International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V73I4P102

Volume 73 Issue 4, 5-18, April 2025
© 2025 Seventh Sense Research Group®

Review Article

Integrating Generative AI into Network Systems: Challenges, Opportunities, and Future Directions

Palanichamy Manikandan

Institute of Engineering, Østfold University College, Fredrikstad, Norway.

[1]*Corresponding Author : manikandan.palanichamy@hiof.no*

Received: 02 March 2025 Revised: 03 April 2025 Accepted: 17 April 2025 Published: 28 April 2025

Abstract *- This paper examines the problems and opportunities when incorporating generative AI (GAI) models in network systems. Model interpretability plays a vital role in creating trust and ensuring these technologies are used responsibly. Training such GAI models require significant computational resources, highlighting the need for advancements in both hardware and software. As AI advances, it is necessary to consider GAI usability in next-generation network technologies, including automated design, real-time optimization and AI-powered security. As a contribution, this paper reviews what happened in recent achievements of the GAI crossing to networking so far and how it can lead to more flexible and intelligent networking infrastructures. It further discusses the challenges that need to be addressed and directions for future research. Thus, the intention of this work is to analyze and explore the potential of applying GAI in next-generation network systems and ensure that it effectively meets future demands.*

Keywords *- Generative AI, 6G network, Network automation, Security, AI models.*

1. Introduction

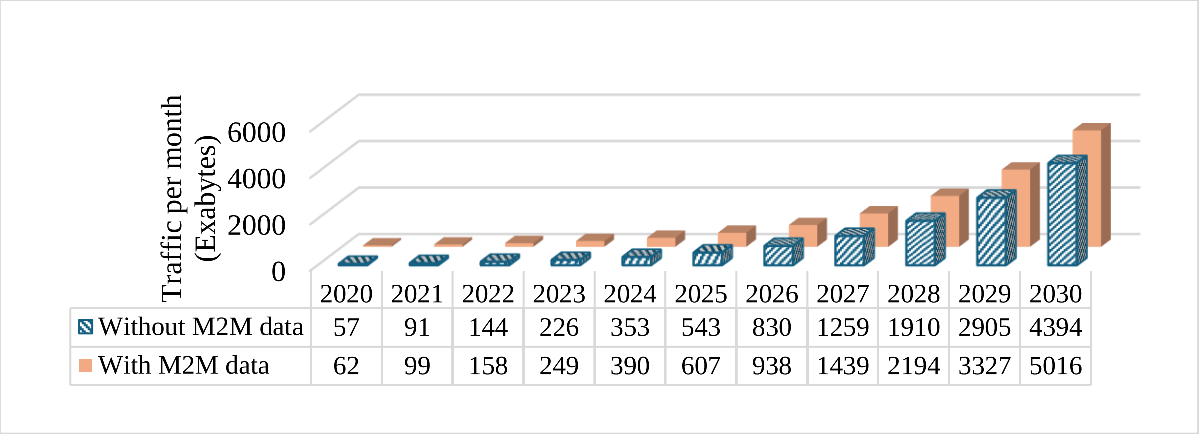
The rapid rise in mobile data usage and the exponential growth of connected devices has made global communication networks more complex. Beyond the growth of the digital age, we see technologies like 5G/6G and Open Radio Access Networks (O-RAN) are emerging to address the challenges. These advanced generation networks aim to deliver higher performance, programmability and flexibility required by modern users.

Unfortunately, the ever-growing demands of these networks create complexity that requires advanced AI-based solutions. Regardless of the advancements in network technologies, a significant research gap remains in the integration of Generative AI (GAI) within network systems. Current research focuses on GAI's capabilities in isolated applications without prioritizing its potential to improve overall network security and management. This overlook presents a significant challenge because the complex network continuously demands innovative solutions to optimize networks and develop an intelligent infrastructure for modern advanced digital services.

This paper reviews the current Generative AI applications in networking and presents a broad context for GAI integration into future network systems. It differs from existing studies by emphasizing the relationship between GAI and various network management functions such as automation, optimization, and security. Additionally, this paper provides a detailed comparative analysis of the most recent research works through a comprehensive table and highlights their findings and methodologies. By addressing both the opportunities and challenges of GAI in networking, this work aims to fill a critical gap and contribute to the development of further resilient and adaptive network infrastructures.

Smartphones have become as essential to our lives as coffee in the morning. They have turned into one of our important gadgets for communication, work and entertainment. Meanwhile, the Internet of Things (IoT) is growing faster every day [1]. Connecting everything from home appliances to industrial machinery. This explosion of connected devices has caused mobile data traffic to skyrocket, as shown in Figure 1.

Experts predict that 2025 mobile data traffic could hit several exabytes annually. To put that into perspective, several exabytes are equivalent to streaming every movie made in ultra-high-definition thousands of times. The volume of information being transmitted through wireless networks keeps increasing because of the extraordinary demand for high-quality services, extreme data rates, and advanced user terminals. Just as a city’s roads become congested during rush hour, the exponential growth in data usage demands smarter, more efficient network infrastructures to prevent digital gridlock [2].



	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
▨ Without M2M data	57	91	144	226	353	543	830	1259	1910	2905	4394
■ With M2M data	62	99	158	249	390	607	938	1439	2194	3327	5016

Fig. 1 Timeline and forecast of global mobile data traffic growth

However, the network framework as it stands today does not have the capacity to operate these data rates. Traditional network management methods have not been able to scale with the modern network. These outdated strategies, by and large, are reactive, not proactive. This results in sub-standard performance, serious security vulnerabilities, and inefficient resource usage. The traditional system, for example, only deals with the network in case of an incident. It does not proactively predict these issues. This method will lead to a certain downtime, slow response and decreased user satisfaction. There is an increasing need for higher-level solutions with artificial intelligence to tackle these challenges. One of the most potential ways is for an advanced approach to learn complex data patterns and synthesize information that can reflect real world situations. Generative AI (GAI) has such ability and is useful in numerous applications, as shown in Figure 2. Particularly, the role of GAI in networking is tremendously practical, and it can transform mobile network management by diversifying services and applications [3]. With GAI, network operators can optimize configurations, test new applications, and explore innovative use cases more effectively.

GAI can help network design by simulating different configurations and traffic patterns. Network operators can create synthetic datasets to see how different setups perform under different conditions. This helps in identifying the optimal configuration. It can also help network security as GAI can build simulated attack patterns that can better train Intrusion Detection Systems (IDS) [4].

In addition to that, GAI can be of major help in traffic control. GAI can also predict traffic patterns based on historical data and then use that information for resource distribution. This ability helps to reduce the congestion and improves service quality in general. GAI allows the dynamic adaptation of the bandwidth allocation during peak usage times to guarantee necessary resources for key applications so that they have lower latency and better user experience.

As we explore this research deeper, it is crucial to think of how GAI can essentially affect the future of network management. Undoubtedly, we are increasingly dependent on digital services; having an adaptive and advanced network infrastructure is even more critical. The rationale for integrating GAI with networking is not only for the sake of operational efficiencies. But it also provides users with a better experience with diverse applications.

This study intends to provide a comprehensive analysis of Generative AI applications in new network technologies.

