International Journal of Emerging Research in Engineering, Science, and Management
Vol. 4, Issue 2, pp.23-31, Apr-Jun 2025.
www.ijeresm.com eISSN – 2583-4894

Integration of Artificial Intelligence in Network Technology: A Literature Review

[1]Gusnul Mahesa, [2]Ahmad Tajri, [3]Eflan Ananda Pujito, [4]Muhammad Rizal, [5]Dimas Arya Bagaskara, [6]Mohammad Givi Efgivia

[1,2,3,4,5,6]Department of Industrial Technology and Informatics, University of Muhammadiyah Prof. Dr. HAMKA, Jakarta, Indonesia.
[1]2203015031@uhamka.ac.id, [2]2203015100@uhamka.ac.id, [3]2203015099@uhamka.ac.id, [4]2203015036@uhamka.ac.id, [5]2203015139@uhamka.ac.id, [6]mgivi@uhamka.ac.id, [1]ORCID: 0009-0005-6136-9519

Abstract: Integrating Artificial Intelligence (AI) and network technology represents a transformative advancement in modern networks' protection, management, and optimisation. This literature review presents a comprehensive overview of current developments, existing challenges, and future directions for AI applications in computer networking. The primary aim is synthesising recent research to illustrate how AI-driven technologies reshape traditional network models and drive the shift toward more intelligent, autonomous, and resilient infrastructures, particularly in emerging 5G and forthcoming 6G networks. Network systems have evolved from simple analogue designs into complex digital ecosystems that support high-speed communication, intelligent devices, and data-intensive applications. However, this rapid growth has outpaced the capabilities of traditional rule-based network management approaches, highlighting the need for adaptive, real-time solutions. AI through machine learning (ML) and deep learning (DL) offers powerful data processing, pattern recognition, and autonomous decision-making capabilities, positioning it as a key enabler for managing growing complexity, enhancing security, and supporting autonomous operations. A systematic review was employed to ensure methodological rigour, focusing on peer-reviewed journal articles, leading conference papers, and expert analyses related to AI use in network security, administration, and optimisation. Thematic and comparative analyses were conducted to identify key trends, performance indicators, and innovative developments across various network layers, particularly emerging AI paradigms such as dynamic graph learning, federated learning, and explainable AI (XAI). The review finds that AI significantly improves network performance, including enhanced intrusion detection, advanced threat analysis, intelligent traffic routing, predictive maintenance, and autonomous resource allocation. Furthermore, AI is instrumental in enabling the full potential of 5G and future 6G technologies, supporting features like network slicing, ultra-low latency communication, and novel use cases such as real-time remote healthcare and immersive extended reality (XR) experiences. Despite these advancements, several research gaps remain. These include the lack of standardisation, challenges balancing model interpretability with accuracy, real-time explainability, developing lightweight AI models suited for constrained networking hardware, and concerns around privacy and ethical use. This review ultimately underscores the importance of continued interdisciplinary collaboration to ensure responsible, effective, and sustainable integration of AI into networking. As the digital landscape continues to grow, AI will be essential in driving the development of faster, more intelligent, and more secure network environments.

Keywords: Artificial Intelligence, Deep Learning, Machine Learning, Network Automation, Network Optimization, Smart Networks.

1 INTRODUCTION

The development of network technology has seen consistent advancements, transitioning from the early days of analogue communication to the sophisticated digital systems that underpin modern life. Initially designed mainly for voice transmission, networks have evolved to support the explosive growth of data traffic driven by the internet and various digital services. Each new generation of mobile networks, from 1G to 5G, has significantly improved data speeds and capabilities, making possible innovations like high-definition video streaming, online gaming, and the widespread use of Internet of Things (IoT) devices [1]. This ongoing pursuit of enhanced performance and functionality aims to accommodate the increasing number of connected devices and to enable the creation of advanced technologies, including smart cities. Rising expectations for greater bandwidth, lower latency, and more reliable connectivity have led to increasingly complex network infrastructures, where traditional management and optimisation methods are becoming less effective [2].

At the same time, Artificial Intelligence emerged as a cutting-edge technology with the potential to transform fields such as computer science, medicine, and engineering. Its ability to trawl through massive datasets of information, recognise complex patterns, and make intelligent decisions in milliseconds makes it an essential utility as a potential solution to problems inherent in contemporary network technology. Machine learning and deep learning, being integral parts of the broad area of artificial intelligence, have been subject to considerable interest in networking because of their ability to learn from network-related data and adapt to emerging situations without requiring explicit programming. Paradigms like supervised learning, unsupervised learning, and reinforcement learning (RL) enable the process of gleaning knowledge from historical data, detecting anomalies, and predicting future trends, thus improving the performance of networks beyond the capabilities of conventional rule-based systems [3].

