University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)

ISSN: 2714-3627

A Journal of the Faculty of Computing, University of Ibadan, Ibadan, Nigeria

Volume 15 No. 1, September 2025

journals.ui.edu.ng/uijslictr
http://uijslictr.org.ng/
uijslictr@gmail.com

University of Ibadan
Journal of Science and Logics in ICT Research

Practical Applications of Network Management Tools in Emerging Technologies

[1]Olokun, T., [2]Yoyinoye, B., [3] Fatai, A. M, and [4]John-Dewole, A. T.

[1, 2, 3 & 4] *Department of Information Technology, Lead City University, Ibadan, Nigeria*

[1]olokuntemitope2018@gmail.com, [2]kehindebolaji250@gmail.com, [3]oluwabhayor123@gmail.com, [4]johndewole.temilola@lcu.edu.ng

Abstract
The rapid evolution of emerging technologies—such as the Internet of Things (IoT), edge computing, 5G network slicing, and artificial intelligence (AI)—has significantly reshaped network management practices. As networks become increasingly complex, large-scale, and diverse, traditional approaches relying on manual oversight and static, rule-based systems are no longer sufficient. To address these growing demands, modern network management is shifting toward intelligent, automated solutions capable of real-time analysis, dynamic resource allocation, and improved security. This article examines the practical applications of advanced network management tools, with a particular emphasis on AI-driven monitoring, anomaly detection, automation, and the move toward standardizing network intelligence. Based on recent technological developments from 2019 to 2025, it evaluates how these tools contribute to building more resilient, adaptive, and secure networks. The discussion highlights key advantages, including predictive maintenance, faster fault detection, optimized traffic handling, and proactive threat response. However, it also addresses limitations such as privacy risks, potential algorithmic bias, and integration challenges with legacy systems. Emerging trends such as self-healing networks, federated learning, and intent-based networking are explored as future directions for scalable and intelligent infrastructure. By addressing both the benefits and challenges, this article emphasizes the essential role of AI-enhanced network management in enabling next-generation connectivity.

Keywords: Network Management, IoT, Edge Computing, 5G, AI, Standardization

1.0 Introduction

Computer networks encompass a broad range of technologies, and their main purpose is to enable communication, cooperation, and sharing of information. The operation of these systems mostly depends on the nature of products and services implemented within the systems. The rapid development of networking technologies and the declining cost of hardware as well as software development improvements have extensively transformed computer network management [1]. Networks are nowadays a fundamental component of business corporation in the age of digital transformation, facilitating growing amounts of service delivery and technological innovation. However, with hardware-focused operations and pre-defined infrastructures, traditional network topologies are decreasingly able to provide the necessary performance, flexibility, and reliability that companies need. Modern networks are now more sophisticated, heterogeneous, and scale-intensive than ever before, and it is now a time-consuming and error-prone job to deal with them manually. Human error remains one of the most frequent reasons for network failures [2].

Networks were small and could be manually managed. As connections increased within subnetworks and in broader frameworks such as wide area networks (WANs), it was not feasible and counter-productive to manage them manually. Network management (NM) emerged as the formal remedy to managing complexity, triggered by this issue. NM has never been administration but has played a central role in the delivery of reliability, performance, and responsiveness. For instance, as early as the

Olokun, T., Yoyinoye, B., Fatai, A. M, and John-Dewole A. T. (2025). Practical Applications of Network Management Tools in Emerging Technologies, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, Vol. 15 No. 1, pp. 172 – 182.

1920s, AT&T extended its networks to provide faster and more reliable services during peak usage [3]. The emphasis in NM systems has progressively been on minimizing human involvement in the control loop. A milestone in this evolution came in 2001, when IBM introduced the autonomic computing initiative, which envisioned IT systems that would self-configure, heal, optimize, and defend themselves [4].

As the new era of larger and more complex infrastructures, distributed processing systems, and decentralized services unfolded, the need for network management grew manyfold in organizations. With growth in networks comes instability and inefficiencies, which enhance the risk of failures. Therefore, human-centric approaches alone cannot suffice anymore. Knowledge-driven and automated network management solutions have emerged on top, especially since decentralization of services maximizes the complexity of managing resources that can physically be distant from the network administrators [5]. The recent decade has witnessed such technologies being widely in demand, enabling the operational resilience of large-scale, data-centric, and mission-critical infrastructures.

At the same time, the development of emerging technologies such as Internet of Things (IoT), 5G, Cloud Computing, Edge Computing, Artificial Intelligence (AI), and Blockchain has raised the need for advanced network management solutions. Although these technologies enable innovation and emerging business models, they also introduce unprecedented demands for bandwidth, ultra-low latency, security, and scalability [6]. Traditional management solutions are insufficient. For instance, 5G network slicing requires elastic, on-demand virtualized resources for supporting diversified applications ranging from autonomous vehicles to telemedicine [7]. Similarly, IoT ecosystems require widespread device provisioning, continuous monitoring, and complex security solutions [8].

To manage these issues, network management solutions are increasingly using automation, AI-driven orchestration, predictive analytics, and zero-touch architectures that enable real-time monitoring, proactive anomaly detection, smart resource allocation, and closed-loop automation [9]. However, despite the significant progress, organizations still struggle with interoperability across multi-vendor platforms, limited access to realistic datasets for training AI models, and concerns related to the transparency and accountability of "black-box" models [10].