It explores the options and threats of combining GAI with networking. For this paper to achieve its goal, it first maps out the key studies and insights from existing research works. Then, it shows a detailed comparison and overview of different architectures and models and their results related to specific applications such as smart cities, trust management, cybersecurity, image synthesis, etc. This paper is organized as follows: Section II reviews the evolution of wireless networks toward 6G and presents the research methodology. Section III discusses the applications of Generative AI in next-gen network technologies with a comparative review of several research papers. Section IV presents relevant Challenges in the adoption of GAI in Networking. The conclusions and implications for future research are presented in Section V.

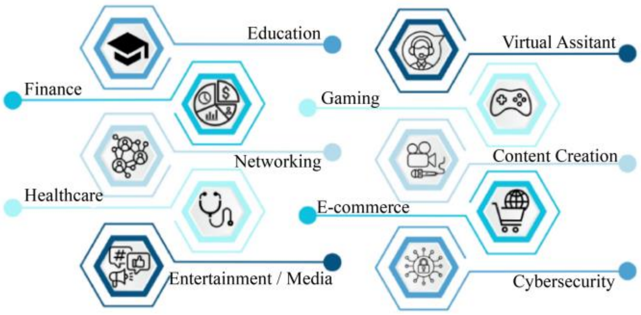


Fig. 2 Applications for generative AI

2. Network Evolution

Wireless network evolution has been driven primarily by technological innovation and the need for faster internet from data intensive applications. The demand for higher data rates, lower latency, and improved resource utilization is obvious from entertainment to commercial industries. The requirement has fundamentally changed how we access information, communicate, and utilize the network. Over the years, advancements in network architecture, spectrum management, and signal processing have taken wireless communication from basic voice transmission to complex and data-centric applications. As illustrated in Figure 3, each generation of wireless technology, from 1G to the lightning-fast 5G and the upcoming 6G, built on both the successes and limitations of its predecessors with increased capacity and speed.

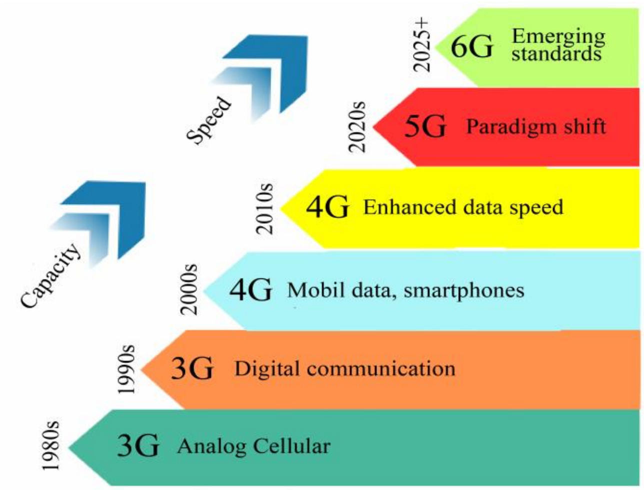


Fig. 3 The evolution of mobile communication from 1G to 6G

2.1. 1G-4G Network Technologies

Figure 4 shows an overview of the technologies used in each generation of mobile networks. Mobile communication started with the first-generation wireless network called the first generation (1G). The networks were analog-based, meaning they allowed users to talk on the phone via radio waves. 1G was limited and not secured enough, and interference was prevalent most of the time. As telecommunication demand grew, the second generation (2G) came. This transition was followed by an increased range of security options, better data capacity and support for text messaging. Powerful approaches to telecommunication were built on top of technologies such as Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA), which eventually led to a data-oriented paradigm shift. Then, the arrival of the 3rd generation (3G) was a major milestone, delivering far more data rates and allowing support for multimedia applications.

Later, technologies like Universal Mobile Telecommunication System (UMTS) and CDMA2000 enabled mobile internet and video streaming, which started the real evolution in the communication network [5]. Then, the fourth generation (4G) provided higher data rates, lower latency, and higher spectral efficiency, enabling High-Definition (HD) video streaming, online gaming, and other data-intensive applications. 4G has first enabled the widespread implementation of cloud computing and real-time data exchange for the Internet of Things (IoT). This technology facilitated the growth of more connected devices and smart systems. However, it was eventually overtaken by 5G technology, which introduced even faster speeds, lower latency, and the capability to support advanced use cases through various industries.

2.2. 5G and 6G Technologies

5G is easier and cheaper to deploy, and it has become a potential cause in the development of smart home electronics for the Industrial Internet of Things (IIoT). It can connect up to a million devices per square kilometer, from battery-powered small sensors to self-driving cars [6]. All these applications are expected to be handled by the same network. Its cases cover enhanced mobile broadband to ultra reliable low latency communication, M2M (machine to machine) communication and big data analysis. With millimeter waves, massive Multiple-Input Multiple-Output (MIMO) and beamforming, among other advanced technologies, 5G promises a higher data rate than we have seen before.

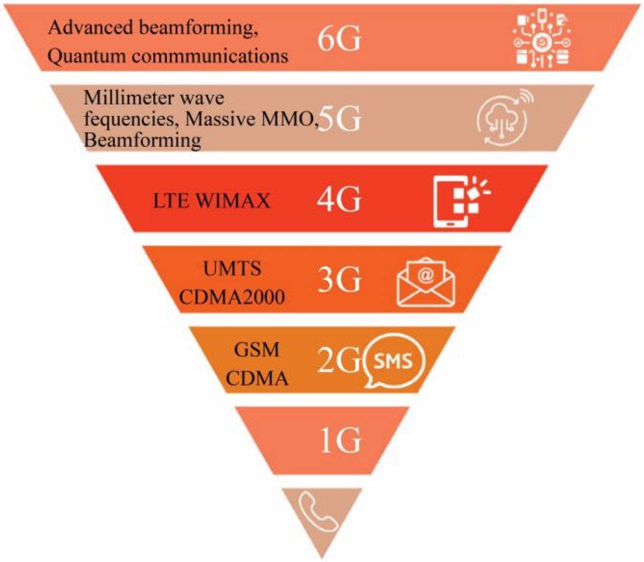


Fig. 4 Technologies used in 1G-6G

However, it also increases the complexity in dataflow between end and intermediary devices, and end-to-end devices, and new network architecture to manage such an extreme amount of data. Research and development on 6G is already underway, in anticipation of where we will be headed. Figure 5 shows the capabilities chart between 5G and 6G. These next-generation technologies, such as 6G and 7G with satellite communication, aim to provide unimaginable possibilities for speed, latency and reliability while merging the physical world into a digital world. To satisfy the requirements of such a digital era, many key requirements need to be addressed in the next-generation wireless network.