The ability of AI to automate complex tasks, enhance security measures, and elevate the overall quality of network operations justifies the growing need for its integration. Integrating AI into networking technology significantly shifts from traditional rule-based management and static configurations. The advancement toward AI-driven intelligent networks enables dynamic adaptation to shifting conditions and evolving user demands. Breakthroughs in AI algorithms are being specifically developed to address distinct networking challenges, such as deep-learning-based routing optimisation and predictive models for regulating network traffic. Innovations like in-network machine learning further illustrate this evolution by allowing faster inference and real-time decision-making at the network edge, bringing computational intelligence closer to where data is generated [4]. Altogether, this convergence signals a move toward proactive and automated network management, enhancing efficiency, resilience, and responsiveness in today's ever-changing digital landscape.

Despite the significant promise of integrating artificial intelligence within networking technology, substantial limitations and challenges remain. One of the key areas of attention needed involves the standardisation of AI methods and assessment metrics across networks to improve interoperability and comparative evaluation of results. There also continues to be a need to eliminate the inherent trade-off between interpretability and accuracy of AI models implemented within networks, especially in critical areas such as security, where understanding the reasonableness of AI-derived decisions is paramount. The development of real-time explainability mechanisms for AI-driven networking platforms and addressing the privacy and security implications of using network traffic for training and inference of AI models are other key areas of interest in the future. There is also a need for networking-oriented AI solutions that take explicit advantage of the unique nature and constraints of networking deployments, such as developing lightweight AI models suitable for running on networking hardware with constrained resources. These shortcomings highlight the need for continued efforts towards obtaining a robust, consistent, and ethical integration of AI within networking technology.

Considering these challenges, there is an urgent need for an extensive literature review to synthesise the state-of-the-art advancements, determine main trends, and understand the potential advantages and limitations involved in integrating artificial intelligence with network technology. This paper aims to contribute significantly to academics, practitioners, and stakeholders interested in the emerging field of artificial intelligence in network technology by synthesising the most up-to-date evidence from research articles. The scope of this review includes the applications of artificial intelligence in different aspects of network technology, such as security, management, optimisation, and its convergence with next-generation networks like 5G and 6G. By assessing the current literature, the review aims to shed light on key innovations, ongoing challenges, and potential directions for future research in this evolving and increasingly relevant area.

2 Literature Survey

Artificial Intelligence is a multifaceted concept lacking a commonly agreed-upon definition. It is most frequently defined as systems that exhibit intelligent behaviour by assessing the environment and determining the actions they need to take to attain stated goals. It again defines AI as the simulation of human intelligence, including perception of the environment, goal setting, initiation of actions, and learning from experience. AI is also defined as the engineering discipline attempting to mimic human intellectual ability and capacity, and having uses spread from simple automation through variably complex machine learning. The definition of AI evolves as the progression of technology dictates. AI exists as narrow AI alone, or as systems created for specific tasks rather than broad human-like intelligence [5].

Network technology comprises the hardware elements, software, protocols, and services platform whereby the device connects, communicates, and exchanges information over distances and between platforms. Having traversed from the time of the circuit-switched phone networks through the advent of packet-switched data networks and the World Wide Web of the internet, the network technology has progressed a long way. Today's networks are advanced to support everything from basic file transfers to real-time video, smart city networks, and industrial automation, all due to the need for more bandwidth, smaller latencies, better scaling, and more security. Innovation of wireless standards (Wi-Fi, LTE, 5G), virtualisation technology (Software Defined Networking - SDN and Network Functions Virtualization - NFV), and the IoT device eruption have also increased the networks' demands. As these converged, the network platforms have shifted from static hardware-imposed settings towards dynamic software-imposed settings based on agility, automation, and responsiveness. All this increased complexity brought along extreme management and security concerns, where the quest began for smarter, data-driven responses such as Artificial Intelligence for improved drive and management of the networks [6].

3 Research Methodology

3.1. Inclusion and Exclusion Criteria

The literature selection for this review was guided by a systematic set of inclusion and exclusion criteria designed to ensure both rigour and relevance. The initial preference was for publications by reputable academic publishers, top-tier journals, and reputable conferences in computer science, networking, and artificial intelligence. The choice of source reliability was designed to ensure the quality and validity of the literature examined. Only investigations explicitly referenced integrating artificial intelligence or its subfields, including machine learning and deep learning, into networking technologies were considered.