This paper therefore explores the application of network management tools in emerging technologies in practice, exploring their application within IoT, 5G, Cloud, AI, and Blockchain networks. It highlights the benefits of such tools in enabling efficiency, scalability, and security, and the challenges and future research directions, such as standardization, AI-native automation, and mechanisms for establishing trust in autonomous networks.

2. Related Works

Current network management (NM) systems facilitate functionalities like automation, optimization, orchestration, anomaly detection, and device control. NM solutions have been discussed from various directions in various publications, ranging from IoT and 5G to AI-orchestrated and digital twin–based 6G networks. Bikkasani and Yerabolu [11] explained how deep reinforcement learning can be applied to optimize the resource allocation in 5G network slicing using machine learning methods. In their research, they demonstrated that traffic flow can be dynamically prioritized with negligible human interference, albeit real-time training and scalability are challenges. Sari and Aksu [12] evaluated autonomic IoT network protocols emphasizing self-healing and self-configuration capabilities to reduce human error in distributed systems. Their study found improvement in efficiency enhancements in managing resource-constrained devices but highlighted gaps in which interoperability and standardization do not receive full support in heterogeneous IoT setups.

Benzaid *et al.* [13] introduced the Zero-Touch Network and Service Management (ZSM) based on a strong reliance on AI methods. They demonstrated that it is possible to automate fault restoration as well as configuration but identified security risks as severe barriers. Tariq *et al.* [14] introduced digital twin-based 6G networks for experience-based traffic management. Their approach ensures real-time synchronization between the physical and

virtual state of the network to increase orchestration efficiency. They also encountered computational overhead as the limitation when this approach is applied to large-scale deployments.

Muhammad *et al.* [15] researched Software-Defined Networking (SDN) as a disruptive NM method. The study stressed SDN's centralized control potential, ease of operations, and improved flexibility. Despite such advantages, the study did acknowledge new single-point failure sources and elevated security vulnerabilities. Khan and Han [16] explored 6G network management with swarm UAV integration, focusing on AI and blockchain as scalability, security, and energy efficiency drivers. While effective in dense and emergency scenarios, they admitted that regulatory challenges and interoperability remain to be solved. Abdallah and Prasad [17] presented NetOrch LLM, a network orchestration framework based on large language models (LLMs). The innovation supports network policies and debugging in natural language, reducing technical complexity. Nevertheless, the authors cautioned that heavy reliance on context-free generative AI without validation could pose operational risks.

Finally, trade publications reflect the growing significance of AI-facilitated NM platforms. Deanna [18] noted that AI-based automation would reduce operation costs by up to 40% and increase ROI by 15%. Ritoban [19] ranked LogicMonitor and Auvik as leading network monitoring platforms due to their hybrid monitoring and automated anomaly detection features. However, Telecom Review [20] reported that IT professionals tend to struggle to quantify the effectiveness and reliability of such tools in real-world deployments.

3.1. IoT and Edge Computing

The Internet of Things (IoT) has appeared as one of the most groundbreaking paradigms of contemporary networked systems, which enables billions of things to communicate, process, and exchange data. From industrial automation equipment to smart city sensors, such things generate enormous amounts of real-time data. The traditional cloud-based architectures are not enough to fulfill the latency-sensitive and bandwidth-demanding requirements of IoT applications [21]. Hence, edge computing has been suggested as an adjunct paradigm that pushes computation and data processing closer to the source of data generation.

Edge computing enhances the performance of IoT systems through latency reduction, relief from network traffic, and real-time analysis. For instance, in smart healthcare environments, patient-monitoring IoT sensors can process data on-site at the edge to provide immediate notifications, thereby minimizing cloud-server reliance [22]. Similarly, industrial IoT (IoT) applications leverage edge-supported designs to automate predictive maintenance, improve safety, and maximize production efficacy [23].

The intersection of IoT with edge computing deeply impacts network management (NM) too. Network operators must handle distributed infrastructures characterized by heterogeneous devices, dynamic topologies, and varied quality-of-service (QoS) demands. Modern NM tools increasingly incorporate artificial intelligence (AI) and machine learning (ML) to autonomously monitor and control in such advanced setups [24]. Having the ability to distribute resources dynamically between edge and cloud environments is now an obligatory feature to ensure scalability and resilience, particularly for mission-critical applications.

Challenges remain nonetheless as security vulnerabilities are increased when data is calculated over multiple distributed nodes rather than within centralized systems [25]. Moreover, interoperability among heterogeneous IoT devices and standardization of edge frameworks are still hard open problems hindering extensive-scale deployment. Energy efficiency is another major bottleneck as many IoT devices and edge nodes are resource constrained. Lightweight protocols, energy-efficient orchestration techniques, and blockchain platforms have been proposed in some recent works to address these challenges, yet there is still much to be done to ascertain their feasibility of scalability [26]

.

