GEN-Multidisciplinary Journal of Sustainable Development

GMJSD VOL 3 ISSUE 1 (2025) ISSN: 2960-3455

Available online at www.gmjsd.org

Journal homepage: https://gmjsd.org/journal/index.php/gmjsd/index

THE ROLE OF ARTIFICIAL INTELLIGENCE IN NETWORKING: A REVIEW

Oghenemarho Anthony **KARIEREN**[1]; Hassan Abisoye **OLUGBILE**[2]; Olisa Albert **OKWUOBI**[3]; Roqeeb Ayodeji **OLANIYI** [4]

[1]Center of Information and Communication Science Department, Ball State University, Indiana, United States.
[2]Department of Computing, East Tennessee State University, United States.
[3]Department of Electrical and Electronics Engineering, University of Ilorin, Ilorin, Nigeria.
[4]Product Support Department, D2L Limited, Canada.

ARTICLE INFORMATION

Article history

Received:
Revised:
Accepted:

***Keywords**:*
Artificial Intelligence,
Software Defined Networking,
Network Function Virtualization,
Machine Learning

ABSTRACT

The growing complexity of digital infrastructures, fuelled by the rise of Internet of Things (IoT) devices, cloud computing, and advanced communication systems, creates considerable challenges for managing networks. Traditional, manual approaches are no longer adequate to meet the evolving demands of modern networks. This paper explores how Artificial Intelligence (AI) is transforming network engineering, shifting from rule-based, manual systems to fully automated, AI-powered operations. Technologies like machine learning, deep learning, and reinforcement learning provide real-time analytics, traffic control, anomaly detection, and predictive insights, significantly boosting network performance, security, and reliability. Additionally, it delves into how this shift is altering the skill set required of network engineers, placing greater emphasis on expertise in AI, machine learning, and data analytics. The paper also examines how AI-driven frameworks, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), enhance network flexibility and scalability. Ultimately, it underscores the essential role of network engineers in integrating AI technologies to maintain the security, efficiency, and resilience of digital infrastructures, while highlighting the need for ongoing professional development to navigate the AI-driven landscape.

1. Introduction

Every generation has started a revolution in the communications ecosystem as the worldwide industry has moved to a new generation almost every decade. Advancements in information technology, mechanical technology, and electrical power technology drive the fourth industrial revolution, transforming and improving the digital economy sector (Shen et al., 2024). A crucial component of this revolution is artificial intelligence (AI). One of the biggest obstacles to explaining artificial intelligence (AI) to a lay audience is figuring out what "I"-intelligence is. The "artificial" element is somewhat simple, yet intelligence is a complicated concept. In general, artificial intelligence (AI) is the ability of a computational system to carry out operations that normally call for human intelligence. These activities cover a variety of cognitive processes, such as language comprehension, learning, reasoning, problem-solving, and perception. This concept places more emphasis on AI systems' capacity to imitate and reproduce these cognitive processes than it does on test scores (Bringsjord and Schimanski, 2003).

The spread of deep learning techniques is driving the third wave of prosperity in AI (Lecun et al., 2015). Among the many sectors in which AI has seen notable success are computer vision, natural language processing, multimedia production, medical applications, and human genetics (Ota et al., 2017; Young et al., 2018). The implementation of the next generation of communication networks suggests that AI allows a shift from reactive to proactive data-driven operations, hence improving network management, security, and performance (Challita et al., 2020). For instance, the telecom industry uses AI to maximise communication-network resources from the viewpoint of communications and network engineering, and it also recognises AI as a possible changing use for 5G and maybe 6G networks (Raihan and Evolution, 2023). In 6G networks, AI is anticipated to help the shift from networked devices to intelligent systems, boosting the quality of life and human cognition (Chen, Li, et al., 2019). 6G communications, which are projected to be more efficient, reliable, intelligent, scalable, and energy-efficient, are intended to solve the constraints natural in 5G communications (Lu and Zheng, 2020).

The evolution of the 6G network is steadily improving the existing communication infrastructure (Meena et al., 2022). 6G technology's deployment will enable the creation and tailoring of a complex toolbox (Dao, 2023). According to (Firouzi et al., 2022), the use of edge AI in a management system helps to enable the methodical administration of complicated integrations. Though the global spread and practical use of 5G technology are still in process, researchers have already turned their attention to the creation of the 6G networking framework (Chavhan and Assessments, 2022). AI-driven networking enhances several facets of network management, including real-time analytics, anomaly detection, and predictive insights. It increases the effectiveness of security protocols, protocol design, and routing (Chen, Challita, et al., 2019). Network engineers have to adapt to new technologies, handle cybersecurity issues, monitor and enhance computer systems, among other vital tasks.

2. The Evolving Role of Network Engineers in the AI Era

2.1 Importance of Network Engineers in the Evolving Technological Landscape

Profound developments in AI and automation are driving fast change in the digital infrastructure supporting modern economies, which is enduring (Wang and Siau, 2019). In this regard, network engineers have changed from traditional connectivity experts to vital builders of robust digital ecosystems in this dynamic climate (Rane et al., 2024). Their knowledge in the design, implementation, and maintenance of secure and scalable networks is crucial for the integration of cutting-edge technologies—including robotics, natural language processing, and machine learning—ensuring that sectors stay flexible in the face of ongoing technological disturbance.

Digitalisation and fast technological change have caused job displacement concomitantly with rising productivity, transforming the labour markets. (Lane and Saint-Martin, 2021) highlights that while AI could directly kill mundane tasks—the displacement effect. It also generates new job prospects needing creative talents; this is sometimes offset by a productivity or reinstatement effect. Network engineers are vital for preserving the agility and resilience of the digital infrastructure during these shifts. Their efforts help companies to benefit from enhanced connectivity and lower manufacturing costs, hence supporting both current and new services. This essential assistance not only helps to reduce the effects of automation but also helps to create a setting that supports the creation of fresh economic possibilities (Mithas et al., 2022).

As businesses grow more connected via digital platforms and cooperative economy models, the duties of network engineers also go beyond the upkeep of operational infrastructure. They are key players in the creation of next-generation technologies such as cloud computing, 5G, and edge computing, which together form the basis for developments in e-commerce, healthcare, manufacturing, and other industries (Moro-Visconti, 2024). Their efforts ensure that enhancements in network performance are directly reflected in higher security and production, hence reinforcing the more general economic structure. Support of policy projects meant to lower skill mismatches and attain labour market resilience in the digital age depends on the ability to include and use new technologies (Van Noordt et al., 2023).

Historical studies of technological revolutions show that, although the first effect of automation often leads to a drop in specific job categories, creation of new jobs (which is often later propelled by such revolutions) drives economic expansion and labour market change (Autor, 2015). Network engineers find themselves uniquely positioned at the crossroads of this process. By building infrastructures that enable the displacement and later reinvention of employment roles, they help robust AI systems integrate smoothly into the workforce. The translation of technological developments into socially fair results depends on this intermediary role, hence ensuring that the advantages of innovation are suitable for a broad spectrum of stakeholders, from individual workers to whole industries (Ernst et al., 2019).

The evolving technological landscape calls for a rethinking of the idea of employment in general, in which network engineers are recognised as vital boosters of economic and social stability as well as technical experts. As AI and digitalisation speed up, their role in the building and preservation of the digital framework becoming more and more crucial (Mossavar-Rahmani and Zohuri, 2024). Future studies should keep looking at the particular skill sets network engineers must have if investments in digital infrastructure are to support an equitable and sustainable future of work (Bukartaite and Hooper, 2023).

Network engineers have been at the foundation of digital communication systems, guaranteeing that data flows efficiently, securely, and reliably across complicated infrastructures. Historically, their primary duties have been the design, execution, and administration of networks linking computers, servers, and other devices (Mistry et al., 2024). Also, they have the responsibilities relating to the choice of appropriate hardware, the setup of network protocols, and the oversight of router, switch, and firewall installation. This is applicable to the planning of network architectures for local area networks (LANs), wide area networks (WANs), or the hybrid infrastructures necessary for company operations. All later programs, including early-stage automation systems and regular office communications, are built on these essential activities (Oladosu et al., 2021).

However, the general duties have grown in the context of the changing technology environments seen in the excerpts, a distinct basis stays anchored in these conventional functions. Often, network engineers are tasked with diagnosing connectivity problems, monitoring network performance, and making sure thorough cybersecurity policies are in place. Essentially, they do regular system maintenance and updates to guard against vulnerabilities since the underlying network is compromised; hence, automating AI applications might aggravate systematic risks. Particularly in light of emerging developments, such as the integration of AI and cloud technologies, conventional tasks like capacity planning, network segmentation, and traffic optimisation stay vital even if more dynamic and scalable solutions are required (Kibria et al., 2018).