The subject included security issues, management, optimisation, automation, and applications specific to individual generations of networks (e.g., 5G/6G). Investigations that treated AI and networking separately without explicit integration were excluded from this review. The literature is from credible academic sources, including conference proceedings, peer-reviewed journals, and other specialised databases in the computer sciences and related fields. The sources were carefully selected based on their strict editorial criteria, their applicability to the study's focus on artificial intelligence in network technology, and their ability to provide a varied but methodologically consistent basis for research.

3.2. Methods for Synthesizing

The collected literature was synthesised and analysed through a systematic, multi-stage methodology. Thematic analysis allowed the identification of common themes, trends, and results, and the categorisation of articles into subtopics such as AI-enhanced network security, management, and developments of 5G/6G technology. Comparative analysis was then used to examine the commonalities, differences, and inconsistencies between methodologies, uses, and results among multiple studies, thus deepening the subject area's understanding. The evidence obtained was recapitulated to identify advancements, challenges, and future directions according to each sub-topic to construct an integrative review. Quantitative findings were synthesised by extracting scientific facts, such as performance measures, experimental outcomes, and comparison studies, to support statements and demonstrate the concrete contribution of AI to network technology. New AI uses in networking, such as adaptive resource control or anomaly detection mechanisms, were reported to be structured to reveal novel strategies and promising breakthroughs. The review explicitly demonstrated research gaps and challenges by analysing the authors' conclusions and suggestions for future work. This process assisted in ensuring rigorous critical evaluation of the field's shortcomings, ranging from scalability issues with AI models to ethical concerns with automated network systems, thereby ascertaining actionable directions for future research.

4 Results and Discussion

4.1. AI in Network Security

4.1.1. AI for Intrusion Detection Systems (IDS)

The application of AI, in machine learning and deep learning algorithms, has dramatically improved the effectiveness of Intrusion Detection Systems (IDS). By learning from past network traffic behaviour, AI-based IDS can detect anomalous behaviour that could be signs of cyberattacks more efficiently than conventional rule-based systems. For example, a study in the financial services industry claimed a 92% degree of precision in identifying possible threats with an AI system, which was significantly better than the 75% precision of their earlier rule-based system [7].

Table 1. Comparison between traditional and AI/ML security.

Metric	Traditional Security	AI/ML Security (FS)	AI/ML Security (HS)
Detection Accuracy	75%	92%	75%
False Positives	300	300	300
TRT	45 Minutes	45 Minutes	45 Minutes

FS – Financial Services, HS – Healthcare Services, TRT-Threat Response Time

Furthermore, AI-powered IDS can identify known threats and novel attacks, i.e., zero-day vulnerabilities, by identifying deviations from normal network behaviour. Different AI techniques have been explored in this direction, including deep transfer learning, which allows IDS to learn new and emerging attack patterns. Neural networks that vote on other AI model predictions have also shown improved detection rates and reduced false positive rates compared to conventional signature-based approaches. These advancements reflect AI's potential to devise stronger and more adaptive security solutions to counter the increasing sophistication of cyber threats.

4.1.2. AI in Threat Analysis and Intelligence

Artificial intelligence is central to threat analysis and intelligence operations since it regulates and aggregates vast quantities of security-related information drawn from various platforms. The information includes data obtained from security logs of networks, threat intelligence feeds, social media platforms, and even the dark web, thus enabling threat detection of growing hazards and improving the level of understanding regarding the methods used by opponents. Natural language processing (NLP) methods within AI platforms are used to infer crucial insights and patterns from text-based threat intelligence, such as the identification of new trends of malware or predicting likely attack methods. Academia-based studies have focused on applying AI to automate threat intelligence-related assessments, providing security teams with timely and actionable intelligence. AI is also applied to monitoring dark web entities to detect cybercrime-related activities and provide insights into the methods used by malicious groups [8].

The ability of AI to traverse and process such large sets of diverse information gives organisations a significant edge in proactive defence measures against cyberattacks.

4.1.3. AI for Malware Classification and Detection

AI algorithms, such as deep learning-based models comprising Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are applied more in malware classification and detection. These AI models interpret the different features of malware, including code patterns, file structure, and runtime behaviour, to facilitate the detection of known and unknown malicious software [9]. One of the most significant advantages of AI in this context is that it can overcome the limitations of traditional signature-based techniques or methods in the sense that it can detect polymorphic and metamorphic malware that keep modifying their code to evade detection. Current research continues to explore the use of AI in creating robust malware detection systems that can keep up with the ever-evolving threat landscape. Based on the inherent features and nature of software, AI offers a more dynamic and improved method of protection from advanced and mutating malware attacks, protecting against sophisticated and evolving malware threats.

