European conference on networks and communications (EuCNC), IEEE, 2017, 1-5.

[17] Zhao, Shuai, Mayanka Chandrashekar, Yugyung Lee, and Deep Medhi. "Real-Time Network Anomaly Detection System Using Machine Learning." In 2015 11th international conference on the design of reliable communication networks (drcn), IEEE, 2015, 267-270.

[18] Yang, Yuqian, Shusen Yang, Cong Zhao, and Zongben Xu. "TelOps: AI-Driven Operations and Maintenance for Telecommunication Networks." IEEE Communications Magazine 62, no. 4 (2023): 104-110.

[19] Swain, Smruti Rekha, Deepika Saxena, Jatinder Kumar, Ashutosh Kumar Singh, and Chung-Nan Lee. "An AI-Driven Intelligent Traffic Management Model for 6G Cloud Radio Access Networks." IEEE Wireless Communications Letters 12, no. 6 (2023): 1056-1060.

[20] Reis, Manuel JCS. "AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities." Electronics 14, no. 12 (2025): 2492.