Moreover, network engineers have to keep operational integrity and serve as the gateway to sophisticated technologies as digitalisation changes employment and business structures. Their work ensures the deliverance of continuous service and the sharing of real-time data by means of seamless integration of AI systems with current digital infrastructure. By keeping rigorous reliability and security criteria, network engineers help to further the strategic goals of companies by optimizing production and reducing the adverse effects of technology disturbances. Consequently, even as network management methods are changed to meet the demands of an AI-enhanced future, their ongoing evolution builds on the century-old disciplines of network design, troubleshooting, and maintenance (Huang, 2023).

2.2 Network Engineers' Roles in AI and Its Implications for Employment

Recent studies stressing both the emergent possibilities and displacement consequences resulting from digitalisation have underlined the transforming influence of AI on job markets. (Yang et al., 2017) emphasise how technology developments can erode traditional roles and generate new job possibilities. Models like the Lotka–Volterra, often known as predator-prey equations, are a pair of first-order, nonlinear differential equations. They are commonly used to simulate the dynamics of biological systems involving two species, one as predator and the other as prey. The equations show the dynamic interaction between AI as a "predator" and human jobs as "prey". This article emphasises the vital role network engineers play in supporting AI integration, guaranteeing durable digital infrastructures, and mediating the balance between automation-driven displacement and the generation of new, technology-centric roles (Strannegård et al., 2021).

The complicated narrative of the emerging technological landscape, as depicted in recent studies, is typified by the displacement of ordinary jobs by AI-driven automation, the acceleration of productivity, and the introduction of new types of employment (Khan et al., 2024). Much research has used ecological models to show this link, placing AI growth and job loss in a dynamic system of feedback loops and equilibrium. At the same time, talks on digitisation highlight the significant influence of technology developments on labour markets, therefore requiring the reduction of displacement consequences and the use of new technical possibilities. Network engineers are acknowledged in this setting as vital agents in charge of the design, deployment, and upkeep of the digital fabric supporting AI breakthroughs (Wang et al., 2015).

Various research show that AI affects jobs both ways. On one hand, its capacity to automate complex and mundane activities creates a displacement effect that endangers conventional work roles. On the other hand, the increasing incorporation of AI into sectors such as banking, and healthcare leads to increased efficiency, innovation, and economic growth (Puaschunder, 2019). This integration not only boosts output but also helps to create new job categories. Network engineers are leading this change. Their knowledge in the building and administration of strong, scalable, safe networks ensures the smooth running of AI applications across digital platforms. As AI technology develops and gets more integrated into daily operations, the essential role of network engineers

The studies also highlight how digitisation and automation are changing labour markets by adding new technological skills and removing outdated jobs (Koski and Husso, 2018). This bifurcation of the work market, which is marked by a drop in everyday middle-skill occupations and an increase in high-skill and non-routine roles, poses both obstacles and opportunities. Network engineers are vital in this dynamic environment for the preservation of the integrity of the digital ecosystem and for the development of efficiency and innovation. Their work contributes to the productivity effect by supporting the development of new economic models, including data-driven corporate strategies and collaborative platforms, boosting employment growth (Tariq et al., 2021). By bridging the gap between the operational needs of modern enterprises and advanced AI systems, network engineers are essential in offsetting the negative consequences of automation and supporting the shift to new kinds of skilled jobs.

According to (Zeng, 2020), the inclusion of AI into the fabric of our digital economy creates a contradiction of both disturbance and change. Though they also provide fresh possibilities that alter employment in the digital age, AI technologies could supplant conventional labour positions. This change is made possible by network engineers, who are in charge of building resilient, flexible digital infrastructures (Argyroudis et al., 2022). Their work not only enables the smooth rollout of AI systems in many different industries but also helps to mitigate the dangers of technological unemployment. Guiding our labour markets towards a more sustainable and dynamic future will depend on our ability to acknowledge and improve the knowledge of network engineers as policy debates and educational projects evolve to meet these issues.

2.3 New Skill Requirements for Network Engineers

As the digital world changes with the fast integration of AI into practically every area, network engineers are being forced to widen their conventional skill sets to incorporate advanced competencies such as machine learning, data analytics, and experience with AI tools (Verma et al., 2022). Historically, network engineers were primarily concerned with the design, implementation, and management of communication infrastructures, with the objective of assuring the security, performance, and connectivity of networks. The rise of AI-driven technology has, however, upset these conventional paradigms and called for a change in professional knowledge (Johnson et al., 2021).

Modern network infrastructure today uses automated systems and predictive analytics to enhance real-time performance. In this framework, a thorough knowledge of machine learning is essential. Network engineers are being forced to design and execute algorithms capable of analysing network traffic patterns, predicting possible problems, and autonomously changing settings to stop failures. This adjustment not only saves downtime but also enhances the overall efficacy and robustness of network operations (Karamchand, 2024).

(Ahmad et al., 2020) highlights the importance of sophisticated data analytics skills by the exponential expansion in data generated by connected devices. Network engineers today have to be skilled in the administration of big data, the extraction of relevant insights using statistical and computational techniques, and the use of these insights to guide Infrastructure as Code (IaC) choices. These features allow engineers to proactively spot abnormalities, maximise resource allocations, and carry out plans altering network conditions.

The integration of AI technologies into network management procedures also emphasises the need for engineers to be knowledgeable about developing AI platforms and frameworks even more (Yang et al., 2021). Whether it be the incorporation of AI into SDN or the use of NFV for scalable and programmable networks, knowledge in these fields dramatically enhances the ability to close the gap between legacy systems and modern, AI-enabled environments. These skills significantly improve the effectiveness of network operations and the security systems meant to protect against the rise of more complex cyber-attacks (Mishra et al., 2024).

Ultimately, the shift driven by AI is redefining the function of network engineers from conventional network maintenance to a more all-encompassing, data-driven, and automated approach to network management. By gaining knowledge in AI technologies, data analytics, and machine learning, network engineers are not only responding to the present technological needs but also defining themselves as important contributors to the innovation and resilience of digital ecosystems of the future.

3. AI in the World of Networking

3.1 How AI is Transforming Network Engineering

The fast development of AI, which has brought revolutionary powers exceeding conventional methods, is significantly reshaping the field of network engineering. One of the most important changes is the automation of network administration and optimisation (Mohamed et al., 2024). Network engineers of the past meticulously changed network settings, defined routing protocols, and tracked system performance via frequent reviews. Algorithms driven by AI can now dynamically control complex network designs in real-time. These intelligent systems can forecast possible congestion, automatically change bandwidth distribution, and optimise traffic flows in line with evolving needs. By allowing networks to self-configure and self-heal, machine learning methods have improved operational efficiency and lowered human error and delay (Shah and Patel, 2024). This shift not only simplifies everyday tasks but also lets network engineers focus on strategic innovation and long-term infrastructure planning.

Apart from its application in management and optimisation, AI is essential for the development of threat detection and network security. Traditional security solutions, which usually depend on predefined rules and manual updates, cannot keep up with the shifting attack vectors as cyber-attacks become more sophisticated (Attkan and Ranga, 2022). By means of real-time data analysis and anomaly detection, modern AI-driven security systems track significant amounts of network traffic and flag unusual patterns that might indicate an incursion or cyberattack. By constantly learning from previous data and new danger inputs, these systems can adjust their detection tactics and neutralise risks more quickly than traditional approaches. Consequently, AI not only increases the accuracy of threat detection but also streamlines incident response procedures, thereby creating a robust defence system that can change with the changing cybersecurity scene (Attkan and Ranga, 2022; Hu et al., 2021)

The integration of AI into NFV and SDN also reflects another notable development in network engineering. By divorcing network control from hardware, SDN and NFV are concepts that enable more flexible, programmable, and scalable networks (Ahmad and Habelamateen, 2023). By providing advanced capabilities for real-time monitoring, predictive analytics, and automated decision-making, AI improves these technologies. AI, for instance, can manage virtualised network functions in NFV settings to guarantee the best performance, efficiency, and scalability, while it can dynamically assign network resources depending on current traffic conditions inside SDN frameworks and improve routing decisions. By enabling companies to deploy new services and adjust to fluctuating demand quickly, this cooperation between AI and virtualised network technology helps to create an adaptable business environment in the digital age (Cunha et al., 2024).

AI has enabled a broad and multifarious change in network engineering. From automating mundane network management tasks and performance optimisation to improving security and pushing SDN and NFV breakthroughs, AI is not only redefining technical operations but also changing the actual function of network engineers. As they adapt to a dynamic environment in which AI tools are more and more integrated into conventional approaches, these experts are ideally suited to focus on strategic oversight and long-term infrastructure growth (Sharma and Nag, 2023). The creation of digital networks that are secure, efficient, and resilient depends on this development. These networks are necessary for the complete use of AI in modern industry and the reduction of the disruptive consequences of technological development.

3.2 AI's Influence on Network Engineering Jobs

3.2.1 AI-driven automation in network management and monitoring

AI-driven automation is helping to quickly change network administration and monitoring by allowing networks to handle dynamic operational issues and exceptional complexity. Traditionally, network administration has been dependent on manual setups and rule-based solutions, which are unable to satisfy the rising demands of IoT proliferation, cloud computing, and 5G technologies (Ahmed et al., 2023). In reaction to the exponential rise of global internet traffic, AI has emerged as a potent solution, capable of autonomously learning traffic patterns, predicting congestion, and dynamically adjusting network routing to optimise performance and reduce packet loss, mostly through Machine Learning (ML), Deep Learning (DL), and Reinforcement Learning (RL) (Boukerche et al., 2020).