4.1.4. AI in Security Automation and Response

Another key use of AI within the area of network security involves the automation of time-consuming and repetitive security tasks. AI is utilised to automate triaging security alarms, investigate incidents, and orchestrate response steps, resulting in enhanced security operations efficiency and a shorter time-to-respond to cyberattacks. Case studies have demonstrated tangible advantages, such as a reported decrease in the average response time from 45 minutes to 15 minutes within a finance services company after adopting a security solution based on AI. This was due to the automation of the most crucial tasks of the response process, such as isolating the infected device and blocking suspicious IP addresses. Studies also point towards the application of AI within Security Operations Centres (SOCs) for round-the-clock monitoring, quick remediation of vulnerabilities, and automated incident management. With the automation of these steps, AI allows the containment and mitigation of the threat within a short period and prevents any resultant damage while enabling the security teams to handle complex and tactical problems.

4.1.5. Research Gaps and Challenges in AI for Network Security

Despite the many benefits of AI for a network's security, many challenges remain for researchers to resolve. The most concerning among these is the lack of XAI for the transparency of the decision-making process of the AI-based security system. Security experts must understand the reason for a detection by an AI-based detection system and take the required measures. The root challenge of the problem of adversarial attack, wherein malicious intent attempts to evade detection by the AI model or a misclassification, and the development of robust and enduring security AI models against such attacks is another challenge. Ethical aspects of using AI-based cyber defence, such as autonomy and unintended impacts, also need serious consideration. There was a lack of a standardised procedure for applying XAI methodologies on Intrusion Detection Systems (IDS) and scaling XAI methodologies for large networks [10]. All these challenges and ethics must be solved for AI's broad application in network security.

4.2. AI in Network Management and Optimisation

4.2.1. AI for Network Automation

Artificial intelligence, machine learning, and deep learning methods are increasingly prevalent in automating diverse network management tasks. These tasks include configuration of the network, provisioning of services, fault detection, and monitoring of the network's performance, each of which traditionally required considerable manual effort. Real-world evidence of corporate deployments shows that AI-based automation of networks can bring about a 91% decrease in human configuration errors and a 67% reduction in Mean Time to Resolution (MTTR) for network issues [11]. Research on the development of self-configuration and self-optimisation of autonomous network management systems has investigated the reduction of human intervention and the increased adaptability of the networks. Artificial intelligence is also being integrated to improve the network's operations and implement predictive maintenance procedures, helping improve overall efficiency levels [12]. All this development towards AI-based automation leads to increasingly adaptive, reliable, and economically efficient networks.

4.2.2. AI in Intelligent Routing and Traffic Management

AI algorithms are successfully implemented for routing protocol optimisation and dynamic network traffic management according to prevailing conditions. The prime goals of this application include delay reduction, throughput enhancement, and quality of service (QoS) enhancement. Deep reinforcement learning (DRL) is implemented for routing decision enhancement and intelligent packet forwarding, enhancing network stability against time-varying traffic patterns and congestion. AI utilisation has also been proven by predicting network congestion and load balance forecasting between networks' channels, enhancing network utilisation, and reducing packet losses [13]. AI's intelligent routing and traffic management abilities enable the networks to function optimally under various conditions.

4.2.3. AI for Resource Optimisation and Allocation

AI is used for intelligent management and optimisation of bandwidth, processor capacity, and storage based on future demands and usage patterns. These achieve enhanced utilisation of the resources and potential cost savings. AI plays a fundamental role by facilitating the realisation of dynamic bandwidth management, where the bandwidth gets dynamically assigned based on variable traffic and application needs at runtime, such that maximum spectrum utilization is achieved, and congestion is avoided. Literature also acknowledges the use of AI for predictive resource management in cloud platforms and power utilization optimisation of the networking infrastructure [14]. AI ensures enhanced performance and effectiveness through the intelligent management of network resources.

4.2.4. AI for Predictive Maintenance

AI-driven algorithms are currently used to monitor the performance parameters of networks and predict possible hardware failures or drops in performance before they happen. The anticipatory method enables timely maintenance interventions while keeping the downtime of the networks at a very minimal level. Real-world evidence on industrial deployments shows that predictive AI maintenance can mitigate downtime by up to 90% by predicting failures ahead of time, thereby decreasing downtime by 35% for large deployments. Investigative work aims to use machine learning-based algorithms to predict the remaining useful life of the network devices and the behaviour of virtualised network functions (VNFs) in virtual networks [15]. The ability of artificial intelligence to predict and prevent network failures gives huge benefits in terms of reliability and cost.

4.2.5. Performance Metrics and Benefits of AI in Network Management

AI-based network management has led to significant performance improvement and various benefits. This varies from increased efficiency to better performance metrics such as reduced latency (e.g., 43% from 35 ms down to 20 ms) and increased throughput (e.g., 33% from 150 Mbps up to 200 Mbps), in addition to cost saving and improved utilisation of resources [16]. AI-based systems can analyse colossal network data in real-time, enabling faster detection and resolution of network issues. Literature underscores how AI can reduce the degree of manual intervention in managing networks and improve overall operational efficiency. The quantifiable improvement in the critical network performance metrics demonstrates the value in applying AI-based methodologies in network management.