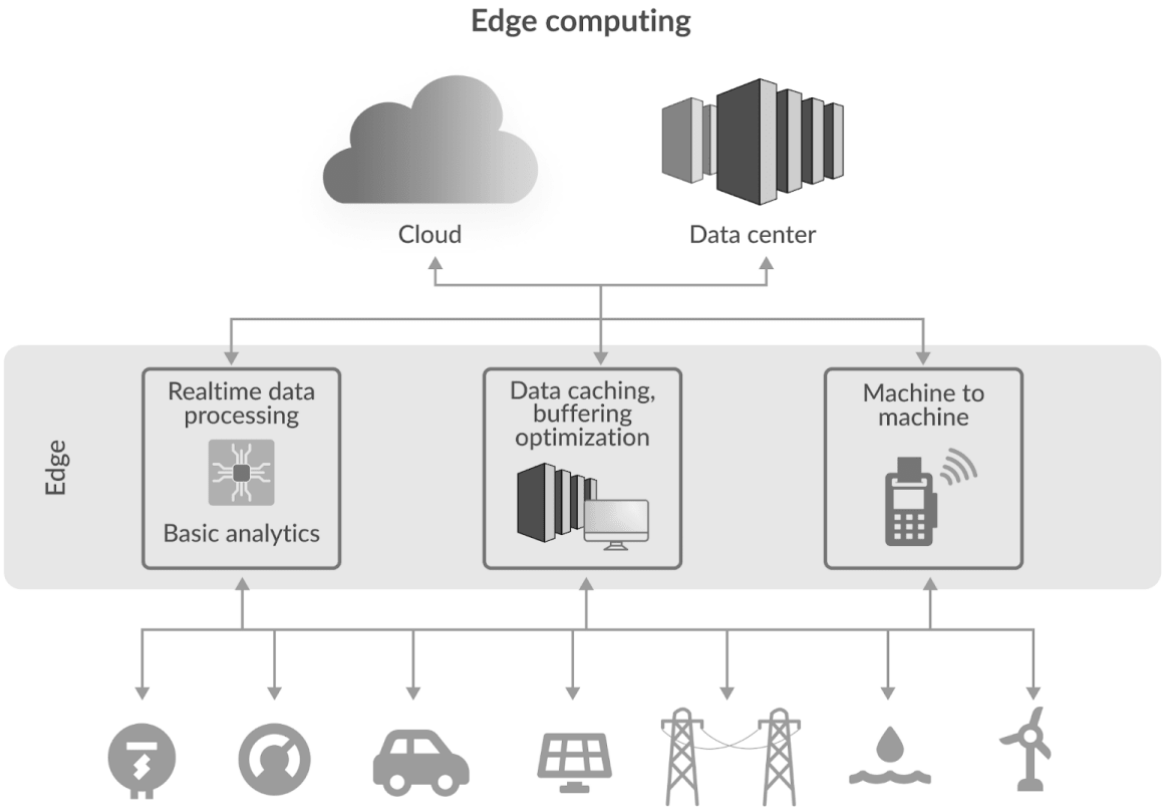

Figure 1: The IoT and Edge Computing
Source: Roman *et al.,* [25]

Overall, IoT and edge computing are a network management and usage revolution. Synergistically, they reduce reliance on centralized platforms while bringing near real-time intelligence to the network edge. With projected breakthroughs like 5G, AI, and digital twins alongside IoT-edge environments, the use of adaptive and autonomous network management systems will expand further.

3.2. 5G Network Slicing and Automation

5G systems target simultaneous support for a wide range of application scenarios and business models (e.g. automotive, utilities, smart cities, high-tech manufacturing) [27]. This future agility is combined with high diversity of demands on network abilities (e.g. security, mobility, policy control functions) and expected performance (e.g. maximum rates of over 10 Gbps, latency below 1 MS with reliability 10−5, 500 km/h mobility target) that cannot be satisfied in most instances by a single network setup. In this regard, the underlying support for network slicing in 5G became a critical prerequisite in order for operators to build and manage customized logical networks (i.e. network slices) with customized functionality, while preserving economies of scale from a shared infrastructure [28]. This is especially relevant to the Radio Access Network (RAN), the most resource- and cost-hungry part of the cellular network and most exposed to enabling network slicing [29].

A network slice can be tailored to provide a particular system behaviour (i.e. slice type) through the deployment of a specific control plane and/or user plane functions to optimally facilitate specific service/applications domains. For instance, a user equipment (UE) for smart metering applications can be supported by a network slice with radio access optimized for very small, infrequent messages without the need to invoke unnecessary features (e.g. no mobility support). Similarly, a network slice can be utilized to provide a particular tenant (i.e. business or organizational body) a particular quantity of guaranteed network resources and isolation with respect to performance from other concurrent slices. For instance, EUs/subscribers of a public safety (PS) organization may be served by a network slice

providing an assured minimum capacity during congestion periods of the network. The necessary capabilities for network slicing support in 5G networks are already specified in the latest 3GPP Release 15 specifications published in June 2018, which include defining identifiers of the network slices, known as Single Network Slice Selection Assistance Information (S-NSSAI and the signalling functions and procedures required to select a network slice between the UEs, the new future RAN (NG-RAN) and the new 5G Core Network (5GC) [30, 31].

From a network point of view, 3GPP standardizes a network slice, denoted by a S-NSSAI, as a particular behaviour offered by a 5G network. Hence, for provisioning of service, UEs are to be registered first to the 5G mobile network, which is addressed based on a Public Land Mobile Network Identifier (PLMNId), and then establish a 5G connectivity service, known as a PDU session, pertaining to a particular S-NSSAI offered in that network. It must be pointed out that, for QoS management, a single or more than one QoS forwarding treatments, known as 5G QoS flows, could be initiated in each PDU session corresponding to the provided S-NSSAI following the 5G QoS model as specified in [30].