Apart from improving performance, AI-driven technologies significantly improve network security. Using traditional intrusion detection systems (IDS) based on predetermined signatures, novel attacks such advanced persistent threats (APTs) and zero-day vulnerabilities are becoming more and more difficult to identify. By using real-time data and anomaly detection algorithms, which constantly adjust to evolving threat environments, AI systems can more efficiently detect and reduce harmful activities. This approach not only lowers the possibility of security flaws in complicated, heterogeneous network settings but also lessens downtime (Saurabh et al., 2025).

AI has also made a more thorough change of network infrastructure possible. Apart from delegating mundane chores, AI is also required for predictive maintenance, proactive disturbance detection, and fast reaction tactics, which together improve the operational efficiency and dependability of internet access networks, as detailed in the literature. This change includes the reorganisation of labour responsibilities, thereby requiring network engineers to include AI tools and approaches into traditional network management techniques (Khawar et al., 2024). Therefore, AI-driven automation is not only about enhancing technical performance; it is also about fostering an ecosystem in which networks may self-configure, self-heal, and continuously develop to meet new problems in a connected and automated society.

3.2.2 Emerging AI-based Networking Tools and Platforms

Accelerated AI progress has caused a new generation of networking tools and platforms to emerge, significantly changing the administration and security of networks. Modern connectivity's growing complexity is challenging conventional network management, which once depended on human settings and predefined, rule-based solutions. Intended to automatically monitor, manage, and secure network settings (Kibria et al., 2018). This is a reaction to the increase in internet traffic generated by IoT devices, cloud computing, and 5G, these new AI-based systems use machine learning and deep learning, and these tools examine large volumes of historical and real-time data to forecast disruptions, quickly change routing courses, and spot traffic trends before they impact network performance (Kashem et al., 2023).

A basic creative idea in these tools is the use of reinforcement learning methods, which enables networks to dynamically change with changing circumstances. By constantly engaging with the network environment, these platforms learn and optimise setups in real-time. This self-adaptive ability is crucial in situations like mobile ad hoc networks (MANETs) and multi-cloud architectures, where conventional static configurations fall behind changing needs. Moreover, network security is now included in the features of new AI-based solutions (Belgaum et al., 2021; Musaddiq et al., 2020). Replacing conventional intrusion detection systems reliant on static signatures, they use intelligent systems that constantly learn and update their threat profiles to identify abnormalities and new attacks, including advanced persistent threats and zero-day vulnerabilities.

Apart from managing network traffic and security, these platforms are reshaping the larger telecoms infrastructure. They are compatible with modern paradigms, including SDN and NFV, in which AI algorithms optimise resource allocation, automate routine maintenance tasks, and minimise operational downtime (Belgaum et al., 2021). This integration creates a flexible framework for including legacy systems in next-generation networks and improves the effectiveness of modern digital environments. Furthermore, the inclusion of AI-driven analytics and decision support systems in these platforms offers network operators practical insights, hence improving the general user experience, lowering service interruptions, and enabling proactive maintenance (Patil, 2024).

AI-based networking tools and platforms are changing the scene of network management and monitoring, hence redefining it. By including advanced analytics, autonomous system optimisation, and improved security measures, they tackle the increasing difficulties presented by complicated, high-demand digital environments. The creative and adaptive capacity of these platforms will influence the future of network infrastructure by guaranteeing secure, efficient, and robust connectivity as they evolve.

3.2.3 How AI is Reducing Routine Networking Tasks

Network administration has been dramatically changed by AI in terms of how to finish once time-consuming, human error-prone everyday activities. Historically, network administration was a manual process that included rule-based changes, continuous performance indicator monitoring, and manual setup. As networks grew in complexity and size, this approach grew more unsustainable (Saeik et al., 2021). By using machine learning and deep learning technologies to examine vast amounts of real-time and historical data, AI-driven systems now automate many of these duties. Advanced algorithms, for instance, can constantly track network traffic patterns, forecast congestion occurrences, and automatically change routing settings, hence guaranteeing the best performance and lowering the need for human involvement (Kibria et al., 2018).

Apart from dynamic traffic control, AI integration is transforming network security and maintenance. Often missing new or changing threats, conventional intrusion detection systems relying on static signature criteria fall short (Belgaum et al., 2021). By means of anomaly detection and behavioural analysis, AI-driven systems identify unusual patterns in network data, hence significantly lessening the load of regular security monitoring on network engineers. The use of reinforcement learning also helps networks to become self-adaptive by allowing them to change configurations in real time to handle developing problems like load imbalances or possible failures. This automation not only increases dependability and decreases downtimes but also minimises the operational overhead associated with human troubleshooting and routine maintenance procedures (Waqar et al., 2024).

In general, AI is effectively offloading repetitive and low-value jobs from network specialists. By automating mundane operations such as traffic optimisation, anomaly detection, and security monitoring, AI enables network engineers to transfer their focus to more strategic, creative, and complex problem-solving tasks. As digital infrastructures grow and evolve, this growth not only improves operational efficiency and network stability but also lays the groundwork for future advances in network management approaches.

3.2.4 The Changing Skill Requirements for Network Engineers

The skill needs for network engineers are changing significantly as AI is quickly integrated into network management and security. Historically, these workers designed, configured, and maintained networks using manual settings, rule-based troubleshooting, and reactive security techniques. The scope of their duties, though, has been widened by the rise of AI-driven technologies. Network engineers are now expected to be skilled in data analytics, deep learning, and machine learning, which will enable them to use AI for dynamic network optimisation and pre-emptive threat detection (Srikanth, 2020). Driven by technologies such as IoT, cloud computing, and 5G, modern networks' increasing complexity is driving this change directly. These technologies call for intelligent systems that are able to perform real-time analysis and autonomous decision-making (Javaid et al., 2018).

Moreover, network engineers have to acquire the capacity to include and control these state-of-the-art platforms as AI-powered networking solutions become increasingly crucial for the preservation of robust infrastructures. This calls for a thorough knowledge of the larger consequences of AI prejudice and openness in decision-making processes, as well as a knowledge of reinforcement learning for adaptive routing and anomaly detection algorithms for improved security (Arshad et al., 2022; Javaid et al., 2018). The changing scene calls for engineers to not only grasp conventional protocols and hardware setups but also have a deep knowledge of AI frameworks and their uses in network environments. Consequently, the expanding role of network engineers today combines traditional IT abilities with advanced data science competencies, positioning them as important strategists in the design and implementation of next-generation networks.

Apart from technical reorientation, the move to AI-enhanced networking calls for a constant commitment to professional development and upskilling. As AI takes on routine tasks like traffic optimisation and predictive maintenance, the literature indicates network professionals can focus on more strategic, high-level issues, including shaping policies around system security, integrating legacy infrastructure with modern AI solutions, and addressing the ethical aspects of AI deployment. Educational curricula and industry training courses are therefore stressing the convergence of network engineering with AI, programming, and data analytics more and more, guaranteeing that the workforce stays competitive and able to propel innovation in a constantly changing technological environment (Billiot, 2023).

Ultimately, AI is changing the conventional function of network engineers from routine task executors to strategic innovators by means of network management. This change calls for a mix of conventional network knowledge and sophisticated knowledge in machine learning, data analytics, and AI-driven system management. As network infrastructures get more complicated and interconnected, the need for engineers who can negotiate this hybrid terrain will only grow, hence stressing the importance of lifelong learning and adaptability in the field.

4. Job Creation and Evolution in Network Engineering

4.1 New Roles Emerging Due to AI in Networking

New roles like AI Network Architect and Network Automation Engineer are growing and becoming vital as AI-driven systems optimise network performance and automate repetitive activities (Ilyas, 2022). Designing network infrastructures that naturally include AI ideas, an AI Network Architect guarantees the smooth integration of machine learning algorithms, dynamic route optimisation using reinforcement learning, and sophisticated anomaly detection systems. To build durable, scalable, and adaptive architectures for fast-changing network environments, this position calls for a thorough knowledge of both traditional network protocols and modern AI frameworks. At the same time, the job of a Network Automation Engineer emphasises implementing automated systems, minimising manual involvement in network administration. These experts create scripts, run AI-powered monitoring systems, and apply adaptive setups, allowing predictive maintenance and real-time decision-making. Both positions call for an interdisciplinary skill set combining conventional network engineering with data analytics, machine learning, and a sharp understanding of cybersecurity concerns related to automated systems (Attkan and Ranga, 2022). Therefore, these new roles are not only crucial in improving network efficiency and security but also important in fostering innovation inside digital infrastructures, thereby preparing the way for a more agile and proactive network administration in the age of AI.