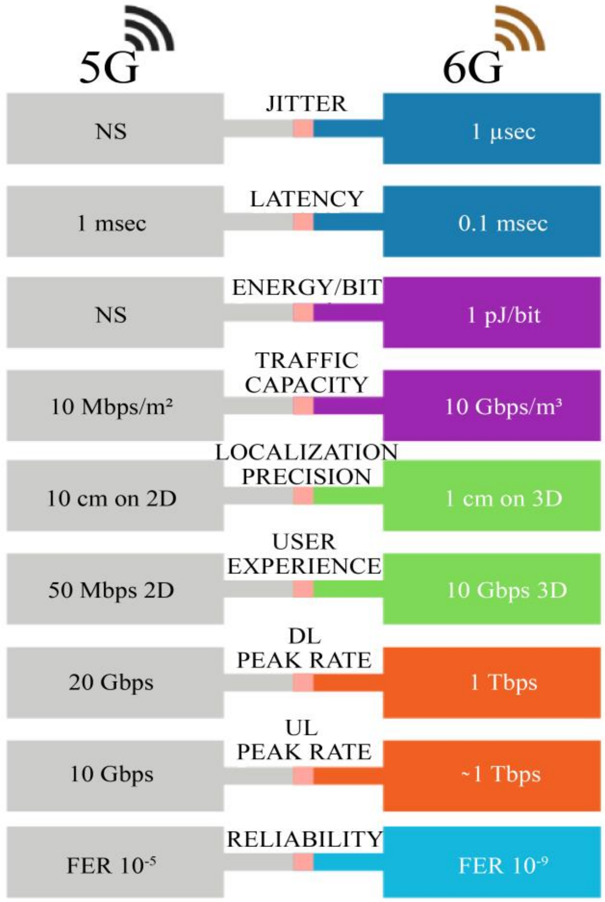


Fig. 5 5G vs. 6G Capabilities chart

One of the critical requirements is ultra-high data rates. Future networks must offer data rates that are many times faster than what current state-of-the-art systems can support. This core feature must be unlocked for things like holographic communication, high-fidelity video streaming and immersive virtual realities [7]. Ultra-low latency communication is one of the other key requirements for some applications such as live control systems, self-driving cars, etc. Such critical applications can only tolerate latency in the order of 1 millisecond or even lower. Maintaining this response time is of the essence for the user's safety and reliable operation of these systems.

With the increasing complexity of networks, the requirement for autonomous decisions along with intelligence and self-optimization becomes mandatory. These capabilities enable networks to self-configure and manage themselves efficiently. It helps to adapt networks among dynamically changing conditions and user demands without requiring constant human intervention. In addition, energy efficiency, reliability and massive connectivity are also becoming important for the next generation networks [8]. Most importantly, wireless communication technologies must be built in such a way that they are environmentally friendly while providing consistent, continuous service.

2.3. Research Methodology

Research on wireless networks usually combines theoretical work, simulations and experiments. A solid foundation based on such research is essential for understanding the key principles and limitations of wireless communication systems. From theoretical models, researchers can look for how the various factors affect the performance of networks. Simulation studies are useful to model different network topologies and system parameters with respect to the variation of different workload scenarios. It could also enable researchers to predict what they will encounter in real world networks. By which they can fine-tune a network and adjust its performance on deployment [9]. In addition, simulations are used to ascertain the influence of novel technologies and methods on the efficiency and effectiveness of networks. On the other hand, experimental evaluations are used to run and authenticate new technologies in live environments. These experiments are needed to verify the theory and simulations of the new technologies. By experimenting with new systems and techniques on actual network environments, researchers can obtain real-time data to judge its performance and observe potential problems.

The research methodology used in research depends primarily on the research questions and scope of technology. For example, a performance study of a 5G network architecture may involve simulations to predict throughput and latency under various traffic conditions. This is followed by laboratory experiments to replicate the findings in real-time [10]. This combination of approaches provides a complete perspective on technology and its potential applications. This paper presents a thorough theoretical analysis and a detailed study of the transformative applications of Generative AI (GAI) within emerging network technologies, including 6G. By examining the intersection of GAI and networking, the paper aims to highlight both the advantages and challenges associated with implementing GAI in wireless communication systems.

3. Generative AI in Emerging Networking

Generative AI is making a deeper impression on various industries, and its influence on network technology is a key part of this transformation. The availability of advanced generative models, including Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs) and autoregressive models, provide the most powerful tools to create realistic, diverse synthetic data within reach.

Table 1. Architecture, Model and Results

Architecture	Years published	Application	Model	Result	Ref
Mobile network optimization in 6G	2024	Smart cities	SRNEMO DMM framework	Improved network performance and reduced delays	[12]
Power optimization for 6G networks	2022	IoT networks	Minimum Distance Scheduling (MDS) Maximum Channel gain scheduling (MCS)	Improved network efficiency	[13]
Holographic communication	2024	Holographic communication in the Metaverse framework	NNs and GAI	Accurate spatial-CSI predictions for enhanced holographic communication	[14]
Intent-based management	2024	Network configuration and management 6G	LLM-centric Intent Lifecycle (LC)	simplify network configuration and management	[15]
6G Wireless Networks	2023	Trust management	Decentralized Public Key Infrastructure (DPKI) Network Functions Virtualization Infrastructure (NFVI)	Improved security and trust	[16]
Security in 6G networks	2025	Cybersecurity for 6G networks	3GPP-based mobile broadband technologies	Mission critical communications	[17]
Security in 6G networks	2023	Anomaly detection using AI	Hybrid EL techniques Support Vector Machines (SVM) Random Forests (RF)	Enhanced detection system	[18]
6G Digital Twins	2023	Use of higher frequency bands	Multi-modal sensing ray tracing DeepSense 6G Deep Verse 6G	Higher data rates multiplexing network gains	[19]
6G Digital Twins	2023	Optimization of 6G network management	Software-Defined Networking (SDN) Digital twin modelling	Zerotouch wireless networks	[20]
Generative Adversarial Networks (GANs)	2021	Image synthesis, super-resolution	StyleGAN	High-quality, realistic images and videos	[21]
Generative Adversarial Networks (GANs)	2025	Image synthesis and data augmentation	Score-Based Diffusion Models	Computational strategies to enhance generative models	[22]
Transformer-based neural network	2025	For SGIVNs aiming to support the high-density and high-mobility requirements of vehicular networks in future 6G communication systems	Deep learning-assisted collision detection and load estimation framework	Enhanced detection performance and reduced computational time compared to existing deep learning-based methods, effectively handling large-scale random-access scenarios in high-dynamic non-terrestrial network environments	[23]
Generative AI techniques	2025	Industrial IoT systems for factory automation and real-time monitoring	Uplink NOMA transmission	Significant improvements in throughput maximization for NOMA-enabled URLLC transmissions, effectively balancing the trade-off between latency and reliability in IIoT communications.	[24]
Autoregressive Models	2025	Autoregressive image generation, where models predict subsequent tokens to generate images	GPT-style Transformer in an autoregressive setting	Experiments on ImageNet demonstrated that models using FlexTok achieved an FID score of less than 2 across 8 to 128 tokens, outperforming previous methods like TiTok and achieving state-of-the-art results with significantly fewer tokens.	[25]
End-to-end AI-driven framework	2025	Network optimization, traffic management, fault detection, and security of 6G networks	Cross-domain AI collaboration, native computing, and native security mechanisms	Strategic integration of AI into the structural and operational aspects of 6G networks to realize the technology’s full potential.	[26]

With this new feature, we can explore the frontiers of research, development and optimization in network technologies, giving researchers and engineers an edge to solve complex problems and leading to unprecedented performance and efficiency in future wireless networks [11]. Generative AI affects different layers across the communication network, from the physical to the application layer, as shown in Figure 6. Table 1 summarizes the architecture, its model, application and results of various research works. It helps us to realize training models developed recently with their network architecture and how they contribute to numerous sectors of communication networking, such as smart cities, holographic communication, network management, trust management, anomaly detection, cybersecurity, etc. The rest of this section will dissect generative AI's major advances over the network stack, specifically in the context of the stack.

