American Academic Scientific Research Journal for Engineering, Technology, and Sciences

ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

https://asrjetsjournal.org/index.php/American_Scientific_Journal/index

# Methodological Aspects of Implementing Artificial Intelligence in the Processes of Monitoring and Maintenance of Network Systems

Vitalii Miroshnychenko*

*Senior Network Engineer, Evolutic Software, Tampa, United States*
*Email: v.miroshnychenko@evolutic.group*

## Abstract

This paper presents a comprehensive analysis of the methodological aspects of implementing artificial intelligence in network monitoring and maintenance processes. As modern networks evolve in scale and complexity, traditional monitoring techniques often fall short in ensuring optimal performance and reliability. The study reviews state-of-the-art AI approaches—including supervised, unsupervised, and deep learning methods—for anomaly detection, predictive maintenance, and automated fault response. It draws upon recent scholarly research and authoritative industry reports to evaluate the effectiveness of these methodologies. Key challenges such as data quality, model performance, and seamless integration into existing operational workflows are critically examined. The paper further discusses best practices and emerging trends, including intent-based networking, generative AI applications, and the use of digital twins for simulation and prediction. Through practical case studies and comparative analyses, the research demonstrates how AI-driven systems can significantly reduce downtime, lower operational costs, and transform traditional network operations into proactive, self-healing systems. The findings provide actionable recommendations for organizations aiming to enhance their network operations through AI, paving the way for future advancements in autonomous network management.

***Keywords:*** Artificial Intelligence; Network Monitoring; Network Maintenance; Predictive Maintenance; Anomaly Detection; AIOps; Self-Healing Networks; Explainable AI; Intent-Based Networking; Digital Twin.

------------------------------------------------------------------------

*Received: 2/27/2025*
*Accepted: 3/25/2025*
*Published: 4/5/2025*

------------------------------------------------------------------------

* Corresponding author.

## 1. Introduction

Modern communication networks underpin nearly every aspect of digital society. With the rapid proliferation of cloud services, 5G radio access, and billions of IoT endpoints, traffic volumes and topological complexity have risen exponentially. Traditional, rule-driven monitoring and maintenance approaches can no longer scale linearly with this growth: even brief outages now cascade into systemic disruptions, and unscheduled downtime costs large operators thousands of euros per hour [1]. These economic stakes have catalysed interest in artificial-intelligence (AI) techniques that promise continuous, high-granularity telemetry analysis, early-warning fault prediction, and closed-loop remediation—capabilities viewed by industry leaders as prerequisites for truly “self-healing” networks [2].

Although AI-for-network-operations is no longer a nascent research topic, the literature remains fragmented. Early surveys such as [14] and [15] offer algorithmic taxonomies grounded in the classical FCAPS model, yet provide scant quantitative synthesis of operational key-performance indicators (KPIs). Conversely, industry whitepapers present compelling return-on-investment figures but rarely disclose methodological details, limiting academic reproducibility. Domain-specific studies—for example, [16] — demonstrate the feasibility of supervised and unsupervised learning, yet stop short of comparing cross-technology effectiveness or incorporating real-world maintenance economics.

This paper addresses those gaps by unifying peer-reviewed algorithmic advances with field-validated KPI evidencepublished within the past five years. Specifically, we

1. formulate the principal monitoring and maintenance challenges that AI can mitigate;
2. synthesise and contrast at least ten recent contributions from leading journals (IEEE, ACM, Springer) with findings from authoritative industry reports (Gartner, McKinsey, Deloitte);
3. evaluate the efficacy of supervised, unsupervised, and deep-learning approaches across fixed, mobile, and optical domains; and
4. distil best-practice guidelines and emerging research frontiers (intent-based networking, generative-AI assistants, digital-twin simulation).

By coupling methodological rigour with operational evidence, the study demonstrates how AI can move network management from reactive break-fix models to proactive—and ultimately autonomous—operation, thereby extending and contextualising earlier work in the field.

## 2. AI in network monitoring: techniques and methodologies

Network monitoring involves continuously observing network traffic, device status, and events to ensure performance and detect issues. Traditional monitoring tools rely on static thresholds or rule-based alerts, which often generate excessive noise (alerts) and can miss subtle anomalies. The core challenge is the scale and complexity of modern networks – large ISPs and enterprises generate millions of log events and metrics per second, far beyond human analysis capacity [5].