4.3. AI in Next-Generation Networks (5G/6G)

4.3.1. The Role of AI in 5G Networks

Artificial intelligence is becoming increasingly crucial to 5G networks, which are integrated in various regions to optimise the efficiency and effectiveness of the networks. These regions comprise radio resource control, network and optimisation planning, traffic steering, and QoS management. Some specific applications of AI in 5G are network traffic prediction for more efficient allocation of resources and AI-based virtual network assistants for the rapid discovery and resolution of network performance issues [17]. Research indicates the pivotal role played by AI in dynamically optimising mobile communications in 5G networks for maximum performance and user satisfaction. The sophistication and saturation of 5G networks require intelligent management solutions capable of optimising for fluctuating loads and delivering peak performance, so AI is at the heart of unleashing the potential of 5G.

4.3.2. AI as a Core Enabler for 6G Networks

In the vision for 6G networks, AI is not merely an additional feature but a deeply integrated core component. AI is expected to drive network control, decision-making, and data processing across all network layers. It will be essential in achieving the ambitious performance goals of 6G, including terabit-per-second data speeds, sub-millisecond latency, and support for many connected devices. These capabilities enable next-generation applications such as holographic communications, immersive extended reality, and autonomous connected systems. Research identifies three key roles for AI in the evolution of 6G: as a means to enhance network functions (AI for RAN), as a foundation for applications and services that rely on mobile networks (AI with RAN), and as a technology embedded directly within the network itself (AI on RAN) [18]. Meeting the unprecedented demands of future hyper-connected environments makes AI an indispensable enabler at the core of 6G development.

4.3.3. AI for Network Slicing in 5G and 6G

Network slicing, a fundamental feature of 5G and the upcoming 6G networks, enables the creation of virtualised end-to-end slices tailored to various applications and services' unique needs. AI plays a crucial role in these slices' intelligent and dynamic management. Machine learning techniques are being applied to tasks such as classifying network traffic for proper slice allocation, forecasting the need for new slices or adjustments to existing ones based on traffic patterns and application demands, and overseeing the seamless handover of users or devices between slices to maintain the necessary QoS. Recent research highlights data- and AI-driven strategies for 6G network slicing, showcasing the potential for real-time, intelligent slicing solutions that can adapt to the diverse performance requirements of applications ranging from enhanced mobile broadband to ultra-reliable low-latency communications [19]. Through AI-driven network slicing, networks can achieve more efficient and adaptable resource management.

4.3.4. Novel Applications Enabled by AI in 6G

The fusion of AI with 6G networks holds the potential to unlock a wide range of transformative applications with significant societal impact. In healthcare, this integration is expected to enable real-time remote patient monitoring, personalised medical guidance, and AI-assisted robotic surgeries offering greater precision and safety [20]. The combination of ultra-high bandwidth, ultra-low latency, and AI capabilities will also revolutionise ultra-high-definition video streaming and cloud gaming, delivering experiences of unmatched quality with minimal interruptions. Additionally, the collaboration between AI and 6G is poised to accelerate the advancement of smart city infrastructures and immersive extended reality technologies, reshaping numerous industries and everyday life.

4.3.5. Security and Privacy Concerns in AI-Integrated 6G Networks

While having numerous benefits, the extensive integration of AI in 6G networks presents vast security and privacy challenges. The increased data collection, processing, and forwarding of enormous amounts of data across a broader set of devices and platforms in 6G networks raises the threat of unauthorised access, data leaks, and exploitation. Additionally, trained AI models are potential new attack surfaces, upon which malicious users could try to degrade their accuracy or steal sensitive data. Machine learning model training via data-driven learning also has privacy implications, such as information leakage and data misuse. Ensuring stable security and privacy measures is thus critical to balance technological advancement and network and user data integrity protection against 6G network deployment and development.

4.4. Novel Applications and Emerging Trends

4.4.1. AI for Dynamic Graph Learning in Networks

Dynamic graph learning, which combines graph theory with machine learning, is a powerful approach for modelling and analysing the evolving relationships within complex networks such as transportation, brain, social, and computer networks, where connections continuously change over time. Recent applications of dynamic graph learning in networking include forecasting future network links, identifying anomalies in traffic patterns that could signal security threats or performance problems, and tracking the spread of information or influence across a network [21]. Graph Neural Networks (GNNs), a specialised form of neural networks designed to process graph-structured data, have proven highly effective in solving challenging problems across various domains, including network behaviour prediction and analysis [22]. The ability to learn and anticipate changes in network structures positions dynamic graph teaching as a vital tool for creating more intelligent, flexible, and adaptive network systems.