4.2 Demand for AI-knowledgeable network engineers

Network engineers used manual or rule-based techniques to configure, monitor, and manage infrastructures. Modern networks' growing complexity—driven by the spread of IoT devices, cloud computing, and 5G connectivity—requires strong technical skills combining traditional networking knowledge with AI capabilities (Agarwal). To drive automation, improve security via dynamic threat detection, and enable adaptive routing strategies in real time, organisations are now looking for people who can include machine learning, deep learning, and sophisticated data analytics in network operations (Chao et al., 2021).

The transformation driven by Artificial intelligence requires constant education and multidisciplinary knowledge. Businesses are realising that solutions driven by AI may increase general operating efficiency, lower downtime, and improve network performance. The market is therefore emphasising people's ability to develop and run smart network infrastructures with self-configuration and predictive maintenance control. This change is not only altering hiring policies but also pushing educational institutions and professional training programs to include AI-focused courses into conventional network engineering curricula, therefore guaranteeing that future network professionals are ready to manage both legacy systems and sophisticated AI environments (Khawar et al., 2024). Moreover, the security issues companies face in the modern digital world underline the urgent need for AI-aware network engineers even more. Organisations depend more and more on AI-driven systems that need qualified engineers to deploy, control, and understand their results since conventional intrusion detection techniques fall short of advanced cyber threats. This integration emphasises a more general trend in which the ability to function under a hybrid framework—a mix of conventional networking and AI-driven automation—becomes a vital strategic asset. Eventually, this shifting need forces teachers as well as industry players to give network engineers' development of AI skills a top priority, therefore guaranteeing that the telecom system stays robust, flexible, and safe in a time of fast digital transformation (Sakshi et al., 2024).

4.3 The Importance of AI-driven Security and Threat Management Roles

Sophisticated cyber dangers in the modern digital environment have called for a significant reworking of network security; at the heart of modern cybersecurity initiatives are AI-driven security and threat management responsibilities. In the past, security systems depended on static, signature-based detection techniques that were unable to detect new or changing threats like advanced persistent threats or zero-day vulnerabilities. By contrast, AI-driven systems analyse enormous data sets in real time, identify anomalies, and quickly react to developing security threats using machine learning and deep learning. This changing power not only decreases the frequency of false positives but also allows proactive threat mitigation, hence enhancing the general resilience of the network (Reddy, 2021).

AI-powered security functions have become vital in settings marked by fast-growing and more complicated networks. The explosion of IoT devices, cloud computing, and 5G technology has exponentially increased the amount of data and possible risks. Security experts with AI knowledge are now able to apply dynamic security policies that adapt and learn with the threat environment. AI-based technologies that can forecast possible attack vectors and automatically modify network defences are under development, administration, and ongoing fine-tuning. Maintaining strong security postures that safeguard vital infrastructures and data integrity depends on this (Iqbal et al., 2023).

AI-driven threat management roles also work as a link between traditional cybersecurity measures and the need for quick, automated reactions to complex threats. These people are in a unique position to include AI in more general security systems using intrusion detection systems and behavioural analytics tools running with little human involvement. Their efforts not only improve defences but also lighten the load on IT departments, allowing them to concentrate on strategic concerns instead of everyday monitoring activities. The functions devoted to AI-driven security and threat management are vital in a time marked by unrelenting cyber threats and growing assault complexity since they help companies stay safe and strong.

Ultimately, as cyber threats evolve, the importance of AI-driven security and threat management jobs is incalculable. The shift from reactive, signature-based defences to proactive, intelligent security systems that can forecast, identify, and neutralise threats in real-time depends on these positions. Incorporating cutting-edge AI technology into security operations not only improves the effectiveness of threat management initiatives but also ensures that companies can stay ahead in an always changing digital battlefield.

4.4 Case Studies of Companies Adopting AI-Enhanced Networking

Recent case studies show that AI-enhanced networking is transforming several businesses. For instance, well-known telecom firms such as Verizon (USA) and AT&T (USA) have used AI algorithms to forecast peak traffic levels and dynamically change network settings. By including machine learning models to examine real-time and historical traffic data, these businesses have efficiently allocated bandwidth, lowered latency, and significantly lowered service degradation during peak demand times. One operator claimed a significant rise in network efficiency, which led to improved customer happiness and a competitive market edge (Agarwal et al., 2024; Sahin and Sathya, 2024).

Financial sector companies such as JPMorgan Chase (USA), HSBC (UK) and Bank of America (USA) have installed AI-driven anomaly detection systems inside their network architecture to strengthen cybersecurity initiatives (Eswaran et al., 2025; Popoola; Tayyab et al., 2025). By surpassing traditional, signature-based intrusion detection techniques, these companies are now able to spot zero-day vulnerabilities and advanced persistent attacks in real-time. By means of ongoing learning from changing data patterns, these systems lower false positives and hasten incident response procedures, so protecting sensitive information more precisely (Ajayi et al., 2024; Lawal, 2025).

E-commerce behemoths and cloud providers such as Alibaba (China) and Amazon (USA) are also leading this technological change. They handle complex virtualised settings, including SDN and NFV, using AI-enhanced networking technologies. These systems use predictive analytics and reinforcement learning to automate regular activities such as network monitoring, resource allocation, and fault correction (Rao, 2018; Zhang et al., 2019). This strategy eventually results in real advantages such as a reduction in outage and cost savings. Case studies from these industries have highlighted the practical value of AI integration by showing significant gains in total cost of ownership (TCO) and bandwidth use.

Together, these case studies show that the application of AI-enhanced networking is a pragmatic solution that produces measurable benefits rather than just a theoretical evolution. Companies in many sectors are seeing improved operating efficiency, better security, and the ability to change with the times to meet modern digital infrastructure needs. The use of AI in network management is expected to provide new benchmarks for proactive threat management, scalability, and dependability, hence enabling a robust and flexible future in telecoms as AI keeps evolving (Thakur et al., 2024).

5. Job Displacement and Reskilling Challenges

5.1 Identifying Roles Most at Risk of Displacement

Rapid integration of AI into network management and more general digital infrastructures is increasing the displacement risk for jobs depending mainly on repetitive, rule-based operations. AI-driven technologies, which can carry out these tasks with incredible speed and accuracy, are very vulnerable for traditional jobs like network technicians, who are solely in charge of manual configuration, routine monitoring, and fundamental troubleshooting (Adhikari, 2024). Positions requiring constant network traffic monitoring for anomalies or manual routing protocol modification, for example, are being increasingly assigned to machine learning algorithms and reinforcement learning systems, which continuously optimise network performance without human involvement. Administrative jobs and support responsibilities linked to network operations, such as data entry and log analysis, face an increased risk of displacement as well because of the natural predictability and recurrence of these activities. As AI-based networking solutions develop to include dynamic threat detection and real-time performance management, jobs that do not require complex decision-making or creative problem-solving become even less important (Man, 2022). The observation underlines this trend even more. The fact that, despite the possibilities AI is creating for specialised professions like AI Network Architects and Network Automation Engineers, who use advanced analytics, programming, and data science, the majority of conventional, task-oriented jobs are struggling with significant challenges emphasises all the more the urgent need for continuous professional development and upskilling. This strategic change is essential to ensure that the workforce can move from jobs vulnerable to automation to ones that leverage human creativity in the administration and innovation of AI-enhanced digital ecosystems (Tschang and Almirall, 2021).

5.2 Importance of Reskilling and Upskilling for Network Engineers

5.2.1 Training Programs in AI, Machine Learning, and Data Science

Traditional network engineering duties are becoming more and more intertwined with sophisticated computational methods and data-driven decision-making in today's quickly evolving digital environment. This paradigm change has underlined the need for thorough training courses, especially meant to teach knowledge in AI, ML and data science (Weiss, 1999). These training programs aim to provide network engineers with a thorough knowledge of the theoretical and practical aspects of AI-driven technology. Courses covering machine learning algorithms—including supervised learning techniques like support vector machines and decision trees and unsupervised methods like clustering and anomaly detection—help engineers more precisely examine network traffic patterns, forecast possible bottlenecks, and find security weaknesses. Likewise, by signing up for deep learning courses focussing on neural network designs and reinforcement learning applications, professionals can create systems that automatically change routing algorithms in real time. Specialised courses in data science also enable network engineers to use modern technologies such as Python, R, TensorFlow, and PyTorch to analyse, visualise, and interpret large amounts of network data (Raschka et al., 2020; Sun and Gao, 2018). These structured training courses offer a framework for critical thinking and problem-solving that spans the gap between conventional network management and the evolving needs of AI-integrated systems, not only about learning new technology. By converting raw data into meaningful insights through participation in these educational paths, network engineers are well-positioned to foster innovation in digital infrastructures and improve network performance and security (Spector and Ma, 2019).