In recent years, emphasis has also been put on the allocation and configuration of the NG-RAN resources (e.g. spectrum, gNB functionality) to implement the slices, which are not covered by the specs. On these lines, implementation of RAN slicing has been explored from multiple viewpoints, ranging from use of virtualization techniques and programmable platforms with slice-aware traffic discrimination and protection mechanisms (e.g. see [31, 32, 33]) to dynamic radio resource allocation schemes to slices (e.g. see [34, 35, 36]) and allocation and configuration of the logical/physical resources for end-to-end slice deployment satisfying multiple service requirements (e.g. see [37]).

Actually, in our earlier work [38], we considered the RAN slicing issue for a multi-cell system with regard to how Radio Resource Management (RRM) features can be utilized to share appropriately the radio resources among slices, while in [14] we defined a set of vendor-neutral configuration descriptors that can be used to define the features, policies and resources to be deployed in the radio protocol layers of a NG-RAN node for the realization of simultaneous RAN slices. Again, in the case of the resource allocation problem, mention should be made that several papers have treated situations where more than one operator or

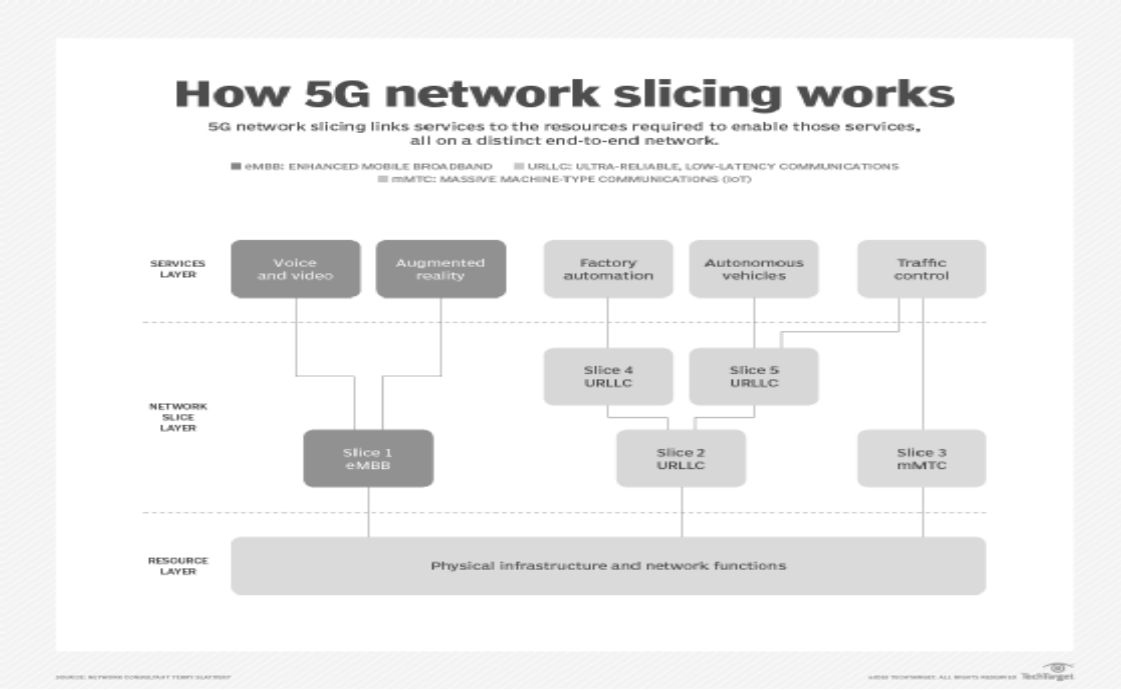

Fig 2: 5G Network Slicing Automation Operations

tenant has been sharing infrastructure over wireless (e.g. see [41, 42]). Additionally, the realization of Service Level Agreements (SLA) through slice-aware Radio Resource Management has been also dealt with [43] as well as introducing trading and pricing methods in the allocation of slice resources to deal with the business aspect [44].

3.3. AI-Based Monitoring and Anomaly Detection

Artificial intelligence (AI) has emerged as a critical enabler of modern network management, particularly in network monitoring and anomaly detection. Traditional network monitoring products employ static rule-based systems that do not fare well in handling the dynamic and complex nature of today's networks. As 5G, Internet of Things (IoT), and edge computing are increasingly being used, the amount and heterogeneity of data traffic require intelligent systems with the capability of real-time analysis and adaptive decision-making. AI-driven monitoring tools address these requirements through the utilization of machine learning (ML) and deep learning (DL) algorithms that have the ability to recognize patterns, detect anomalies, and even forecast impending failures before they escalate to service outages [43].

Machine learning algorithms are at the centre of anomaly detection, discovering baseline patterns of normal network behaviour and identifying deviations. Supervised approaches have been widely applied in intrusion detection systems, with unsupervised methods such as clustering and autoencoders becoming more popular where labelled data sets are not feasible. For example, [44] demonstrated the use of deep learning-based RNNs for anomaly detection in large-scale IoT traffic, with a significant reduction in false positives compared to conventional threshold-based approaches.

AI-based monitoring also facilitates predictive maintenance in network operations. Through the application of time-series forecasting algorithms, network operators can predict congestion, hardware failure, or service degradation. According to [46], AI-based predictive anomaly detection systems can improve mean time to detection (MTTD) and mean time to resolution (MTTR), leading to higher reliability of services and reduced operational costs.