4.4.2. AI in Complex Network Science

AI, particularly machine learning techniques, is increasingly used to address longstanding challenges in complex network science. Key areas of focus include advancing our understanding of how large-scale order emerges from interactions among individual network components, predicting the collective behaviour of complex networks based on their structure and node dynamics, and identifying critical nodes or tightly connected communities within networks. AI also offers promising approaches to exploring the intricate relationship between network topology and the dynamic processes occurring at the nodes and tackling problems related to the statistical mechanics of complex networks [23]. By introducing new computational capabilities and analytical methods, AI significantly contributes to deepening our understanding of the fundamental principles governing complex systems' structure and dynamics across both technological and social domains.

4.4.3. AI-Driven Optimisation in Diverse Network Environments

AI-based optimisation techniques are rapidly becoming a leading trend across various network environments, including telecommunications networks, data centre networks, and content delivery networks (CDNs). These methods aim to boost network performance, efficiency, and overall reliability. Specific applications include AI-driven algorithms that dynamically adjust routing protocols to optimise traffic flow, intelligently allocate resources like real-time bandwidth based on current demand, and predict hardware or software failures to enable proactive maintenance and avoid service disruptions. Using AI-based optimisation strategies, industry implementations, and research studies have demonstrated notable improvements in key performance metrics, such as reduced latency, increased throughput, and better resource utilisation. These results highlight AI’s effectiveness and versatility in meeting the diverse optimisation challenges of modern network infrastructures.

4.4.4. Emerging Trends in AI for Networking

Several emerging trends are actively shaping the future of AI in networking. One key development is the expanding use of GNNs across various networking applications. GNNs are particularly effective for network data analysis due to their ability to model the graph-based structure of networks, making them ideal for tasks such as traffic forecasting, anomaly detection, and network topology analysis. Another significant trend is the growing interest in federated learning. This distributed machine learning approach enables the collaborative training of AI models across multiple devices or servers without requiring the centralisation of personal data. This makes it especially valuable for network security and management, where data privacy is critical [24]. Additionally, XAI is gaining momentum in networking. As AI increasingly integrates into mission-critical network infrastructure, understanding and interpreting AI-driven decisions is vital for building trust and ensuring effective troubleshooting and monitoring.

5 Research Gaps and Challenges

5.1. Lack of Standardisation and Scalability of AI Techniques

A significant research gap in AI-integrated networks lies in the absence of standardised approaches and evaluation metrics for deploying AI techniques. This lack of standardisation hinders the establishment of industry best practices and complicates the comparison of the effectiveness of different AI methods. Additionally, many existing AI models and algorithms struggle with scalability when applied to the vast data volumes and rapid processing demands of modern large-scale networks. This issue is particularly pronounced in resource-intensive tasks such as anomaly detection and real-time traffic analysis, where current AI solutions can become overwhelmed. Addressing these challenges related to standards and scalability is essential for the successful and widespread adoption of AI across complex network environments.

5.2. Balancing Interpretability and Accuracy

One of the core challenges in applying AI to network applications is the trade-off between model interpretability and predictive or classification performance. Highly accurate models, such as deep neural networks, often function as "black boxes," making it difficult for users to understand the reasoning behind their decisions. Conversely, models that are more transparent and easier to interpret often sacrifice a degree of accuracy. This issue presents a significant research gap, particularly in security-critical applications where trust and validation depend on understanding the rationale behind an AI system's decisions. Further research is necessary to develop AI models and explanation techniques to balance these two essential aspects better, offering strong performance and clear, interpretable insights into their operations.

5.3. Real-time Explainability and Privacy Concerns

Providing real-time explanations for AI-driven network decisions remains a significant challenge, particularly when using computationally intensive post-hoc explanation methods. In many networking environments, rapid insights are critical, and introducing substantial latency for explanations would make real-world applications impractical. Additionally, because network data often includes sensitive user information, training and deploying AI models raise serious privacy concerns. Beyond exploring privacy-preserving methods like federated learning, which allows collaborative model training without centralising sensitive data, further research is needed to develop efficient real-time explanation tools for AI in networking. Addressing these challenges is essential for the responsible and effective integration of AI into network technologies.

5.4. Need for Network-Tailored AI and Lightweight Solutions

Many AI methods currently applied in networking were initially developed for other domains, such as natural language processing or image recognition. This highlights a significant research gap in designing AI models and algorithms tailored explicitly to network technologies' unique requirements and characteristics. Moreover, deploying sophisticated AI models on networking hardware like routers and switches is challenging due to their limited processing power and memory [25]. This situation underscores the need for efficient, lightweight AI solutions capable of performing effectively within such constraints. Future research should prioritise the development of AI models and techniques optimised explicitly for the tasks and environments encountered in networking.