5.2.2 The Role of Continuous Learning in Career Sustainability

Apart from the first training courses, network engineers working in an AI-enhanced environment find continuous learning to be absolutely vital for career sustainability. In such a dynamic environment, the commitment to lifelong learning is not only beneficial but also essential for the maintenance of professional relevance and a competitive edge (Edwards-Fapohunda and Adediji, 2024). Ongoing education includes advanced certifications, industry conferences, peer networking, and self-directed study via Internet resources. These possibilities for constant learning keep engineers aware of emerging trends, including the most recent developments in cognitive network management, automated threat mitigation techniques, and the integration of SDN with AI algorithms (Marquardson, 2024). Furthermore, constant learning helps professionals to develop an adaptive attitude that helps them handle unanticipated challenges like the implementation of new network security protocols to fight the spread of IoT and the evolution of cyber threats or the recalibration of system architectures to fit multi-cloud environments (Malik et al., 2021). This unyielding quest for knowledge guarantees that businesses have access to a workforce able to negotiate complex digital environments, hence improving individual skill sets and strengthening 32rganizational resilience. In the end, constant learning changes the traditional function of network engineers from one of technical maintenance to one of strategic innovation, so enabling them to proactively affect long-term technological directions and guarantee the dependability, efficiency, and security of contemporary network infrastructures.

5.3 Industry Trends in AI-Based Networking Education

In recent years, the fast integration of AI into the domain of network engineering has produced a fundamental change in the presentation and educational material. Academic institutions and training providers have come to increasingly 32emocrati the need to 32emocrati conventional curricula once solely concentrated on the configuration of routers, the administration of local and wide area networks, and the application of basic cybersecurity policies. Networking education today includes advanced topics such as data analytics, deep learning, and machine learning. These courses are meant to teach students the principles of modern networking technologies and to include pragmatic, hands-on learning opportunities. These experiences comprise reinforcement learning for dynamic network 32emocratizat, predictive modelling for traffic control, and real-time anomaly detection for improved security (Abbasi et al., 2025).

At the same time, the number of collaborations between industry and academia has significantly risen. Universities are working with telecom operators and large IT corporations to provide specific quick courses and certification programs. These alliances ensure that the training material is directly relevant to the needs and expectations of the sector, hence giving professionals and students direct access to state-of-the-art tools and methods. These partnerships expose participants to projects simulating real-world situations, including the management of complex network ecosystems in cloud settings and the integration of SDN with AI algorithms. The certification programs that have arisen from these alliances have received notable acclaim since they certify that graduates possess the hybrid knowledge required to negotiate both conventional networking and new AI-driven infrastructures (Cantú-Ortiz et al., 2020).

The expansion of online education platforms has also significantly influenced industry trends in AI-based networking education. The adoption of Massive Open Online Courses (MOOCs) and virtual laboratories has enabled learners all around the world to receive inexpensive, flexible, high-quality instruction. Courses provided by digital platforms such as Coursera, edX, and Udacity all include hands-on projects, real-time data analysis exercises, and interactive simulations. This 33emocratization of learning has not only increased access to advanced networking education but has also allowed professionals to continuously upgrade their abilities in line with fast technical developments. Often included in such platforms, adaptive learning systems guarantee that students get tailored education depending on their particular development and needs (Mutawa, 2023).

Investment patterns underline even more the importance of AI-based networking education. Within both the public and private sectors, resources are being directed to projects meant to develop a workforce highly skilled in the management of modern digital infrastructures. Government funding, venture capital investments in educational companies, and public-private partnerships all significantly favour the inclusion of sophisticated AI themes into the networking curriculum. This financial assistance not only enables the development of creative course material but also ensures that educational programs keep adapting to meet the evolving requirements of the telecoms industry (Yerlikaya and Erzurumlu, 2021).

The dynamic growth of AI-based networking education is expected to last. Educational programs are progressively including multidisciplinary approaches combining aspects of cybersecurity, IoT management, and even developing fields like quantum computing. Faculty and business professionals are constantly honing these courses to ensure that graduates are sufficiently prepared to meet the several challenges of modern network administration. In the end, these trends guarantee that the future generation of network engineers will be competent in both conventional networking and the revolutionary AI technologies transforming digital communications, security, and general network efficiency (Hadzovic et al., 2023).

6. Future Trends and Predictions

6.1 Predictions on the Future of AI in Networking

In the management and optimisation of digital infrastructures, AI in networking is about to undergo a paradigm shift. As network management protocols develop, they will become more closely connected with AI technologies, hence producing a progressive shift from static, manually designed systems to dynamic, self-adaptive entities (Krenn et al., 2023). Future networks are expected to show self-optimising features whereby machine learning algorithms constantly examine performance measurements, forecast any problems, and automatically change settings to preserve the best data flows. This change ensures networks that are more resource-efficient, durable, and able to handle the exponential growth of connected devices, therefore ensuring dependable connectivity even during peak times (Dandamudi et al., 2025).

Artificial intelligence is anticipated to transform network environment cybersecurity in concert with the evolution towards resource optimisation and self-management. The constantly changing malware patterns, complex advanced persistent threats, and emerging zero-day attacks in the growing threat environment call for more adaptable security mechanisms. Future networks are probably going to have AI-driven security and threat management systems capable of incident response and real-time anomaly identification. Continuous learning of these systems from new data helps to enable the ability to detect tiny anomalies from regular activity and reduce risks before they escalate (Alshahrani, 2023). Apart from lowering the incidence and effect of security breaches, the general use of such innovative defences would also create the basis for networks capable of self-defence against cyber attacks and preservation of data integrity.

The incorporation of AI is also expected to inspire the development of creative networking topologies combining modern software-defined solutions with conventional hardware. For instance, the combination of AI with NFV and SDN will allow the creation of networks that are programmable, scalable, and able to handle a broad spectrum of applications, including IoT and 5G. As these technologies develop, networks will become more adaptable since they will dynamically allot resources and reroute traffic depending on real-time monitoring and predictive analysis. By cutting the need for human interaction and hastening the reaction to urgent network issues, this degree of automation is expected to lower operational overhead significantly (Barakabitze et al., 2020).

The future of AI in networking will also significantly change the job market and the skill needs of network workers. The need for network engineers with advanced knowledge in data analytics, machine learning, and AI will keep rising as network administration and routine troubleshooting become more automated. Jobs like AI Network Architect and Network Automation Engineer will be absolutely vital in companies in charge of designing, integrating, and managing smart network systems. The future scene will see the blurring of the lines between conventional network administration and data science, hence producing a workforce that is very flexible and orientated on strategic innovation in digital infrastructure (Gürer et al., 1996).

Ultimately, the future of AI in networking is anticipated to be revolutionary, marked by the integration of smart software with conventional networking hardware, improved cybersecurity systems, and self-optimising networks. These changes are expected to offer significant benefits in terms of efficiency, flexibility, and performance, as well as create new roles and skill sets for network professionals. Furthermore, the ongoing evolution of AI-driven networking will call for the resolution of integration issues and ethical questions, including transparency and bias in algorithmic decision-making, and the need for constant upskilling as well as integration issues (Bala et al., 2023). As these obstacles are surmounted, the possibility of AI transforming the functioning of networks will be fulfilled, thereby creating a digital ecosystem that is resilient, safe, efficient and ready to satisfy the needs of an ever more linked society.

6.2 The Need for Human-AI Collaboration in Networking Jobs

Notwithstanding the amazing developments brought by automation technologies, network management still depends on human knowledge. Though AI-driven technologies are good at data processing and running pre-programmed reactions, they often lack the contextual awareness, creative problem-solving skills, and strategic vision that human engineers provide. Human intuition and decision-making are required in complicated situations like understanding confusing network patterns, making judgement calls in the face of unanticipated security events, or creating totally new architectural solutions. In these situations, network engineers offer the vital supervision required to confirm automated procedures, adjust system reactions, and guarantee that the goals of the network correspond with more general organisational objectives (Jarrahi, 2018).

Though automated and AI-driven tools have made many mundane chores easier, like real-time threat identification and traffic optimisation, they have not made human knowledge irrelevant. Little wonder, modern digital infrastructures are being built on a hybrid model of human-AI cooperation. In this model, human operators offer strategic decision-making, creative problem-solving, and monitoring, while AI systems do most of the tedious, data-intensive tasks. This symbiotic partnership leverages the contextual understanding and ethical reasoning of human specialists as well as the speed and analytical capacity of AI (Wang et al., 2020).

Many important domains show clear human-AI cooperation in networking employment. For instance, AI technologies track network performance and constantly examine data to forecast possible security breaches or disturbances. Still, human judgment is required for the subtle choices on how to interpret these forecasts and how to address them. Therefore, the setup of these AI systems, the verification of their results, and the intervention of network engineers in the case of unanticipated events continue to be significantly influenced by network engineers. Moreover, in complex scenarios where AI algorithms could come across unclear or novel data patterns, human intuition and domain knowledge provide vital direction that enhances automated operations. This cooperative strategy ensures that choices are aligned with the general organisational objectives and are balanced and strong (Waqas et al., 2022).