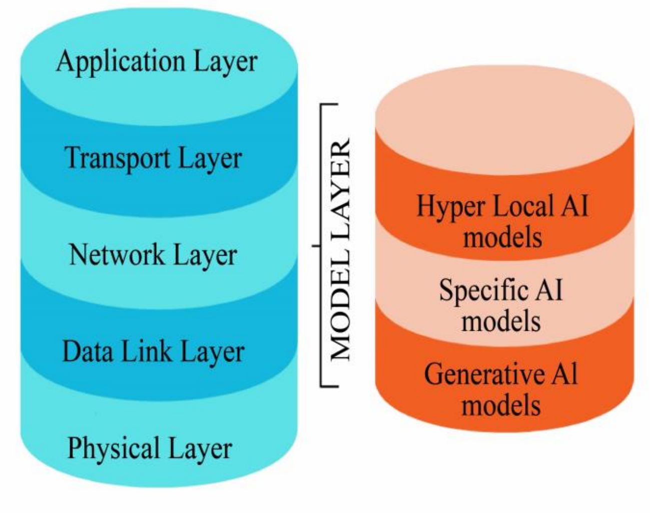


Fig. 6 Network stack with Generative AI applications

3.1. Network Design

The major usage of Generative AI in networking is to design communication networks with more operating efficiency under real-world conditions. Network design via traditional top-down methods and algorithms can be tedious and require intensive manual configuration. This can greatly benefit from using Generative AI models to fine-tune network topologies routing protocols and optimize resource allocation strategies. For instance, GANs can be used to find the best network placement to maximize throughput, minimise delay in data deliveries and reduce energy consumption to a reasonable extent [27]. Learning from existing network data allows these models to identify specific data patterns and configurations that give better results. In complex environments where, traditional optimization can struggle because of unpredictable network dynamics.

Additionally, Generative AI can synthesize network traffic datasets crucial for training models and validating new protocols and algorithms. These realistic traffic datasets enable researchers to prototype and iterate designs in a closed loop before deploying them into live networks. This method minimizes the possibility of error and increases the certainty of reliability in network designs overall. It helps the network design to work as expected in real-world conditions.

3.2. Security and Intrusion Detection

As cyber threats get more advanced, traditional security measures struggle to keep pace. As part of the networking characteristic, it must provide security and integrity to user data. Any unauthorized data breaching needs to be eliminated or avoided completely. GAI can generate synthetic attack patterns and anomalies by using aggressive generative models or training sets, as shown in Figure 7. It plays a critical role in detecting intrusions and improving the Intrusion Detection System (IDS) during training.

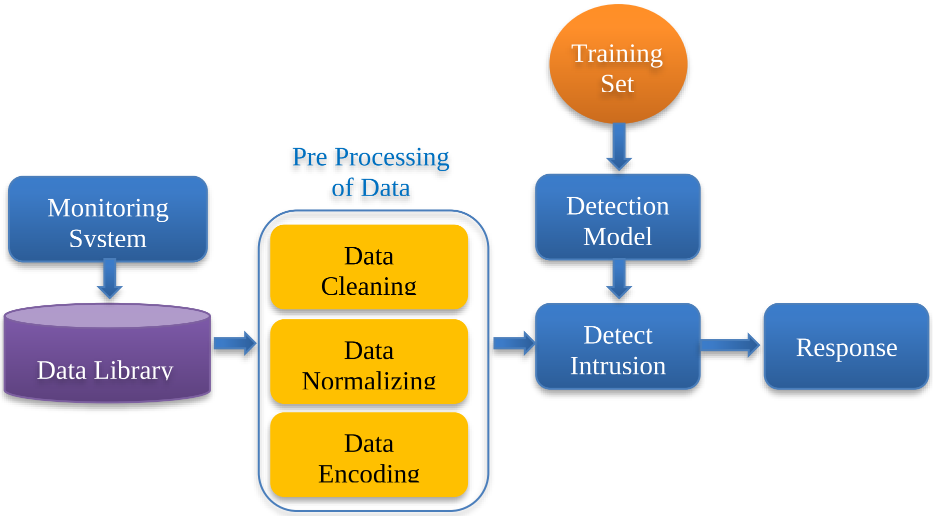


Fig. 7 Intrusion detection system workflow

IDS could further strengthen its ability to identify and respond to real-world threats in a synthetic dataset that mimics many attack styles and adversary patterns. In networking, if a system got trained on synthetic datasets, diverse attack data can be easily identified and spot latent indicators of malicious activity. Lastly, the approach to security is a proactive standpoint for enhanced network security and part of proactive improvement in cybersecurity practices. This exclusive characteristic of Generative AI in modelling adversarial examples and potential threats demonstrates flaws in current security systems [28]. It is practical to simulate various possible attacks within network operations and find weaknesses in their own defence systems. The key point is keeping pace with new vulnerabilities and updating network security protocols automatically through detection datasets. It is important to adapt such technology into a dynamically changing network environment.

3.3. Data Traffic Prediction and Management

Another major advantage of generative AI is data traffic prediction and its management. If there is a failure in some nodes due to heavy data traffic, such as star topologies where thousands of end nodes are connected to a single intermediary node such as a gateway. This kind of scenario should not affect the network performance, and the communication network needs to continuously working despite failures and ensure no loss of service. It means that the network must provide fault and traffic tolerance by re-routing the data packets to the nearest best possible route and continuing to provide the service. For network service to remain responsive, especially during peak hours, understanding traffic patterns is essential to allocate resources [29] efficiently. With generative models, the network operators can allocate resources in advance using historical data on traffic demands.

By accurately predicting traffic patterns, network operators can mitigate congestion and improve overall Quality of Service (QoS). This adds to the network's ability to set priorities and manage data traffic to reduce data loss and delays. If routers receive multiple data packets at the same time, routers make autonomous decisions on how to give the priority and re-route them efficiently. For instance, if a model predicts an increase in traffic for a specific application, that information helps the operators allocate additional bandwidth or adjust routing to accommodate the surge. This proactive management helps maintain service quality and user satisfaction, even during high-demand periods.

Additionally, Generative AI can fabricate realistic network traffic that operators can use to characterize and validate their system across variable load conditions. This feature may be helpful in verifying the network’s scalability without degrading performance when data traffic goes up. Network operators can simulate and evaluate different situations to find out what bottlenecks might exist and move forward optimizing the system.

3.4. Wireless Channel Modelling and Simulation

Generative AI is also key in wireless channel modelling and simulation. Channel models are the foundation of wireless communication networks, they tell us how the signals behave and travel through all kinds of environments to work efficiently. Typically, the exchange of data between different nodes via some form of communication link or transmission medium is also known as Data Flow. The conventional channel models for data flow are typically oversimplified and, therefore, do not reflect the true nature of real-world conditions. It causes inaccuracy in performance measures and channel models, resulting in imperfect network designs.

On the other hand, generative models can be trained on real-world data to produce channel realizations that look just like wireless channels seen in the field. These models provide a means of incorporating datasets where the effect of interference, multipath propagation and environmental variations are considered. Such trustworthiness is very important to create systems that can dynamically accommodate rapidly changing channel conditions [30]. Certainly, it leads to better reliability and efficiency in communication. The channel modelling generation capability allows for better wireless communication systems design. These models are a great place for engineers to run whatever new technology they need and measure its ability against several situations. It supports verifying and fulfilling the requirements of various application sectors. This matters especially as we approach the next iteration in wireless technologies, where channel interaction complexity is scheduled to rise substantially.