One of the significant developments in this area is the integration of explainable AI (XAI) into anomaly detection systems. As [47] argue, XAI makes anomaly detection decisions more interpretable so that administrators can understand the cause of alerts and thus build trust in AI-driven network management systems. This is particularly critical in mission-critical environments such as healthcare or finance, where transparency and accountability are of utmost importance.

Despite these advantages, AI-based monitoring and anomaly detection are faced with several challenges. Good models require large and representative datasets to train, which may not always be available due to privacy concerns or evolving network conditions. Moreover, adversarial attacks on AI models can compromise detection performance, which raises robustness and security concerns [10]. Active research is ongoing to develop federated learning and privacy-preserving AI solutions to mitigate these limitations.

3.4. Standardizing Network Intelligence

With networks becoming increasingly sophisticated due to the convergence of 5G, IoT, edge computing, and cloud infrastructures, the demand for standardized approaches to network intelligence rises. Standardization ensures interoperability, scalability, and consistency across heterogeneous network infrastructures, which results in different vendors, operators, and systems functioning harmoniously. In the absence of standard methods, the deployment of intelligent network management tools will result in fragmentation, inefficiency, and security threats [48].

Interoperability among multi-vendor environments is one of the primary motivations for network intelligence standardization. Devices and management products from different vendors are used by firms, and vendor-specific solutions can inhibit the timely integration. According to [10], integration of standards such as the Network Management Forum (TM Forum) frameworks and ETSI Zero-touch Network and Service Management (ZSM) has significantly promoted automation, orchestration, and lifecycle management of smart networks. These frameworks facilitate improved interoperability across different

systems by offering common protocols, data models, and management architectures.

Artificial intelligence (AI) and machine learning (ML) are the backbone of network intelligence, but they are being hindered by the absence of standardized datasets, performance metrics, and evaluation procedures. As noted by [39], AI-powered network management requires standardization to offer fairness, reproducibility, and robustness across implementations. Initiatives such as the ITU-T Focus Group on Machine Learning for Future Networks (FG-ML5G) are now stepping up to standardize frameworks and interfaces for integrating AI into network management.

Security and trust are also the motivation behind the push towards standardization. Intelligent network solutions that are heterogenous and non-standardized are likely to have vulnerabilities through unreliable security protocols. [45] argue that standard security frameworks, particularly in AI-based anomaly detection systems, are critical in safeguarding confidential information and adhering to regulations such as GDPR and sectorial regulations.

Furthermore, standardization is central to the creation of 5G and later network slicing. Slices need common service-level agreements (SLAs) in numerous domains. The 3rd Generation Partnership Project (3GPP) has issued specifications for orchestrating and managing slices, opening doors to intelligent, AI-driven slice operations. These standards are not only imperative for ensuring quality of service but also enabling multi-operator slice federation.

4.0. Discussion

The rapid evolution of emerging technologies such as IoT, edge computing, and 5G has profoundly changed the landscape of network management. Manual control-oriented as well as rule-based methods are no longer sufficient to deal with the present heterogeneous, complex, and large-scale networks. Literature studied and future technologies identify the increasing reliance on clever, automated, and AI-driven solutions to ensure resilience, scalability, and efficiency in modern network infrastructures.

Another thread that is common to these technologies is the shift towards proactive as opposed to reactive network control. AI-powered monitoring and anomaly detection, for instance, make predictive maintenance and proactive identification of threats possible, reducing downtime and enhancing quality of service. Similarly, network slicing in 5G networks makes it possible for operators to provide differentiated services and be efficient and reliable, something that would be out of the question with traditional architectures. These advancements reflect an underlying paradigm shift toward autonomic, self-optimizing, and self-healing networks, in line with the autonomic computing vision espoused in earlier decades.

The conversation also indicates the symbiotic relationship between the technologies. IoT and edge computing increase the need for real-time processing and localized decision-making, which can be facilitated by AI-based monitoring systems in analyzing distributed data streams.

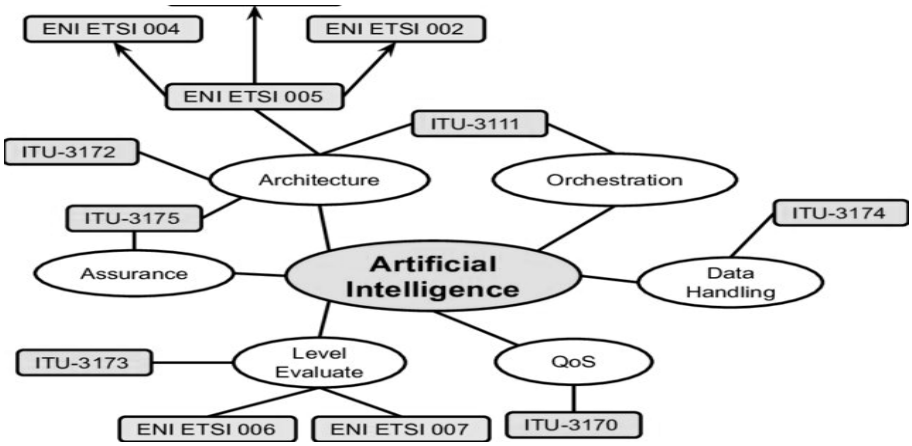

Fig 3: Standardizing Network Intelligence
Source: Ferrús et al., (2018) [39]

At the same time, 5G's low-latency infrastructure provides the foundation needed to accommodate seamless communication between distributed devices and centralized management systems. Together, these technologies create an ecosystem where intelligence at the edge and automation at the core are complementary.