The evolving scene has also led to the creation of new positions stressing the need for human-AI cooperation. Jobs like AI Network Architect and Network Automation Engineer highlight the dual skills people are required to have. These jobs call for a deep understanding of conventional networking concepts and the capacity to apply AI-driven solutions. Individuals working in these hybrid jobs must cooperate effortlessly with autonomous systems as the development, training, and fine-tuning of AI algorithms, as well as the formulation of high-level choices about network strategy, compliance, and security, all depend on this cooperation. These positions show that the future of networking is not in an either/or situation of people against algorithms but in the use of the unique benefits of both to attain operational excellence and innovation (Sowa et al., 2021).

As digital infrastructures evolve, the concept of human-AI cooperation in networking functions is anticipated to grow increasingly important. As AI technologies develop, the need for constant human supervision to handle ethical issues, guarantee openness in decision-making, and offer flexibility in the face of unanticipated obstacles will stay vital. Through ongoing training and a commitment to multidisciplinary knowledge, network professionals will be even more empowered to augment AI skills with strategic and creative ideas. In the end, the cooperative integration of human knowledge with AI's computational capacity offers a road to more robust, safe, and efficient networks, so guaranteeing that the digital environment can evolve and thrive under fast technology developments (Berretta et al., 2023).

Maintaining an ideal balance between automation and human expertise will be crucial if innovation and security in the networking field are to be sustained. The integration of strong training programs, multidisciplinary cooperation, and ongoing professional development will be especially important in guaranteeing that human skills complement always-advancing automated technology as networks grow more dynamic and interconnected (Billiot, 2023). Those who effectively combine the analytical power of AI with the strategic and ethical judgement of human experts will be better able to navigate the complexity of current digital infrastructures. This approach not only meets present operational requirements but also lays a solid basis for future developments in network management and security. The synergy between automation and human knowledge is especially clear in settings where digital infrastructure's complexity and diversity keep rising. By shouldering normal operating responsibilities, automated systems free up human resources and let engineers concentrate on strategic projects, including system innovation, policy formulation, and long-term infrastructural enhancements. Human supervision of automated systems fosters ongoing progress, and this balance improves the general strength and resilience of network operations. Engineers can find minute variations in automated outputs, modify systems to meet new demands, and include feedback for iterative improvement of network algorithms, guaranteeing that automation acts as an extension of human understanding rather than operating in isolation (Das, 2024).

6.3 Recommendations for Network Engineers to Stay Relevant in the AI Era

Network engineers, as the vanguard of the management of more complicated infrastructures shaped by the growing integration of AI in the fast-changing digital environment of today, have to aggressively seek continuous skill development and knowledge if they are to keep their competitive edge and vital position. Acquiring a fundamental knowledge of data analytics, machine learning methods, and AI technology starts this process (Awaludin et al., 2024). Engineers are urged to enrol in additional courses, certificates, and specialised training focussing on the theoretical foundations and practical uses of these technologies. Programs provided via industry-recognised platforms—such as MOOCs or vendor-specific training—can help to close the knowledge gap between conventional network administration and new AI-driven approaches (Camilleri and Tannhäuser, 2013). Understanding the ways in which AI tools may optimise performance, improve threat detection, and automate network activities depends on this basic improvement.

Apart from finishing the first training, continual professional development is absolutely necessary to keep current with the always-changing character of technology. Network engineers are advised to participate in conferences, seminars, and workshops focussing on the most recent developments in networking and emerging AI trends. Participating in active learning communities—both online and offline—helps to foster an environment of peer-to-peer learning and hence promotes the exchange of ideas and best practices. Moreover, self-directed projects like the creation of prototypes, including AI solutions or the support of open-source networking technologies, provide useful experience and improve technical knowledge (Chemouil et al., 2019). This constant commitment to lifelong learning not only helps people to stay current on industry changes but also opens doors for creativity and leadership in network operations.

Other important suggestions call for using an interdisciplinary approach. Professionals are required to have a hybrid skill set that exceeds traditional technical skills since networking and AI are converging. Network architects should closely cooperate with cybersecurity professionals, software developers, and data scientists if they are to build integrated, resilient systems. Often, this cooperation calls for learning how to use cross-functional tools and platforms—including SDN controllers and NFV systems—as AI algorithms are progressively improving these systems (La Sala et al., 2024). By understanding the larger digital ecosystem and actively participating in cross-disciplinary teams, engineers may greatly shape the evolution of the next generation of smart networks.

Maintaining a successful profession in the AI age also requires strategic thinking and soft skills. As AI takes over repetitive jobs, the human component of strategic oversight, ethical decision-making, and creative problem-solving gets more and more important. Network engineers have to develop leadership traits and honed communication skills if they are to properly lead teams, interact with stakeholders, and convert complex technical knowledge into practical business ideas (Alafnan et al., 2024). By means of executive education or management training, network engineers can be positioned as strategic partners guiding digital transformation projects that complement technical knowledge. Achieving organisational success in an age marked by constant digital disruption and innovation depends on this harmonic combination of technical knowledge and interpersonal abilities.

To be relevant in the AI era, network engineers have to embrace a multidimensional approach that includes the growth of soft skills, ongoing technical education, interdisciplinary cooperation, and a thorough knowledge of ethical and regulatory issues. Network engineers can ensure their ongoing vital contribution to digital infrastructures by actively engaging in these activities and accepting the transforming power of AI, hence ensuring tomorrow's and driving innovation.

Finally, one must keep aware of the ethical, legal, and security consequences of AI implementations. Growing reliance on AI in network management makes understanding issues, including data protection, algorithmic bias, and cybersecurity systems, all the more important. Network engineers have to be well-versed in the shifting regulatory environments and work closely with compliance teams to ensure that AI deployments follow ethical and legal criteria. This thorough knowledge not only lowers risk but also enhances the engineer's role as a reliable counsel in policy creation and strategic planning (Korobenko et al., 2024).

7. Conclusion

The integration of AI into network engineering is not merely an incremental technological advancement; it represents a fundamental transformation of the field. This paper has explored the multifaceted impact of AI on network management, security, and the evolving role of network engineers in the context of emerging technologies like 6G. The transition from traditional, manual network administration to AI-driven, automated systems signifies a paradigm shift, demanding a profound re-evaluation of the skills and responsibilities of network engineers.

The analysis has underscored how AI-driven automation is streamlining routine tasks, enhancing network performance, and bolstering security measures. By leveraging machine learning, deep learning, and reinforcement learning, AI enables real-time analytics, predictive maintenance, and adaptive security protocols, thereby optimizing network efficiency and resilience. This automation, however, does not diminish the importance of network engineers; rather, it elevates their role to strategic oversight and complex problem solving.

The evolving landscape necessitates a significant expansion of the skill set required for network engineers. Proficiency in AI technologies, data analytics, and machine learning is becoming indispensable for managing and securing intricate digital infrastructures. This shift underscores the importance of continuous education and professional development to ensure network engineers remain relevant in an AI-driven environment.

Furthermore, this paper has highlighted the implications of AI integration on employment within the network engineering domain. While AI automates routine tasks, it simultaneously creates new opportunities requiring advanced technical expertise. The ability to design, implement, and manage AI-driven networking tools and platforms becomes a crucial asset, fostering innovation and driving the development of robust digital ecosystems.

In essence, the future of network engineering is inextricably linked to the advancement of AI. Network engineers, equipped with the necessary skills and knowledge, are pivotal in facilitating the seamless integration of AI technologies, ensuring the reliability and security of digital infrastructures. As we move towards more intelligent and interconnected networks, the role of network engineers will continue to evolve, demanding adaptability, innovation, and a proactive approach to embracing emerging technologies. The successful navigation of this evolving landscape will be crucial in building secure, efficient, and sustainable digital environments that support the ever-growing demands of our interconnected world.

8. Reference

Abbasi, Wu and Luo. (2025). Exploring the impact of artificial intelligence on curriculum development in global higher education institutions. *Education and Information Technologies, 30*(1), 547-581.

Adhikari. (2024). Exploring the Nexus between Artificial Intelligence and Job Displacement: A Literature Review. *Journal of National Development, 37*(1), 1-13.

Agarwal. How Artificial Intelligence is Employed in Business Managerial Decision.

Agarwal, Mangla and Ramadani. (2024). Enlightening cases: Utilization of exemplary AI-enhanced research endeavors *Utilizing AI Tools in Academic Research Writing* (pp. 158-170): IGI Global.

Ahmad and Habelamateen. (2023). Application of Artificial Intelligence and Machine Learning in Software Defined Networks. *Journal of Smart Internet of Things, 1*, 14-22.

Ahmad, Shahabuddin, Sauter, Harjula, Kumar, Meisel, Juntti and Ylianttila. (2020). The challenges of artificial intelligence in wireless networks for the Internet of Things: Exploring opportunities for growth. *IEEE Industrial Electronics Magazine, 15*(1), 16-29.

Ahmed, Yong and Shrestha. (2023). The integral role of intelligent IoT system, cloud computing, artificial intelligence, and 5G in the user-level self-monitoring of COVID-19. *Electronics, 12*(8), 1912.

Ajayi, Omokanye, Olowu, Adeleye, Omole and Wada. (2024). Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity.