5.5. Ethical Considerations and Trustworthiness of AI in Networks

Ethical and reliability concerns emerge as AI becomes increasingly integrated into network technologies. Key issues include determining accountability for network failures or security breaches caused by AI systems, ensuring AI's overall trustworthiness and reliability within critical network infrastructures, and addressing potential biases in AI models that could lead to unfair or discriminatory outcomes in network services [26]. To promote fairness, accountability, and transparency and mitigate broader societal impacts, it is essential to establish clear ethical standards and frameworks for developing and deploying AI in networking. Ensuring the ethical and responsible use of AI is vital for gaining public trust and supporting the sustainable growth of these technologies.

6 Conclusions

This article highlights the significant progress made in integrating AI into network technologies. AI is transforming various networking areas, including security, management, optimisation, and the evolution toward next-generation networks such as 5G and 6G. Its ability to learn from data, automate complex tasks, and make intelligent real-time decisions drives the development of more efficient, secure, and adaptable network infrastructures capable of meeting the ever-growing digital age demands. The review highlights that artificial intelligence enhances network security by reducing false positives, improving intrusion detection rates, delivering more precise threat analysis and malware classification, and enabling faster, more efficient security automation and response.

In network management and optimisation, AI is driving greater automation, smarter traffic and routing control, more efficient resource allocation, and the adoption of proactive maintenance strategies, all of which contribute to improved performance and reduced operational costs. Furthermore, AI is considered a core enabler for next-generation networks, particularly 6G, which is crucial in achieving unprecedented performance targets and supporting a wide range of novel applications. Despite these advancements, several research gaps and challenges remain. These include the need for standardisation of AI techniques and evaluation metrics, balancing the interpretability and accuracy of AI models, developing real-time explainability methods, addressing privacy concerns related to network data, creating network-tailored AI solutions, and ensuring AI's ethical and trustworthy deployment in critical network infrastructure. Emerging trends such as dynamic graph learning, federated learning, and explainable AI hold significant promise for future research and innovation in this field. Continued research and collaboration between experts in artificial intelligence and network technology are essential to overcome these challenges and fully realise AI's potential in shaping the future of network technology. This will ultimately lead to more intelligent, efficient, and secure networks that can support the ever-growing demands of a connected world.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ETHICS STATEMENT

This study did not involve human or animal subjects and, therefore, did not require ethical approval.

STATEMENT OF CONFLICT OF INTERESTS

The authors declare no conflicts of interest related to this study.

REFERENCES

[1] B. Kommadi, "AI and ML Applications: 5G and 6G," in *IntechOpen eBooks*, 2023. doi: 10.5772/intechopen.106698.

[2] M. Yang *et al.*, "From 5G to 6G: A survey on security, privacy, and standardisation pathways," *arXiv.org*, Oct. 04, 2024. https://arxiv.org/abs/2410.21986

[3] N. U. J. Umoga *et al.*, "Exploring the potential of AI-driven optimisation in enhancing network performance and efficiency," *Magna Scientia Advanced Research and Reviews*, vol. 10, no. 1, pp. 368–378, Feb. 2024, doi: 10.30574/msarr.2024.10.1.0028.

[4] C. Zheng *et al.*, "Planter: Rapid Prototyping of In-Network Machine Learning Inference," *ACM SIGCOMM Computer Communication Review*, vol. 54, no. 1, pp. 2–21, Jan. 2024, doi: 10.1145/3687230.3687232.

[5] H. Sheikh, C. Prins, and E. Schrijvers, "Artificial intelligence: definition and background," in *Research for policy*, 2023, pp. 15–41. doi: 10.1007/978-3-031-21448-6_2.

[6] A. Lutepo and K. Zhang, "A review of Artificial intelligence applications in contemporary computer network Technologies," *Communications and Network*, vol. 16, no. 03, pp. 90–107, Jan. 2024, doi: 10.4236/cn.2024.163005.

[7] Jérôme François et al., "Research challenges in coupling artificial intelligence and network management," *IETF Datatracker*. https://datatracker.ietf.org/doc/draft-irtf-nmrg-ai-challenges/

[8] N. S. Temara, "Harnessing the power of artificial intelligence to enhance next-generation cybersecurity," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 797–811, Aug. 2024, doi: 10.30574/wjarr.2024.23.2.2428.

[9] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," *Frontiers in Big Data*, vol. 7, Dec. 2024, doi: 10.3389/fdata.2024.1497535.