3.5. Network Automation

Generative AI can have a big impact on network automation. The more complex the networks are getting, the more important it comes to manage them efficiently. Automated tasks, from configuration management to monitoring and troubleshooting, can all be handled by the Generative models. In traditional networks, each router, switch, and firewall must be configured manually, which is tedious, error-prone, and requires expertise. A Generative model may analyse historical network data and data processing challenges and devise optimized settings based on the changing network conditions [31], as shown in Figure 8. Thus, generative AI engines use learning and pattern recognition techniques to make automated decisions. This self-optimization ensures minimal downtime and improves the overall performance of networked systems.

Through historical data, real-world occurrences are being learned from these AI models. It can make complex everyday tasks much easier and minimise manual intervention dependency. AI models, such as Generative Adversarial Networks (GAN) and Variational Autoencoders (VAEs), can teach normal network behaviours. It supports the identify of network anomaly in real-time, which are typically indicators of cyber-attacks, overloads or hardware failures. The AI models inspect causality in network traffic in real-time, spotting what it perceives as possible problems and mitigating them without human intervention automatically.

Automation is good not only for operational efficiency but also for improving network reliability in general. AI-driven systems can figure out solutions to problems by Analysing historical incidents and failure patterns. They either suggest a fix or implement it directly to minimize downtime and maintenance requirements. This is especially critical in cloud and edge computing, such as distributed infrastructures, which need quick, automated responses to reroute or renew services on the fly.

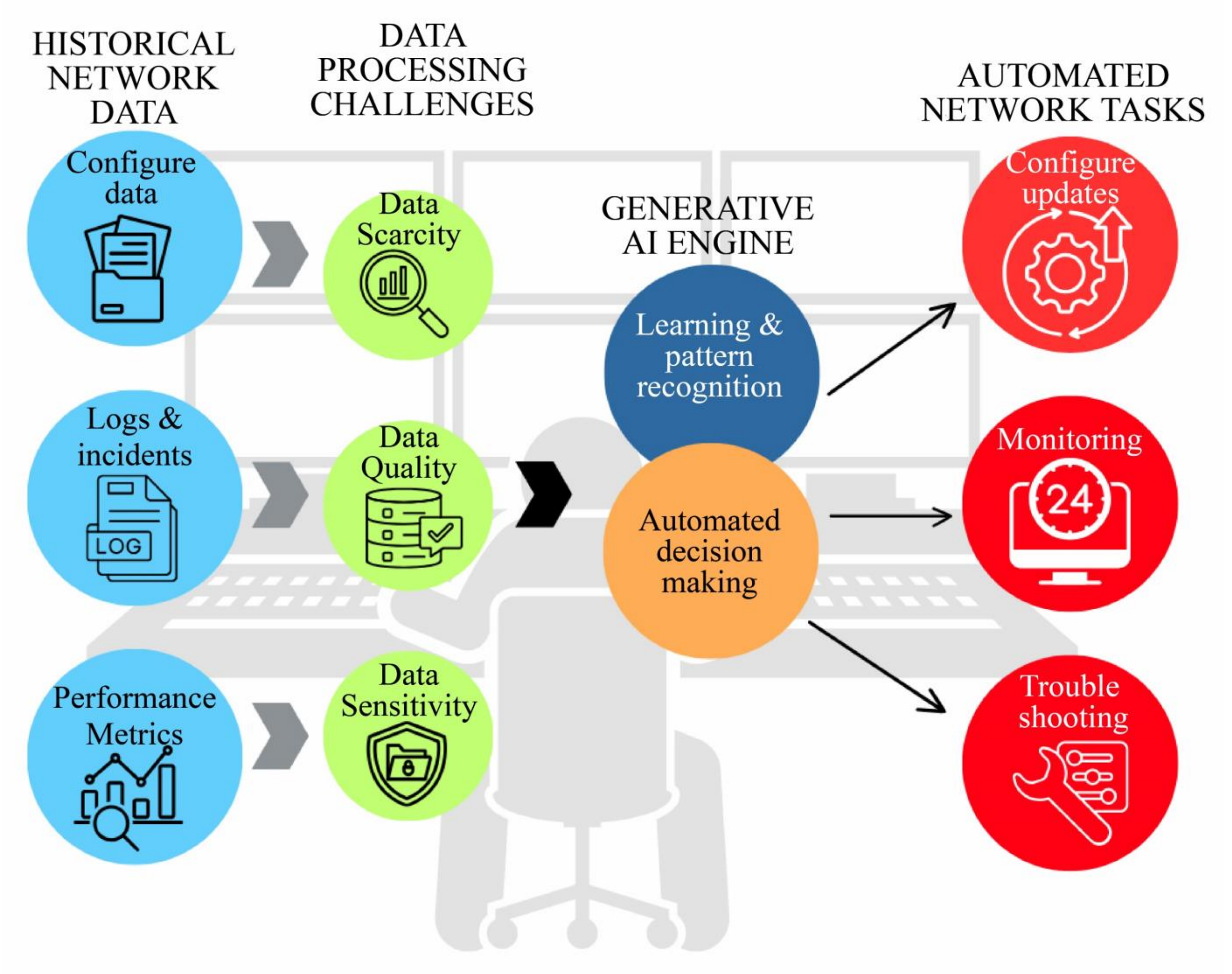


Fig. 8 Historical network data vs Generative AI engine in network automation

The reduced manual interventions and better use of resources help operators do the same. Most importantly, it generates lower operational costs and higher service reliability. A study by Gartner [32] reported that AI-based automation in network operations could reduce operational expenditures by up to 25%, making it a strategic investment for telecom and enterprise networks alike.

3.6. Enhanced User Experience

Generative AI also tends to improve user experience in networked services. Content delivery and allocation of resources can be personalized by generative models through user preference analysis. For instance, a generative model in a streaming service can predict what content a user may pick next and pre-buffer that content to cut load time. Which gives a better user experience and smoother execution [33]. Additionally, generative models can assist in building real-time responsive user interfaces that transform based on user needs. These models learn from user interactions and preferences so they can adapt. Personalization like this is becoming more critical as users pursue the tailoring of their own digital experiences.

3.7. Resource Optimization

Generative AI potentially made large contributions to resource optimization. Generative models are used to find resource optimization opportunities via mining data from diverse sources such as user-level behaviour, traffic patterns and network performance metrics. They could, for example, propose tweaking the bandwidth allocation, server load balancing and cache management to improve efficiency. This optimization is very crucial in environments where resources are constrained or demand changes rapidly. Network operators can optimize resource allocation to improve performance, reduce costs, and improve the end user's experience. While generative models can produce impressive results, they require good and diverse data for training. High-quality training in datasets is essential. Training models on the representational dataset is a necessity to get accurate and optimized performance in real-world situations [34]. Incorporating Generative AI on top of operational network architectures improves current resource allocations. The operators must also adapt their infrastructure and workflows to utilize the full capacity of the advanced AI models.

The scope and versatility of Generative AI applications in new network technologies are almost endless. Generative AI is doing the heavy lifting, from optimizing network design and synthesizing security to predict data traffic in wireless mobile communication systems. With the next generation of 6G network technology, Generative AI and its integration into the networking sector will be at the forefront of addressing the increased complexity. The exploration of generative models in this field can accelerate the performance of the existing networks and may also deliver new possibilities for creative applications.