Alafnan, Dishari and Mohdzuki. (2024). Developing soft skills in the artificial intelligence era: Communication, business writing, and composition skills. *Journal of Artificial Intelligence and Technology, 4*(4), 305-317.

Alshahrani. (2023). *Optimising IDS configurations for IoT networks using AI approaches.* University of Sheffield.

Argyroudis, Mitoulis, Chatzi, Baker, Brilakis, Gkoumas, Vousdoukas, Hynes, Carluccio and Keou. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management, 35*, 100387.

Arshad, Ali, Muneer, Aziz, Naseer, Khan and Taib. (2022). Deep reinforcement learning for anomaly detection: A systematic review. *Ieee Access, 10*, 124017-124035.

Attkan and Ranga. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. *Complex & Intelligent Systems, 8*(4), 3559-3591.

Autor. (2015). Why are there still so many jobs? The history and future of workplace automation. *Journal of economic perspectives, 29*(3), 3-30.

Awaludin, Yasin and Risyda. (2024). The Influence of Artificial Intelligence Technology, Infrastructure and Human Resource Competence on Internet Access Networks. *Inform: Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi, 9*(2), 111-120.

Bala, Mijwil, Ali and Sadıkoğlu. (2023). Analysing the connection between AI and industry 4.0 from a cybersecurity perspective: Defending the smart revolution.

Barakabitze, Ahmad, Mijumbi and Hines. (2020). 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks, 167*, 106984.

Belgaum, Alansari, Musa, Alam and Mazliham. (2021). Impact of artificial intelligence-enabled software-defined networks in infrastructure and operations: Trends and challenges. *International Journal of Advanced Computer Science and Applications, 12*(1).

Berretta, Tausch, Ontrup, Gilles, Peifer and Kluge. (2023). Defining human-AI teaming the human-centered way: a scoping review and network analysis. *Frontiers in Artificial Intelligence, 6*, 1250725.

Billiot. (2023). Continuous learning and advancing technologies: a framework for professional development and training in artificial intelligence. *Development and Learning in Organizations: An International Journal, 37*(3), 28-31.

Boukerche, Tao and Sun. (2020). Artificial intelligence-based vehicular traffic flow prediction methods for supporting intelligent transportation systems. *Computer networks, 182*, 107484.

Bringsjord and Schimanski. (2003). What is artificial intelligence? Psychometric AI as an answer. Paper presented at the IJCAI.

Bukartaite and Hooper. (2023). Automation, artificial intelligence and future skills needs: an Irish perspective. *European Journal of Training and Development, 47*(10), 163-185.

Camilleri and Tannhäuser. (2013). Assessment and recognition of open learning *Openness and Education* (pp. 85-118): Emerald Group Publishing Limited.

Cantú-Ortiz, Galeano Sánchez, Garrido, Terashima-Marin and Brena. (2020). An artificial intelligence educational strategy for the digital transformation. *International Journal on Interactive Design and Manufacturing (IJIDeM), 14*, 1195-1209.

Challita, Ryden and Tullberg. (2020). When machine learning meets wireless cellular networks: Deployment, challenges, and applications. *58*(6), 12-18.

Chao, Hsu, Liu and Cheng. (2021). Knowledge of and competence in artificial intelligence: Perspectives of Vietnamese digital-native students. *Ieee Access, 9*, 75751-75760.

Chavhan and Assessments. (2022). Shift to 6G: Exploration on trends, vision, requirements, technologies, research, and standardization efforts. *54*, 102666.

Chemouil, Hui, Kellerer, Li, Stadler, Tao, Wen and Zhang. (2019). Special issue on artificial intelligence and machine learning for networking and communications. *IEEE Journal on Selected Areas in Communications, 37*(6), 1185-1191.

Chen, Challita, Saad, Yin, Debbah and Tutorials. (2019). Artificial neural networks-based machine learning for wireless networks: A tutorial. *21*(4), 3039-3071.

Chen, Li, Deng, Li and Yu. (2019). Distributed deep learning model for intelligent video surveillance systems with edge computing.

Cunha, Ferreira, Castro, Oliveira, Nicolau, Núñez, Sousa and Serôdio. (2024). Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet, 16*(7), 226.

Dandamudi, Sajja and Khanna. (2025). Advancing Cybersecurity and Data Networking Through Machine Learning-Driven Prediction Models. *International Journal of Innovative Research in Computer Science and Technology, 13*(1), 26-33.

Dao. (2023). Internet of wearable things: Advancements and benefits from 6G technologies. *138*, 172-184.

Das. (2024). Exploring the symbiotic relationship between digital transformation, infrastructure, service delivery, and governance for smart sustainable cities. *Smart Cities, 7*(2), 806-835.

Edwards-Fapohunda and Adediji. (2024). Sustainable development of distance learning in continuing adult education: The impact of artificial intelligence. *IRE Journals, 8*(1), 113-114.

Ernst, Merola and Samaan. (2019). Economics of artificial intelligence: Implications for the future of work. *IZA Journal of Labor Policy, 9*(1), 1-35.

Eswaran, Eswaran, Murali, Eswaran, Banking and Services. (2025). Role of Edge Technologies and Applications in Banking and Finance Industry. 290.

Firouzi, Farahani and Marinšek. (2022). The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *107*, 101840.

Gürer, Khan, Ogier and Keffer. (1996). An artificial intelligence approach to network fault management. *Sri international, 86*.

Hadzovic, Mrdovic and Radonjic. (2023). A path towards an internet of things and artificial intelligence regulatory framework. *IEEE Communications Magazine, 61*(7), 90-96.

Hu, Kuang, Qin, Li, Zhang, Gao, Li and Li. (2021). Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys (CSUR), 55*(1), 1-36.

Huang. (2023). Digital engineering transformation with trustworthy AI towards industry 4.0: emerging paradigm shifts. *Journal of Integrated Design and Process Science, 26*(3-4), 267-290.

Ilyas. (2022). Emerging Role of Artificial Intelligence. *Journal of Systemics, Cybernetics and Informatics, 20*(6), 58-65.

Iqbal, Rizvi, Haider and Raza. (2023). Artificial Intelligence in Security and Defense: Explore the integration of AI in military strategies, security policies, and its implications for global power dynamics. *International Journal of Human and Society, 3*(4), 341-353.

Jarrahi. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business horizons, 61*(4), 577-586.

Javaid, Sher, Nasir and Guizani. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. *IEEE Communications Magazine, 56*(10), 94-100.

Johnson, Jain, Brennan-Tonetta, Swartz, Silver, Paolini, Mamonov and Hill. (2021). Impact of big data and artificial intelligence on industry: developing a workforce roadmap for a data driven economy. *Global Journal of Flexible Systems Management, 22*(3), 197-217.

Karamchand. (2024). Networking 4.0: The Role of AI and Automation in Next-Gen Connectivity. *Journal of Big Data and Smart Systems, 5*(1).

Kashem, Shamsuddoha, Nasir and Chowdhury. (2023). Supply chain disruption versus optimization: a review on artificial intelligence and blockchain. *Knowledge, 3*(1), 80-96.

Khan, Shad, Sethi and Bibi. (2024). The Impact of Artificial Intelligence (AI) on Job Displacement and the Future Work. *Social Science Review Archives, 2*(2), 2296-2306.

Khawar, Salman, Shaheen, Shakil, Iftikhar and Faisal. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. *Spectrum of Engineering Sciences, 2*(4), 115-132.

Kibria, Nguyen, Villardi, Zhao, Ishizu and Kojima. (2018). Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks. *IEEE access, 6*, 32328-32338.

Korobenko, Nikiforova and Sharma. (2024). Towards a privacy and security-aware framework for ethical AI: Guiding the development and assessment of AI systems. Paper presented at the Proceedings of the 25th Annual International Conference on Digital Government Research.

Koski and Husso. (2018). Work in the age of artificial intelligence: Four perspectives on the economy, employment, skills and ethics.

Krenn, Buffoni, Coutinho, Eppel, Foster, Gritsevskiy, Lee, Lu, Moutinho and Sanjabi. (2023). Forecasting the future of artificial intelligence with machine learning-based link prediction in an exponentially growing knowledge network. *Nature Machine Intelligence, 5*(11), 1326-1335.

La Sala, Fuller, Riolli and Temperini. (2024). The rise of hybrids: plastic knowledge in human–AI interaction. *Journal of Knowledge Management, 28*(10), 3023-3045.

Lane and Saint-Martin. (2021). The impact of Artificial Intelligence on the labour market: What do we know so far? *OECD Social, Employment, and Migration Working Papers*(256), 0_1-60.

Lawal. (2025). AI-Powered Anomaly Detection: Revolutionizing AML Compliance in US Banks.

Lecun, Bengio and Hinton. (2015). Deep learning. *521*(7553), 436-444.

Lu and Zheng. (2020). 6G: A survey on technologies, scenarios, challenges, and the related issues. *19*, 100158.

Malik, Tripathi, Kar and Gupta. (2021). Impact of artificial intelligence on employees working in industry 4.0 led organizations. *International Journal of Manpower, 43*(2), 334-354.