Another critical issue is the role of standardization in enabling interoperability and trust. Without common frameworks, the benefits of AI-driven monitoring, anomaly detection, and network slicing risk being undermined by vendor lock-in, inconsistent implementations, and security vulnerabilities. Standardization initiatives such as ETSI's ZSM, ITU-T's FG-ML5G, and 3GPP's specifications for 5G slicing highlight the global recognition of this challenge. These activities not only enable technical coherence but also establish performance, justice, and accountability standards in intelligent network management systems.

There are, however, several challenges and research issues remaining to be addressed. AI-based anomaly detection performance depends on access to vast, high-quality datasets, yet privacy and security typically limit data availability. In addition, adversarial attacks against machine learning models pose a serious threat to the reliability of networks. Similarly, since 5G network slicing brings flexibility, it introduces complexities in ensuring end-to-end service quality among various operators and vendors. To mitigate these issues, innovation is required in privacy-preserving machine learning, secure AI model deployment, and cross-domain orchestration mechanisms.

In practice, applications of these network management tools have long-range ramifications in the sectors of healthcare, finance, and smart cities. Secure patient monitoring systems are assured through trusted IoT management; AI-based anomaly detection reduces fraud in financial transactions; and intelligent water and energy management systems promote sustainability. These uses emphasize the social value of intelligent network management and place it not just as a tech innovation but also as an enabler of economic growth and public welfare.

5.0. Conclusion

This paper has examined the practical use of network management solutions in response to emerging technologies, including IoT, edge computing, 5G network slicing, AI-based monitoring, and standardizing network intelligence. The analysis recognizes that traditional ways of network management characterized by manual control and static rule-based architectures are not sufficient to handle the scale, complexity, and heterogeneity of modern digital infrastructures. New technologies, powered by artificial intelligence, automation, and global standardization efforts, provide new possibilities for creating resilient, scalable, and flexible networks.

The discussion confirms some key findings. AI-powered monitoring and anomaly detection brought about the paradigm shift toward proactive network management from reactive methods, reducing downtime and enhancing service reliability. Second, IoT and edge computing demand low-latency, distributed intelligence, which is harmonious with centralized automated architecture. Third, automation and 5G slicing enable personalization of high-quality services across multiple application domains from healthcare to smart cities. Finally, standardization processes such as ETSI ZSM, ITU-T FG-ML5G, and 3GPP's slicing frameworks are required for offering interoperability, fairness, and security in the introduction of intelligent network management systems.

Although these developments have been achieved, some of the challenges still exist. The dependence of AI-based systems on representative high-quality data poses issues of data availability, security, and privacy. The possibility of adversarial attacks on machine learning models evokes issues of the reliance and robustness of automated solutions. In addition, interoperability management in multi-vendor and multi-operator environments is also a challenging activity, particularly regarding cross-domain orchestration for 5G slicing.

5.1 Future Research Directions

Future research needs to address a few main areas. First, privacy-enhancing machine learning techniques such as federated learning and homomorphic encryption can mitigate data-sharing challenges while enabling efficient

model training. Second, reliable and explainable AI (XAI) frameworks need to be designed to strengthen trust and explainability in predictive analytics and outlier detection. Third, more work is necessary in developing secure and robust orchestration techniques for 5G and beyond multi-domain, where service-level agreements (SLAs) are guaranteed to be met in heterogeneous settings. Finally, integrating sustainability guidelines in network management e.g., power-aware monitoring and environmentally friendly AI techniques is an urgent field to explore in the light of worldwide climate and energy challenges.

In summary, the convergence of AI, IoT, edge computing, and 5G is transforming the science of network management in a revolutionary way. Through a convergence of intelligent automation and robust standardization, organizations could create networks that are not only optimized and resilient but also smart and future-proof. Continuous collaboration across academia, industry, and standardization organizations will be key to overcoming the challenges facing us today and realizing the full potential of smart network management in the era of digital transformation.

References

[1] Abeck, S. (2009). Network Management know it all. Morgan Kaufmann.

[2] Xu, L., Assem, H., Yahia, I. G. B., Buda, T. S., Martin, A., Gallico, D., ... & Mullins, R. (2016, June). CogNet: Anetwork management architecture featuring cognitive capabilities. In 2016 European Conference on Networks andCommunications (EuCNC) (pp. 325-329). IEEE.

[3] Pras, A., Schonwalder, J., Burgess, M., Festor, O., Perez, G. M., Stadler, R., & Stiller, B. (2007). Key researchchallenges in network management. IEEE communications magazine, 45(10), 104-110.

[4] Benson, T., Akella, A., & Maltz, D. A. (2009, April). Unraveling the complexity of network management.In NSDI (pp. 335-348) *(PDF) A Critical Review of Network Management Tools and Technologies in the Digital Age*. Available from: https://www.researchgate.net/publication/386137272_A_Critical_Review_of_Network_Management_Tools_and_Technologies_in_the_Digital_Age [accessed Sep 11 2025].