4. Challenges in Adoption

Generative AI holds immense potential for networking, but it comes with several big tradeoffs and challenges, as shown in Figure 9. This technology needs refinement to be deployed on a scale. The challenges range from data acquisition to data processing and ethical considerations such as privacy, bias, security, trust, model interpretability, computational demands, and more. We must ensure that the introduction of Generative AI into networking does not risk inadvertently fueling new problems that might hinder the benefits [35]. This section goes into these challenges in more detail to give perspectives on what Generative AI challenges exist at the level of deploying them into communication networks.

4.1. User Data Handling by Generative AI

Generative AI models, especially GAN (Generative Adversarial Networks) and VAE (Variational Autoencoder), require a lot of data to operate properly. The difficulty is designing models that can work with mega datasets at the same time ensuring the privacy of individuals and corporations.

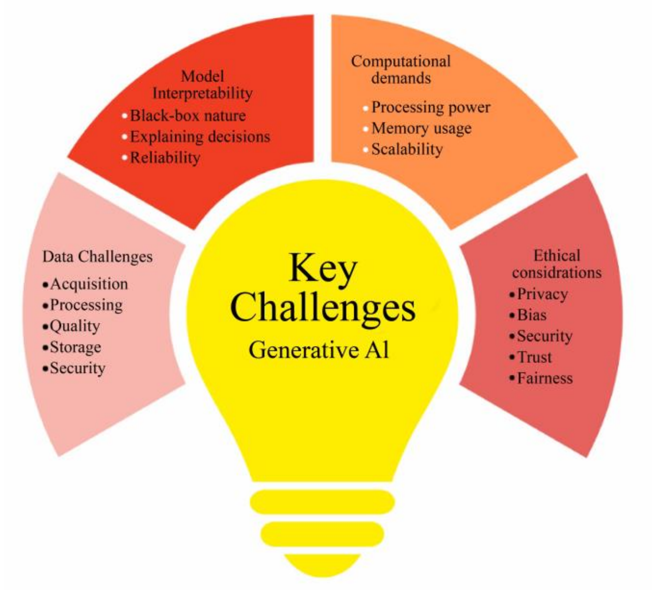


Fig. 9 Challenges in generative AI adoption for networking

4.1.1. Data Scarcity

Network data in real-time is prone to security breaches, which often restrict the ability to train models. It is one of the primary issues while using GAI models. Generative models are designed to predict rare security incidents that need massive historical data of different attack scenarios. Models will not be able to learn details without enough data, and it make incorrect predictions and reactions.

4.1.2. Data Quality

Data quality is another significant challenge. The network itself generates terabytes of data that may be incomplete, inconsistent and duplicated. Although data pre-processing can be employed to tackle the issues to some extent, such processes take a lot of time and resources. It is hard to guarantee good data quality in heterogeneous network environments and hardware configurations. However, data pre-processing is required to achieve high-quality datasets and improve stable generative models.

4.1.3. Data Sensitivity

User activities and network parameters encompassing network data are usually sensitive. This data must be secured against cyber threats and data leaks. User data of Generative AI applications should be secured during the collecting, storing and processing phases. Anonymization techniques need to be good enough, and data governance policies must be stringent to protect the personal information of individuals and organizations. In the absence of such protection, user data and its privacy remain at risk, which can weaken trust in network technologies [36]. Collecting the correct data, augmentation, and creating synthetic data are essential to address these challenges. Effective learning methods allow models to learn from distributed datasets without needing the personally identifiable information of a user. For instance, synthetic network data generation methods enable the statistical properties of raw data to be maintained. Thus, models can generate different scenarios without disclosing private data.

4.2. Deep Learning Models and Model Interpretability

Deep learning-based generative AI models often operate as black boxes, making it difficult to understand how they process data and produce outputs [37]. This lack of interpretability poses several challenges.

4.2.1. Debugging and Enhancement

Debugging and enhancing the accuracy of generative AI models needs an understanding of their decision-making process. When an error is generated, it is essential to identify the underlying cause. However, debugging such problems is impossible without interpretability, making it hard to improve model performance.

4.2.2. Reliability and Compatibility

To deploy network infrastructure, generative AI models must be reliable and robust. Although the models themselves should be trustworthy, they should be able to model the network behavior to create trust. If network operators do not trust generative models to be reliable, they are unlikely to integrate it into real-world systems.

4.2.3. Explainable AI (XAI)

Explainable AI (XAI) includes different techniques to clarify what AI models predict from historical data. To bridge the gap between human comprehension and AI functionality, the interpretability issue needs to be addressed by adopting XAI principles. Much research is still underway to develop visualizing, and explaining the internal representations learned by generative models. The layer-wise data pattern propagation features the predictive patterns that need to be focused on data pattern processing. It can be useful and informative while making autonomous decisions and governing network performance.

4.3. Complexity and Resource Requirements

Executing complex generative models, especially those based on deep learning, is often computationally expensive. This presents challenges for real-time and resource-constrained network environments.

4.3.1. Training time

Conducting end-to-end training of big generative models may take days or weeks and be highly computationally expensive. The extended training time can hinder the development process. In a fast-moving technology world, the drawback of not being able to iterate rapidly on models can be a significant setback.

4.3.2. Inference Latency

Real-time applications, such as network traffic management and intrusion detection, cannot afford high latency in generating outputs. If a generative model takes too long to give results, it is not suitable for use cases where we need quick responses from those models. Other than critical applications, delays in detection can be dangerous in case of an ongoing cyber-attack.

4.3.3. Resource Constraints

End-node deployment of generative models has extra challenges, especially with the Internet of Things (IoT) and its sensor networks. Such environments generally have very limited computational resources, often requiring small model sizes and efficient interpretation algorithms. In such cases, hardware accelerators are needed for deep generative model implication, model compression and distributed systems, which allow them to operate efficiently in resource-constrained settings. Without compromising on performance, specialized hardware for GAI, such as Tensor Processing Units (TPUs), may substantially cut down the data processing time and energy demand. After that, quantization techniques can still reduce the model size without impacting performance. This is key to enabling generative AI on a scale in resource-constrained environments.

4.4. Ethical Considerations and Avoiding Manipulation

Ethical considerations are an extended area of data sensitivity in User Data Handling by Generative AI. As Generative AI is integrated deeper into networking, some serious ethical issues will need careful consideration. It includes data privacy, biased data, misinformation and security risks. If not managed properly, privacy invasions, unfair decision-making, and attacks by malicious actors will easily grow [38]. Adopting responsible AI requires strong data governance, fairness of model training and the right security to minimize potential risks while maximizing the gains of AI in networking.

4.4.1. Data Privacy

The capacity to train generative models in networks operated by untrustworthy sources arises data privacy issues for training data. Unfortunately, these models would be easily susceptible to leaking users' personal information to malicious entities. Data privacy requires robust anonymization techniques such as differential privacy and homomorphic encryption in addition to Standard Operating Procedures for ethical data handling. Novel and improved dataset-learning algorithms are needed to mitigate the risk. It allows AI models to be trained on data hosted at its source without exposing the user's raw data. Therefore, government and privacy organizations and network service providers must start placing greater value and investment in privacy frameworks that must comply with regulations such as the General Data Protection Regulation (GDPR) - EU and California Consumer Privacy Act (CCPA) to protect personal data.

4.4.2. Bias and Fairness

Bias in generative models usually originates from imbalanced datasets in certain network scenarios or demographic groups that are not represented equally. This creates trouble in the trustworthiness of networking, where biased models might lead to results that are unfair for users, impacting aspects of networking security [39]. Addressing these in practice requires the adoption of rigorous data and models. Diversity and representation of training data can also help in preventing bias in generative AI applications. Algorithmic debiasing, adversarial training and fairness-aware learning models can be used to identify and mitigate these biases to obtain a fairer and more robust AI-driven networking solution.