Man. (2022). *Towards the Future of Work: Managing the Risks of AI and Automation.* Massachusetts Institute of Technology.

Marquardson. (2024). Embracing Artificial Intelligence to Improve Self-Directed Learning: A Cybersecurity Classroom Study. *Information Systems Education Journal, 22*(1), 4-13.

Meena, Pal, Jain and Pamula. (2022). 6G communication networks: introduction, vision, challenges, and future directions. *125*(2), 1097-1123.

Mishra, Ravinder Reddy, Tyagi and Arowolo. (2024). Artificial intelligence-enabled edge computing: Necessity of next generation future computing system *IoT Edge Intelligence* (pp. 67-109): Springer.

Mistry, Mavani, Goswami and Patel. (2024). Artificial intelligence for networking. *Educational Administration: Theory and Practice, 30*(7), 813-821.

Mithas, Chen, Saldanha and De Oliveira Silveira. (2022). How will artificial intelligence and Industry 4.0 emerging technologies transform operations management? *Production and Operations Management, 31*(12), 4475-4487.

Mohamed, Ahmed Ibrahim, Hamed and Abdelnaby. (2024). Engineering's Next Leap: How Fourth Industrial Revolution is Shaping the Future of the Industry. *ERU Research Journal*, 1-21.

Moro-Visconti. (2024). Natural and Artificial Intelligence Interactions in Digital Networking: A Multilayer Network Model for Economic Value Creation. *Journal of Comprehensive Business Administration Research*.

Mossavar-Rahmani and Zohuri. (2024). Artificial intelligence at work: Transforming industries and redefining the workforce landscape. *Journal of Economics & Management Research SRC/JESMR-284 J Econ Managem Res, 5*(2), 2-4.

Musaddiq, Ali, Bajracharya, Qadri, Al-Turjman and Kim. (2020). Trends, issues, and challenges in the domain of IoT-based vehicular cloud network. *Unmanned Aerial Vehicles in Smart Cities*, 49-64.

Mutawa. (2023). Perspective chapter: MOOCS at higher education–Current state and future trends. *Massive Open Online Courses-Current Practice and Future Trends*.

Oladosu, Ike, Adepoju, Afolabi, Ige and Amoo. (2021). The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. *Magna Scientia Advanced Research and Reviews*.

Ota, Dao, Mezaris, Natale and Applications. (2017). Deep learning for mobile multimedia: A survey. *13*(3s), 1-22.

Patil. (2024). Artificial Intelligence-Driven Predictive Maintenance In Manufacturing: Enhancing Operational

Efficiency, Minimizing Downtime, And Optimizing Resource Utilization. *Minimizing Downtime, And Optimizing Resource Utilization (December 11, 2024)*.

Popoola. Big Data-Driven Financial Fraud Detection and Anomaly Detection Systems for Regulatory Compliance and Market Stability.

Puaschunder. (2019). Artificial intelligence in the healthcare sector. *Scientia Moralitas-International Journal of Multidisciplinary Research, 4*(2), 1-14.

Raihan and Evolution. (2023). An overview of the implications of artificial intelligence (AI) in sixth generation (6G) communication network. *9*, 120-146.

Rane, Choudhary and Rane. (2024). Artificial intelligence for enhancing resilience. *Journal of Applied Artificial Intelligence, 5*(2), 1-33.

Rao. (2018). Reimagining service assurance for NFV, SDN and 5G.

Raschka, Patterson and Nolet. (2020). Machine learning in python: Main developments and technology trends in data science, machine learning, and artificial intelligence. *Information, 11*(4), 193.

Reddy. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *NeuroQuantology, 19*(12), 764-773.

Saeik, Avgeris, Spatharakis, Santi, Dechouniotis, Violos, Leivadeas, Athanasopoulos, Mitton and Papavassiliou. (2021). Task offloading in Edge and Cloud Computing: A survey on mathematical, artificial intelligence and control theory solutions. *Computer Networks, 195*, 108177.

Sahin and Sathya. (2024). Network quality prediction in a designated area using GPS data. *Journal of Network and Computer Applications, 231*, 104002.

Sakshi, Tyagi and Jain. (2024). Emerging trends in hybrid information systems modeling in artificial intelligence. *Hybrid Information Systems: Non-Linear Optimization Strategies with Artificial Intelligence*, 115.

Saurabh, Sharma, Singh, Khondoker, Vyas and Vyas. (2025). Hms-ids: Threat intelligence integration for zero-day exploits and advanced persistent threats in iiot. *Arabian Journal for Science and Engineering, 50*(2), 1307-1327.

Shah and Patel. (2024). Adaptive AI Architectures: Integrating Machine Learning and Self-Healing Capabilities. *International bulletin of History and Social Science, 1*(4), 63-76.

Sharma and Nag. (2023). Cognitive software defined networking and network function virtualization and applications (Vol. 15, pp. 78): MDPI.

Shen, Zhang and Communications. (2024). The impact of artificial intelligence on employment: the role of virtual agglomeration. *11*(1).

Sowa, Przegalinska and Ciechanowski. (2021). Cobots in knowledge work: Human–AI collaboration in managerial professions. *Journal of Business Research, 125*, 135-142.

Spector and Ma. (2019). Inquiry and critical thinking skills for the next generation: from artificial intelligence back to human intelligence. *Smart Learning Environments, 6*(1), 1-11.

Srikanth. (2020). The Role of Network Engineers in Securing Cloud-based Applications and Data Storage.

Strannegård, Engsner, Ferrari, Glimmerfors, Södergren, Karlsson, Kleve and Skoglund. (2021). The ecosystem path to general AI. *arXiv preprint arXiv:210807578*.

Sun and Gao. (2018). The construction of undergraduate machine learning course in the artificial intelligence era. Paper presented at the 2018 13th International Conference on Computer Science & Education (ICCSE).

Tariq, Poulin and Abonamah. (2021). Achieving operational excellence through artificial intelligence: Driving forces and barriers. *Frontiers in psychology, 12*, 686624.

Tayyab, Hameed, Mumtaz, Muzammal, Mahadevappa and Sunbalin. (2025). AI-Powered Threat Detection in Business Environments: Strategies and Best Practices *Generative AI for Web Engineering Models* (pp. 379-436): IGI Global.

Thakur, Sandhu and Yehuwalashet. (2024). E-Commerce and Trade: The Role of Artificial Intelligence *Handbook of Artificial Intelligence Applications for Industrial Sustainability* (pp. 232-248): CRC Press.

Tschang and Almirall. (2021). Artificial intelligence as augmenting automation: Implications for employment. *Academy of Management Perspectives, 35*(4), 642-659.

Van Noordt, Medaglia and Tangi. (2023). Policy initiatives for Artificial Intelligence-enabled government: An analysis of national strategies in Europe. *Public Policy and Administration*, 09520767231198411.

Verma, Lamsal and Verma. (2022). An investigation of skill requirements in artificial intelligence and machine learning job advertisements. *Industry and Higher Education, 36*(1), 63-73.

Wang, Churchill, Maes, Fan, Shneiderman, Shi and Wang. (2020). From human-human collaboration to Human-AI collaboration: Designing AI systems that can work together with people. Paper presented at the

Extended abstracts of the 2020 CHI conference on human factors in computing systems.

Wang, Li and Leung. (2015). Artificial intelligence-based techniques for emerging heterogeneous network: State of the arts, opportunities, and challenges. *IEEE Access, 3*, 1379-1391.

Wang and Siau. (2019). Artificial intelligence, machine learning, automation, robotics, future of work and future of humanity: A review and research agenda. *Journal of Database Management (JDM), 30*(1), 61-79.

Waqar, Bhatti and Khan. (2024). AI-powered automation: Revolutionizing industrial processes and enhancing operational efficiency. *Revista de Inteligencia Artificial en Medicina, 15*(1), 1151-1175.

Waqas, Tu, Halim, Rehman, Abbas and Abbas. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review, 55*(7), 5215-5261.

Weiss. (1999). Multiagent systems: a modern approach to distributed artificial intelligence: MIT press.

Yang, Yu, Bai, Wang, Zhang, Wen and Yu. (2017). A study of ai population dynamics with million-agent reinforcement learning. *arXiv preprint arXiv:170904511.*

Yang, Zhuang and Pan. (2021). Multiple knowledge representation for big data artificial intelligence: framework, applications, and case studies. *Frontiers of Information Technology & Electronic Engineering, 22*(12), 1551-1558.

Yerlikaya and Erzurumlu. (2021). Artificial intelligence in public sector: a framework to address opportunities and challenges. *The fourth industrial revolution: Implementation of artificial intelligence for growing business success*, 201-216.

Young, Hazarika, Poria and Cambria. (2018). Recent trends in deep learning based natural language processing. *13*(3), 55-75.

Zeng. (2020). Artificial intelligence and China's authoritarian governance. *International Affairs, 96*(6), 1441-1459.

Zhang, Huang, Wang, Liu and Engineering. (2019). Future Internet: trends and challenges. *20*(9), 1185-1194.