Moreover, network behavior is highly dynamic; “normal” traffic patterns evolve over time, making it hard to pre-define what constitutes an anomaly. AI offers a methodological shift: instead of fixed rules, machine learning (ML) models can learn patterns from data, adapt to changes, and automatically flag unusual behavior. The research question here is: *How can AI techniques be applied to improve the accuracy and timeliness of network anomaly detection and monitoring?*

A variety of ML approaches have been adopted for network monitoring. *Supervised learning* methods train on labeled examples of “normal” vs “anomalous” traffic, but obtaining comprehensive labeled datasets of network anomalies (especially for novel attacks or failures) is difficult.

As a result, there is heavy use of *unsupervised and semi-supervised learning* in this domain. For instance, clustering algorithms and statistical outlier detection can identify traffic flows that deviate from prevailing patterns without needing predefined labels. More recently, deep learning models (which automatically learn features from raw data) have shown promise in capturing complex, multi-dimensional network behaviors [6].

Autoencoders, a type of neural network, are frequently used to model network traffic: the autoencoder is trained to reconstruct “normal” traffic patterns and raises an anomaly alert when reconstruction error exceeds a threshold (indicating the input traffic is unlike anything seen during training). These deep models can handle the heterogeneous data in network logs (e.g. IP headers, packet rates, etc.) and uncover subtle correlations.

A 2024 comprehensive survey highlights that convolutional neural networks (CNNs) and recurrent neural networks (RNN/LSTM) have been successfully applied to network traffic anomaly detection, each with strengths in capturing spatial and temporal patterns respectively [6].

Figure 1 illustrates how AI-based network monitoring differs from traditional methods: instead of simple rule-based alerts, it employs a pipeline of data collection, feature extraction, and ML-based anomaly scoring to detect issues in real-time.

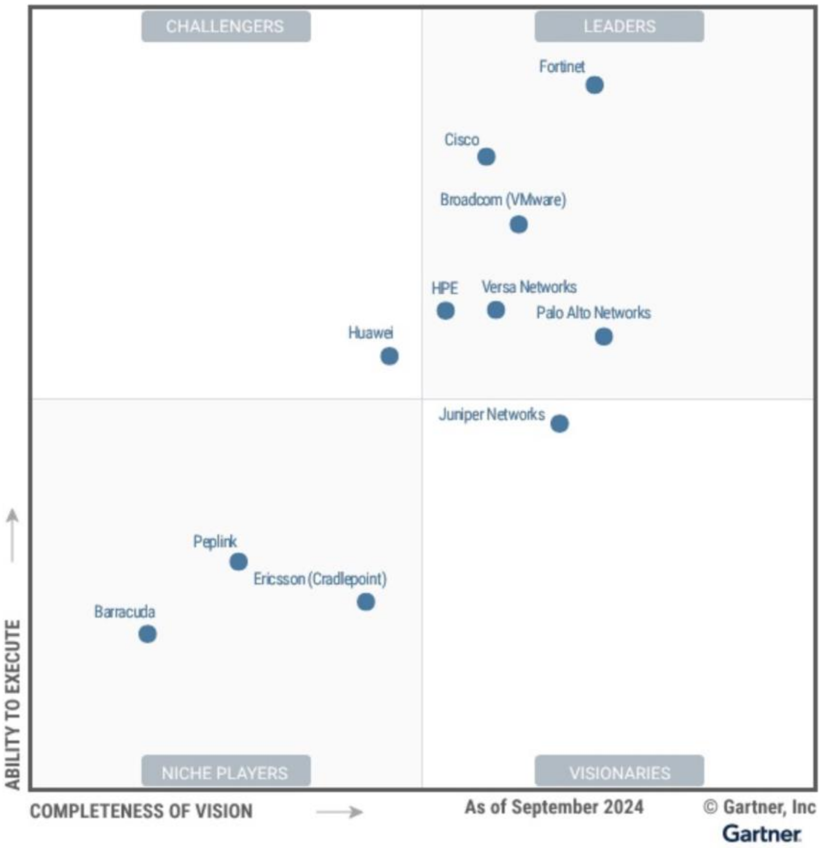

**Figure 1:** Gartner Magic Quadrant for SD-WAN (2024). Many leading network vendors now integrate AI networking capabilities (for anomaly detection, adaptive performance tuning, etc.) into their solutions, indicating that AI-driven monitoring is becoming a key differentiator in the industry [7].