4.4.3. Manipulation and Security Risks

There are risks of misinformation and manipulation due to Generative AI creating very convincing but entirely fabricated network traffic patterns. Malicious actors could exploit this capability to generate fake attack patterns to confuse and create security breaches. It is very important to prevent such misuse, and solutions need to focus on detecting such misinformation algorithmically while ensuring the ethical use of AI technologies.

Generative models are vulnerable to adversarial attacks. Because these attacks can intentionally distort input data, change their outputs, or leak sensitive information. They take advantage of model flaws, backdoor triggers or training-set manipulation, which may wrongly classify network traffic and allow unauthorized data reads. The vulnerability is more dangerous in network security because an adversarial attack could bypass Intrusion Detection Systems (IDS) and permit automated phishing attacks [40]. These attacks can produce deep fake network traffic to mask malicious network traffic.

To mitigate these threats, it is crucial to have ethical conduct and a regulatory framework for how Generative AI is being executed. In addition, stronger adversarial defenses such as adversarial training, differential privacy, and homomorphic encryption can be subsequently used to fortify models against security threats. AI-powered networks need more improved security features. This can be achieved by embedding zero-trust architectures, anomaly detection systems and AI-enabled security policies. The Adoption of Generative AI in networking is multi-dimensional and hard. This is critical for the integration of Generative AI into network infrastructures, from data security explainable AI models to scalability, speed and computation efficiency. As the discipline progresses, ongoing research in an interdisciplinary approach and implementation of common security protocols will be necessary to keep these risks low relative to the upside afforded by AI-driven networking.

4.5. Discussions and Future Directions

In the growth of communication engineering and technology, the potential of applied Generative AI (GAI), particularly in networking, is admirable and promising. Research and development efforts are keeping pace with the forthcoming generation of generative AI capable of being embedded across networking applications. This integration could likely result in enhanced network performance with improved security and automated data management.

Generative AI can significantly enhance network security. Simulating attacks closer to actual attack flows can help improve the training for Intrusion Detection Systems and Intrusion Prevention Systems. This helps to detect and counter the probable threats [41] instantly. Additionally, GAI can create realistic patterns to persuade attackers, allowing organizations to study their methods and strengthen defenses. While numerous sophisticated cyber threats are emerging day by day, AI security mechanisms need to scale, monitor networks and proactively predict what cyber-attack may come next. The complexity of wireless networks highlights the importance of Generative AI. Through generative AI, network resources can be allocated dynamically, allowing for full utilization of throughput and no interference. In dense areas, it can process live data for real-time decisions to give optimal service. This is central for high-quality networking with changing demand. Networking is being reshaped through the integration of emerging technologies such as generative AI, edge computing, blockchain and the Internet of Things [42]. GAI can leverage synthetic data to teach edge IoT devices themselves, minimising the use of gigantic cloud-based datasets and improving response times. Since edge devices perform data processing locally, they can be more autonomous.

As generative models become more advanced, they are also becoming easier to use. These advances will likely help with the further adoption of GAI in networking, enabling more organizations to use its benefits. The normal progression of AI in networking combined with emerging technologies will result in major network formation, management, and security breakthroughs. To fully realize the potential of Generative AI in networking, it is crucial to address deployment challenges. The use of GAI responsibly and ethically is essential to benefit society. Ongoing work is needed to establish best practices for the ethical application of GAI in networking. Generative AI holds hopeful progress for the future of networking. That its functions in security enhancement and resource management lead to it as a key element for network solutions. With research and ethics to evolve, it is expected to move towards a transformative era in networking enabled by Generative AI.

5. Conclusion

The embedding of Generative AI in current networking solutions is a network paradigm shift. It is about designing a network, optimising operations and secure data management. This technology could enable network architectures to manage all by themselves for improved operational efficiency, security and self-configurability. Obstacles on the path to this vision are quite substantial, such as data privacy, model interpretability, computational efficiency and ethical issues.

The biggest challenge at the top is appropriately collecting and processing large datasets with strong privacy constraints. As the usage of AI-enabled insights grows, powerful federated learning approaches, homomorphic encryption, and differential privacy will be required to protect user data. Eventually, model interpretability and explainability should be enhanced to achieve trust and transparency in AI-driven decision-making, especially for critical applications. From a technical standpoint, the heavy computations of generative models require hardware accelerators to be improved and advanced, energy-efficient AI architectures, as well as training algorithms. To simplify future experiments, research should shift towards lightweight generative models, knowledge distillation approaches and the use of AI for resource management, allowing real-time network adaptation to be more feasible. It is also important to consider bias mitigation strategies and adversarial robustness methods in the development so that unintended security issues do not go unnoticed. GAI can drastically minimize latency and optimise security and resource usage in unpredictable network environments. This can be achieved by merging emerging technologies such as edge computing, blockchain-based security, and AI-based threat intelligence with GAI. Moving forward, we will need the ongoing efforts of academia, industry, and policymakers to collectively create standard guidelines for deploying ethical AI in the networking sector as this field matures. The solutions to the challenges mentioned in this paper will enable GAI-driven networks' full potential and build a more intelligent, stable and inter-connected digital future.

6. Conflicts of Interest

Regarding the publication of this article, the author has no conflict of interest to report. The study was carried out without any vested interests in the authors, personnel, or financial gain that may influence the study's findings, conclusion, or recommendations. No sources were given preference over others, and the data governance models presented in this paper result from a fair analysis of literature and current practices.

7. Funding Statement

This research did not receive any special grants from any funding body. The publication relevant fee is supported by the Institute of Engineering at Østfold University College. The author performed the primary research without any sponsor’s financial contributions from various organizations, commercial entities, or governmental agencies. The authors also take full responsibility for designing, conducting, and analyzing the research. Every claim and suggestion in this paper stems from the literature and a critical analysis of existing data governance frameworks.

8. Acknowledgments

The author acknowledges all the reviewers and the editor for their fruitful reviews and time.

References

[1] Yingchi Mao et al., “Artificial Intelligence in Mobile Communication: A Survey,” *IOP Conference Series: Materials Science and Engineering, International Conference on Science in Engineering and Technology*, Palu, Indonesia, vol. 1212, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mohammad Al-Quraan et al., “Edge-Native Intelligence for 6G Communications Driven by Federated Learning: A Survey of Trends and Challenges,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 7, no. 3, pp. 957-979, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Zhenyu Tao et al., “Wireless Network Digital Twin for 6G: Generative AI as a Key Enabler,” *IEEE Wireless Communications*, vol. 31, no. 4, pp. 24-31, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Dure Adan Ammara, Jianguo Ding, and Kurt Tutschku, “Synthetic Data Generation in Cybersecurity: A Comparative Analysis,” *arXiv*, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Lane Tom, “The Evolution of Mobile Networks from 1G to 6G,” *Journal of Telecommunication System and Management*, vol. 13, no. 3, pp. 1-2, 2024. [Publisher Link]