[10] V. Z. Mohale and I. C. Obagbuwa, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhance transparency and interpretability in cybersecurity," *Frontiers in Artificial Intelligence*, vol. 8, Jan. 2025, doi: 10.3389/frai.2025.1526221.

[11] Saikat Choudhury, "Intelligent Network Optimization: Revolutionizing Network Management Through AI and ML," *International Journal of Computer Engineering and Technology*, vol. 15, no. 6, pp. 2077-2085, 2024. doi: 10.34218/IJCET_15_06_178.

[12] R. and M. Ltd, "AI in Networks Market by Offering (Router & Switches, AI Networking Platform, Management Software, Software Defined Networking), Function (Optimization, Cybersecurity, Predictive Maintenance), Technology (Gen AI, ML, NLP) - Global Forecast to 2029," *Research and Markets Ltd 2025*. https://www.researchandmarkets.com/reports/5993893/ai-in-networks-market-offering-router-and?srsltid=AfmBOorj5WhdnUDwPQ_bqz2v89_oWqujzmP47sMlkpAh0WdQBle-bXyj

[13] H. K. Mistry, C. Mavani, A. Goswami, and R. Patel, "Artificial Intelligence for Networking," *Educational Administration: Theory and Practice*, vol. 30, no. 7, pp. 813-821, 2024. doi: 10.53555/kuey.v30i7.6854.

[14] M. El-Hajj, "Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions," *Network*, vol. 5, no. 1, p. 1, Jan. 2025, doi: 10.3390/network5010001.
[15] H. Ju, S. Jeong, S. Kim and B. Shim, "Transformer-Aided Parametric CSI Feedback for mmWave Massive MIMO Systems," *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, 2023, pp. 3596-3601, doi: 10.1109/ICC45041.2023.10279055.
[16] O. Ergun, "Comparing Traditional Network Management vs. AI-Enhanced Practices | Orhan Ergun," *Orhan Ergun*, Feb. 07, 2025. https://orhanergun.net/comparing-traditional-network-management-vs-ai-enhanced-practices
[17] Q. Cui *et al.*, "Overview of AI and communication for 6G network: fundamentals, challenges, and future research opportunities," *Science China Information Sciences*, vol. 68, no. 7, Apr. 2025, doi: 10.1007/s11432-024-4337-1.
[18] Lovén, Lauri, Miguel Bordallo López, Roberto Morabito, Jaakko Sauvola, and Sasu Tarkoma, 6G Flagship, "LLM in the 6G-Enabled Computing Continuum: a White Paper," *6G Flagship*, Feb. 03, 2025. https://www.6gflagship.com/llm-white-paper/
[19] R. Botez, D. Zinca, and V. Dobrota, "Redefining 6G Network slicing: AI-Driven solutions for future use cases," *Electronics*, vol. 14, no. 2, p. 368, Jan. 2025, doi: 10.3390/electronics14020368.
[20] R. Chataut, M. Nankya, and R. Akl, "6G Networks and the AI Revolution—Exploring technologies, applications, and emerging challenges," *Sensors*, vol. 24, no. 6, p. 1888, Mar. 2024, doi: 10.3390/s24061888.
[21] S. H. Fard, "Machine Learning on Dynamic Graphs: A Survey on Applications," *2023 IEEE Ninth Multimedia Big Data (BigMM)*, Laguna Hills, CA, USA, 2023, pp. 32-39, doi: 10.1109/BigMM59094.2023.00012.
[22] H. Li *et al.*, "GrAPH Neural Networks in Intelligent Transportation Systems: Advances, applications and trends," *arXiv.org*, Jan. 01, 2024. https://arxiv.org/abs/2401.00713
[23] J. Ding *et al.*, "Artificial intelligence for complex Network: Potential, Methodology and application," *arXiv.org*, Feb. 23, 2024. https://arxiv.org/abs/2402.16887
[24] K. Trichias *et al.*, "AI/ML as a Key Enabler of 6G Networks: Methodology, approach and AI-Mechanisms in SNS JU," *Zenodo*, Feb. 2025, doi: 10.5281/zenodo.14623109.
[25] Tahir Bashir, Najeeb Abbas Al-Sammarraie, "Revolutionizing Network Security with AI and Machine Learning Solutions," *International Journal of Computer Applications,* vol. 186, no. 86, pp. 975-8887, 2024. doi: 10.5120/ijca2024924217.
[26] S.-N. Vulpe, R. Rughiniș, D. Țurcanu, and D. Rosner, "AI and cybersecurity: a risk society perspective," *Frontiers in Computer Science*, vol. 6, Oct. 2024, doi: 10.3389/fcomp.2024.1462250.