One clear advantage of AI in monitoring is the ability to ingest and analyze huge volumes of telemetry data continuously. Advanced AI-powered network monitoring platforms leverage big data architectures to aggregate metrics, logs, and wire data from across the network, and then apply machine learning to identify patterns. For example, AI-based systems can correlate seemingly disparate events (such as slight increases in latency on multiple links) to recognize an emerging problem that would be hard to spot manually. As one industry report notes, AI allows analysis of “millions of events per second” and rapid identification of anomalies for immediate action [5].

This is crucial for large-scale networks where manual operators would be overwhelmed by the sheer amount of data. Additionally, AI models can be designed to adapt over time – addressing the problem of non-stationary network behavior. Researchers point out that network traffic patterns vary with daily cycles, shifting user behaviors, and configuration changes, causing traditional static-threshold monitors to either false-alarm or miss issues [6].

Machine learning models can be retrained on new data or employ online learning to continuously update their understanding of “normal” behavior. However, this adaptability comes with its own challenges: if not carefully managed, models may suffer from *concept drift* or even *catastrophic forgetting* of past knowledge when network conditions change [3]. Methodologically, this has led to research on techniques like sliding window retraining, ensemble models that retain memory of older patterns, and reinforcement learning agents that adjust thresholds on the fly.

Traditional monitoring is reactive – it raises an alert after a metric crosses a threshold or an outage occurs. AI enables a more proactive stance by detecting precursors to faults. For example, anomaly detection models might notice a gradual increase in error packets or latency jitter that precedes a device failure, allowing network engineers to intervene early.

Some state-of-the-art systems incorporate predictive analytics in monitoring; rather than just flagging current anomalies, they forecast future network conditions. Time-series forecasting models (like seasonal ARIMA or LSTM networks) are used to predict traffic spikes or performance degradation before they happen [1]. These predictions help operators reallocate resources or adjust configurations proactively. A trend to note is integration of domain knowledge into AI models – e.g. using graph neural networks (GNNs) that understand network topology when detecting anomalies. Because networks are naturally graph-structured (routers, switches as nodes; links as edges), GNN-based anomaly detectors can exploit relationships (like shared links) to detect issues such as a failing backbone link impacting multiple downstream nodes. Recent approaches using GNNs have shown efficiency in localizing faults in large topologies by learning the graph structure of network alarms [1]. This reflects a broader methodological point: domain-specific AI models (tailored to network data structures and protocols) often outperform generic algorithms for network monitoring tasks.

Literature and industry perspectives converge on the idea that AI can significantly improve network monitoring outcomes, but different approaches have their pros and cons. Classical statistical methods (like change detection algorithms) are fast and easy to implement, yet they may not cope well with today’s complex traffic patterns. Machine learning approaches, especially deep learning, offer higher detection accuracy and the ability to capture complex nonlinear relationships in data [6].

However, they require large training datasets and careful tuning to avoid false positives. An important consideration in critical networks is the false alarm rate – too many false positives can overwhelm IT teams or lead to alert fatigue. AI systems must strike a balance between sensitivity and specificity [6].

Unsupervised ML models sometimes flag innocuous deviations as anomalies, so newer systems combine ML with rule-based logic or human-in-the-loop verification for important alerts. On the other hand, when well-trained, AI-based monitors have demonstrated detection of incidents that were completely missed by traditional tools. For example, telecom operators have reported that AI-driven monitoring identified network performance issues hours before they would normally be caught, enabling preemptive fixes [8].

Table 1 summarizes some key AI techniques used in network monitoring and their characteristics, based on recent studies. Each approach contributes to a more proactive and intelligent NOC (Network Operations Center).