[6] Georgios Gkagkas et al., “The Advantage of the 5G Network for Enhancing the Internet of Things and the Evolution of the 6G Network,” *Sensors*, vol. 24, no. 8, pp. 1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Arjun Singh et al., “Wavefront Engineering: Realizing Efficient Terahertz Band Communications in 6G and Beyond,” *IEEE Wireless Communications*, vol. 30, no. 6, pp. 50-58, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Shah Zeb et al., “Industrial Digital Twins at the Nexus of NextG Wireless Networks and Computational Intelligence: A Survey,” *Journal of Network and Computer Applications*, vol. 200, pp. 1-23, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Adaramola Ojo Jayeola, and J.R. Olasina, “Network Model Analysis in OPNET Simulation,” *International Journal of Engineering and Applied Sciences and Technology*, vol. 5, no. 1, pp. 47-51, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Hamed Ahmadi et al., “Networked Twins and Twins of Networks: An Overview on the Relationship between Digital Twins and 6G,” *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 154-160, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Raha Vafaei, Pioneering the Future of Radar Systems and Wireless Communications Optimization with Synthetic Data on Demand, Ansys, 2024. [Online]. Available: https://www.ansys.com/blog/pioneering-future-radar-systems-wireless-communications/

[12] Shayla Islam et al., “Mobile Networks toward 5G/6G: Network Architecture, Opportunities and Challenges in Smart City,” *IEEE Open Journal of the Communications Society*, vol. 6, pp. 3082-3093, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ashu Taneja et al., “Power Optimization Model for Energy Sustainability in 6G Wireless Networks,” *Sustainability*, vol. 14, no. 12, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Alexey V. Shvetsov, and Saeed Hamood Alsamhi, “When Holographic Communication Meets Metaverse: Applications, Challenges and Future Trends,” *IEEE Access*, vol. 12, pp. 197488-197515, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Abdelkader Mekrache, Adlen Ksentini, and Christos Verikoukis, “Intent-Based Management of Next-Generation Networks: An LLM-Centric Approach,” *IEEE Network*, vol. 38, no. 5, pp. 29-36, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Yiying Wang et al., “Six-Trust for 6G: Toward a Secure and Trustworthy Future Network,” *IEEE Access*, vol. 11, pp. 107657-107668, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jani Suomalainen et al., “Cybersecurity for Tactical 6G Networks: Threats, Architecture, and Intelligence,” *Future Generation Computer Systems*, vol. 162, pp. 1-17, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mamoon M. Saeed et al., “Anomaly Detection in 6G Networks Using Machine Learning Methods,” *Electronics*, vol. 12, no. 15, pp. 1-28, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ahmed Alkhateeb, Shuaifeng Jiang, and Gouranga Charan, “Real-Time Digital Twins: Vision and Research Directions for 6G and Beyond,” *IEEE Communications Magazine*, vol. 61, no. 11, pp. 128-134, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Fahad Alaklabi et al., *Digital Twins for Resilient and Reliable 6G Networks*, IET Digital Twins for 6G: Fundamental Theory, Technology and Applications, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Sungmin Hong et al., “3D-StyleGAN: A Style-Based Generative Adversarial Network for Generative Modeling of Three-Dimensional Medical Images,” *Deep Generative Models, and Data Augmentation, Labelling, and Imperfections*, pp. 24-34, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jan Stanczuk, “*Topics in Deep Generative Modelling: Mathematical and Computational Aspects of Diffusion Models and Generative Adversarial Networks*,” Ph.D. Dissertation, University of Cambridge, pp. 1-284, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Li Zhen et al., “A Lightweight Transformer-Based Collision Detection and Load Estimation Scheme for Massive Random Access in 6G Satellite-Ground Integrated Vehicular Networks,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1-15, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Sekione Reward Jeremiah, David Camacho, and Jong Hyuk Park, “Maximizing throughput in NOMA-Enabled Industrial IoT Network using Digital Twin and Reinforcement Learning,” *Journal of Advanced Research*, vol. 66, pp. 59-70, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Zexu Li et al., “Evolving Towards Artificial-Intelligence-Driven Sixth-Generation Mobile Networks: An End-to-End Framework, Key Technologies, and Opportunities,” *Applied Sciences*, vol. 15, no. 6, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Hannah Ruschemeier, “Generative AI and Data Protection,” *Cambridge Forum on AI: Law and Governance*, vol. 1, pp. 1-16, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[27] Lina Bariah et al., “Large Generative AI Models for Telecom: The Next Big Thing?,” *Institute of Electrical and Electronics Engineers*, vol. 62, no. 11, pp. 84-90, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Krishnashree Achuthan et al., “Advancing Cybersecurity and Privacy with Artificial Intelligence: Current Trends and Future Research Directions,” *Frontiers in Big Data*, vol. 7, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Xuwei Xue et al., “Optical Switching Data Center Networks: Understanding Techniques and Challenges,” *Computer Networks and Communications*, vol. 1, no. 2, pp. 272-291, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[30] Yuvraj Singh Ranawat, and Suraj Kumhar, “Performance Improvement of Indoor and Outdoor Channel Models in Wireless Networks,” *International Journal for Research in Applied Science and Engineering Technology*, vol. 7, no. 5, pp. 3019-3034, 2019. [CrossRef] [Publisher Link]

[31] Chaitanya Kumar Kadiyala, Shashikanth Gangarapu, and Sadha Shiva Reddy Chilukoori, “AI-Powered Network Automation: The Next Frontier in Network Management,” *Journal of Advanced Research Engineering and Technology*, vol. 3, no. 1, pp. 223-233, 2024. [Google Scholar] [Publisher Link]

[32] M. Leibovitz Gartner, and A. Lerner, Hype Cycle for Enterprise Networking, Gartner, 2024. [Online]. Available: https://www.gartner.com/en/documents/5500595

[33] Yi Li et al., “Advancing Design with Generative AI: A Case of Automotive Design Process Transformation,” *DRS Conference Proceedings*, Boston, USA, pp. 1-22, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[34] Zhihang Song et al., “Synthetic Datasets for Autonomous Driving: A Survey,” *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 1, pp. 1847-1864, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[35] Thilo Hagendorff, “Mapping the Ethics of Generative AI: A Comprehensive Scoping Review,” *Minds and Machines*, vol. 34, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[36] Lalita Takle, Mihir Sircar, and Advait Tare, "A Survey on Data Privacy Threats and Preservation Techniques," *International Journal of Advanced Research in Computer Science*, vol. 11, no. 2, pp. 57-63, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[37] Sheikh Rabiul Islam et al., "Explainable Artificial Intelligence Approaches: A Survey," *arXiv*, pp. 1-14, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Lubna Luxmi Dhirani et al., "Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review," *Sensors*, vol. 23, no. 3, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[39] Tahsin Alamgir Kheya, Mohamed Reda Bouadjenek, and Sunil Aryal, "The Pursuit of Fairness in Artificial Intelligence Models: A Survey," *arXiv*, pp. 1-37, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[40] João Vitorino, Isabel Praça, and Eva Maia, "Sok: Realistic Adversarial Attacks and Defenses for Intelligent Network Intrusion Detection," *Computers & Security*, vol. 134, pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[41] Kadhir Palani et al., "Impact of AI and Generative AI in transforming Cybersecurity," *Journal of Student Research*, vol. 13, no. 2, pp. 1-12, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[42] Samuel Olaoluwa Folorunsho et al., "Optimizing Network Performance and Quality of Service with AI-Driven Solutions for Future Telecommunications," *International Journal of Frontiers in Engineering and Technology Research*, vol. 7, no. 1, pp. 73-92, 2024. [CrossRef] [Google Scholar] [Publisher Link]