[5] Klijn, E. H., Steijn, B., & Edelenbos, J. (2010). The impact of network management on outcomes in governancenetworks. Public administration, 88(4), 1063-1082. *(PDF) A Critical Review of Network Management Tools and Technologies in the Digital Age*. Available from: https://www.researchgate.net/publication/386137272_A_Critical_Review_of_Network_Management_Tools_and_Technologies_in_the_Digital_Age [accessed Sep 11 2025].

[6] Shen, H., Zhang, Y., & Li, W. (2023). Intelligent network management in emerging technologies: A survey of AI-enabled frameworks. *Future Generation Computer Systems, 146*, 81–96. https://doi.org/10.1016/j.future.2023.03.009

[7] Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., & Flinck, H. (2022). ""Network slicing and softwarization: A survey on principles, enabling technologies, and solutions."" ("Figure 2 from Network Slicing and Softwarization: A Survey on ...") ("SoftFloat | Proceedings of the 5th International ACM Mobicom Workshop ...") ("SoftFloat | Proceedings of the 5th International ACM Mobicom Workshop ...") *IEEE Communications Surveys & Tutorials, 24*(1), 1–25. https://doi.org/10.1109/COMST.2021.3105684

[8] Bello, O., Zeadally, S., & Badra, M. (2021). Network management in the Internet of Things: A review and open research challenges. *IEEE Communications Surveys & Tutorials, 23*(2), 904–939. https://doi.org/10.1109/COMST.2020.3047116

[9] Rashed, A., Al-Saba, M., & Hussain, R. (2024). AI-driven orchestration and zero-touch management for 6G and beyond: Opportunities and challenges. *Computer Networks, 240*, 110028. https://doi.org/10.1016/j.comnet.2024.110028

[10] Zhang, L., Wu, J., & Lin, X. (2025). Explainable AI for autonomous network management: Toward trustworthy automation. *Artificial Intelligence Review, 58*(1), 77–101. https://doi.org/10.1007/s10462-025-11108-x

[11] Bikkasani, K., & Yerabolu, K. (2024). Machine learning for network slicing in 5G and beyond. *American Journal of Artificial Intelligence, 8*(2), 68–77. https://www.sciencepg.com/article/10.11648/j.ajai.20240802.14

[12] Sari, A., Fayed, M., & Aksu, A. (2021). Autonomic IoT network protocols: A review. *Information, 12*(8), 292. https://doi.org/10.3390/info12080292

[13] Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G networks: A zero-touch service management vision. *IEEE Network, 34*(6), 186–193. https://doi.org/10.1109/MNET.011.2000154

[14] Tariq, F., Naeem, A., & Poor, H. V. (2022). Digital twin–enabled 6G: Vision, architecture, and future challenges. *arXiv*. https://arxiv.org/abs/2201.04259

[15] Muhammad, N. (2021). Software-defined networking: A transformative approach to modern network management. *International Journal of Computer Networks and Communications*, *13*(5), 45–57. https://doi.org/10.5121/ijcnc.2021.13503

[16] Khan, L. U., Saad, W., Han, Z., & Hong, C. S. (2022). Swarm of UAVs for network management in 6G: Vision, opportunities, and challenges. *arXiv*. https://arxiv.org/abs/2210.03234

[17] Abdallah, A., Hassija, V., Saxena, N., Rathore, S., & Prasad, R. (2024). *NetOrchLLM: Large language model-based orchestration of wireless networks*. arXiv. https://arxiv.org/abs/2412.10107

[18] TechTarget. (2023). AI in network management poses challenges for network pros. *TechTarget Networking*. https://www.techtarget.com/searchnetworking/feature/AI-in-network-management-poses-challenges-for-network-pros

[19] TechRadar. (2025). *LogicMonitor review*. TechRadar Pro. https://www.techradar.com/pro/logicmonitor-review

[20] Telecom Review. (2024). Enhancing network operations efficiency with AI. *Telecom Review*. https://www.telecomreview.com/articles/reports-and-coverage/8999-enhancing-network-operations-efficiency-with-ai

[21] Chiang, M., & Zhang, T. (2020). Fog and IoT: An overview of research opportunities. IEEE Internet of Things Journal, 7(8), 6828–6850. https://doi.org/10.1109/JIOT.2020.2988259

[22] Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R. H., Morrow, M. J., & Polakos, P. A. (2021). A comprehensive survey on fog computing: State-of-the-art and research challenges. ("(PDF) A Comprehensive Survey on Fog Computing: - Amanote") IEEE Communications Surveys & Tutorials, 23(1), 1–42. https://doi.org/10.1109/COMST.2020.3037745

[23] Ahmed, E., Yaqoob, I., Hashem, I. A. T., Khan, I., Ahmed, A. I. A., Imran, M., & Vasilakos, A. V. (2022). The role of edge computing in industrial IoT. IEEE Communications Surveys & Tutorials, 24(1), 22–49. https://doi.org/10.1109/COMST.2021.3105525

[24] Alam, M., Rufino, J., Ferreira, J., Ahmed, S. H., Shah, N., & Chen, Y. (2022). ("Orchestration of Microservices for IoT Using Docker and Edge Computing") Orchestration of microservices for IoT and edge computing: A machine learning perspective. Future Generation Computer Systems, 128, 358–371. https://doi.org/10.1016/j.future.2021.10.010

[25] Roman, R., Lopez, J., & Mambo, M. (2019). Mobile edge computing, Fog et al.: A security and privacy perspective. Sensors, 19(4), 854. https://doi.org/10.3390/s19040854

[26] Zhou, X., Yu, W., Ning, Z., Tang, X., & Wang, F. (2023). Energy-efficient edge intelligence for IoT applications: A blockchain-based framework. IEEE Transactions on Industrial Informatics, 19(3), 2789–2800. https://doi.org/10.1109/TII.2022.3195887

[27] NGMN Alliance, 5G White Paper, February 2015

[28] 3GPP TR 22.864: Feasibility study on new services and markets technology enablers - network operation; stage 1 (release 15), September 2016

[29] Rost P. et al., in *IEEE Communications Magazine, vol. 55, no. 5*. Network slicing to enable scalability and flexibility in 5G mobile networks (2017), pp. 72–79

[30] 3GPP TS 23.501 V15.3.0, System architecture for the 5G system; stage 2 (release 15), September 2018

[31] 3GPP TS 38.300 V15.3.0, NR; NR and NG-RAN overall description; stage 2 (release 15), September 2018

[32] Costa-Perez X., Swetina J., Guo T., Mahindra R., Rangarajan R., in *IEEE Communications Magazine, vol. 51, no. 7*. Radio access network virtualization for future mobile carrier networks (2013), pp. 27–35

[33] Chang C., Nikaein N., in *IEEE Vehicular Technology Magazine, Vol. 13, No. 4*. Closing in on 5G control apps: enabling multiservice programmability in a disaggregated radio access network (2018), pp. 80–93 ("(PDF) On the automation of RAN slicing provisioning ... - ResearchGate")

[34] Ksentini A., Nikaein N., in *IEEE Communications Magazine, vol. 55, no. 6*. Toward enforcing network slicing on RAN: flexibility and resources abstraction (2017), pp. 102–108

[35] Pateromichelakis E. et al., Service-tailored user-plane design framework and architecture considerations in 5G radio access networks. IEEE Access **5**, 17089–17105 (2017)

[36] Richart M., Baliosian J., Serrat J,. Gorricho J.-L, Resource slicing in virtual wireless networks: a survey. IEEE. Trans. Netw. Service. Manag. **13**(3), 462–466 (2016)

[37] Caballero P., Banchs A., de Veciana G., Costa-Pérez X., Azcorra A., in *IEEE Transactions on Wireless Communications, Vol. 17, No. 10*. Network slicing for guaranteed rate services:

admission control and resource allocation games (2018), pp. 6419–6432

[38] Guan W., Wen X., Wang L, Lu Z., Shen Y, A service-oriented deployment policy of end-to-end network slicing based on complex network theory. IEEE Access **6**, 19691–19701 (2018)

[39] Sallent O., Perez-Romero J., Ferrús R., Agusti R., On radio access network slicing from a radio resource management perspective. IEEE Wirel. Commun., 166–174 (2017)

[40] Ferrús R., Sallent O., Pérez-Romero J, Agustí R., On 5G radio access network slicing: radio interface protocol features and configuration. IEEE Communications Magazine **PP**(99), 2–10, Early access in IEEEXplore (2018)

[41] Lee Y.L., Loo J., Chuah T.C., Wang L, Dynamic network slicing for multitenant heterogeneous cloud radio access networks. IEEE Trans. Wirel. Commun. **17**(4), 2146–2161 (2018)

[42] Caballero P., Banchs A., de Veciana G., Costa-Pérez X, Multi-tenant radio access network slicing: statistical multiplexing of spatial loads. IEEE/ACM Transactions on Networking **25**(5), 3044–3058 (2017)

[43] Khodapanah B., Awada A., Viering I, Oehmann D., Simsek M., Fettweis G.P., in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring), Porto*. Fulfillment of service level agreements via slice-aware radio resource management in 5G networks (2018), pp. 1–6

Akguel O.U., Malanchini I, Suryaprakash V., Capone A., in *GLOBECOM 2017–2017 IEEE Global Communications Conference, Singapore*. Service-aware network slice trading in a shared multi-tenant infrastructure (2017), pp. 1–7

[44] Kim, J., Park, S., & Choi, H. (2022). Deep learning-based recurrent neural networks for anomaly detection in large-scale IoT traffic. *IEEE Internet of Things Journal, 9*(14), 11532–11545. https://doi.org/10.1109/JIOT.2022.3156789

[45] Liu, Y., Chen, Z., & Wang, L. (2023). Predictive anomaly detection in network operations using time-series forecasting. *Journal of Network and Computer Applications, 215*, 103556. https://doi.org/10.1016/j.jnca.2023.103556

[46] Sharma, A., Gupta, R., & Singh, P. (2021). Artificial intelligence techniques for anomaly detection in next-generation networks. *Computer Communications, 180*, 200–212. https://doi.org/10.1016/j.comcom.2021.09.005

[47] Xu, K., & He, Y. (2024). Explainable AI for anomaly detection in mission-critical network systems. *IEEE Transactions on Network and Service Management, 21*(1), 112–124. https://doi.org/10.1109/TNSM.2024.3345678

[48] Bikkasani, K., & Yerabolu, K. (2024). Machine learning for network slicing in 5G and beyond. *American Journal of Artificial Intelligence, 8*(2), 68–77. https://www.sciencepg.com/article/10.11648/j.ajai.20240802.14