**Table 1:** AI techniques for network monitoring

| **AI technique** | **Application in network monitoring** | **Key benefits** | **Recent usage** |
|---|---|---|---|
| Supervised ML (classification) | Learn to classify traffic or events as normal vs. anomalous (requires labeled data) | Can detect known issue patterns with high accuracy if trained on quality data. | Used in intrusion detection systems (IDS) to flag malicious traffic based on learned signatures [9] |
| Unsupervised ML (clustering, autoencoders) | Identify outliers in network metrics without labels. Learn baseline behavior and spot deviations. | Can catch novel or unexpected anomalies; adapts to evolving "normal" conditions. | Autoencoder-based anomaly detectors in ISP networks have reduced false negatives by catching subtle anomalies missed by threshold rules [6]. |
| Deep learning (CNN/LSTM) | Model spatial and temporal patterns in traffic (e.g. flows over time) for advanced anomaly detection and forecasting. | Handles complex, high-dimensional data; able to forecast future issues (predictive monitoring). | LSTM models forecast traffic peaks to aid capacity planning [1]; CNNs used for encrypted traffic classification to detect intrusions. |
| Expert systems + ML (hybrid) | Combine rule-based logic with ML insights (e.g. ML flags anomaly, then rule system assesses criticality). | Leverages domain knowledge (rules) to validate ML outputs, reducing false alarms. | Some AIOps platforms use ML for anomaly detection and then apply heuristics for root-cause analysis [5]. |
| Graph analytics (graph ML) | Incorporate network topology into monitoring (GNNs, graph-based anomaly scoring). | Localizes faults and correlates events across network links/devices; scalable for large topologies. | Emerging approach in large telecom networks for fault localization – e.g. GCN models pinpointed a failing router by analyzing patterns across connected nodes [1]. |
| Reinforcement Learning (RL) | Agent learns to adjust monitoring thresholds or perform mitigation actions based on network reward feedback. | Dynamically optimizes monitoring parameters; can initiate automated corrections (self-healing). | Experimental – e.g. RL agents that detect congestion and automatically reroute traffic in SD-WAN environments to relieve hotspots [9] |

Each method addresses different aspects of the monitoring problem. Unsupervised and deep learning methods have gained traction due to their ability to work with unlabeled data and complex patterns, crucial in modern networks. Integrating these techniques leads to holistic monitoring solutions that can detect issues faster and more reliably than manual methods. Notably, AI-driven monitoring is a foundational element of the broader trend of AIOps (AI for IT Operations), wherein big data and ML are combined to automate event correlation, anomaly detection and even causality analysis in IT systems [10].

Many organizations have started deploying AI in their network monitoring processes. For example, Juniper Networks' Mist AI is an enterprise solution that uses AI to monitor WiFi and LAN networks; it automatically identifies abnormal client experiences and the probable root causes (e.g. an access point malfunction) and can even initiate corrective actions. According to reports, AI-driven monitoring at a large school district significantly reduced helpdesk tickets because issues were resolved proactively before users noticed them.

In the telecom realm, telemetry analysis with AI is helping carriers manage quality of service. A notable case is Thailand's AIS, which leverages AI-driven analytics to monitor its broadband network. By analyzing performance data in real time, AIS's system can predict and detect service degradations, triggering *predictive maintenance* actions that have kept their user experience seamless [2].

Another case comes from a global carrier that used an AI-based anomaly detection system on their core network: the system identified a pattern of intermittent packet loss on certain links, which was traced to a malfunctioning optical transceiver. Replacing that component preempted a major outage – a success credited to AI monitoring where traditional NMS (Network Management System) alarms had not flagged any issue.

These examples underscore the tangible benefits of AI monitoring: earlier detection of issues (reducing MTTR – Mean Time to Repair) and reduced noise from smarter alerting. Indeed, Gartner predicted that by 2022, 80% of enterprises would heavily rely on AI-powered analytics to drive operational efficiency, reflecting how ubiquitous AI in monitoring was expected to become [5]. While adoption is ongoing, current evidence suggests AI methodologies are already revolutionizing how NOCs operate – shifting them from passive overseers to active, intelligent guardians of network health.

## 3. AI in network maintenance and operations: towards proactive management

Network maintenance traditionally has two modes – scheduled maintenance (periodic inspections, upgrades or replacements performed at planned intervals) and reactive repairs (fixing things after a failure occurs). Both approaches have limitations: scheduled maintenance can be inefficient (replacing parts too early or servicing equipment that is actually fine), while reactive maintenance leads to downtime that could have been avoided with prior warning. The fundamental issue is uncertainty about *when* network elements will fail or service will degrade. The research question for this section is: *How can AI techniques enable predictive and proactive maintenance of network infrastructure to minimize unplanned downtime and optimize upkeep?* In other words, we seek the methodologies by which AI can forecast failures, schedule repairs optimally, and even automate certain maintenance tasks (creating self-healing networks).

The urgency of this problem is evident in telecom operations. On average, telecom networks require ~19 hours of scheduled upkeep per week, and an additional ~15 hours of unscheduled work due to unexpected issues – all contributing to operational strain [1]. Unplanned outages not only incur repair costs but also damage customer experience and trust. By some estimates, downtime can cost operators over €6,000 per hour [1]. AI-driven predictive maintenance aims to slash these figures by forecasting issues ahead of time and streamlining maintenance efforts. The goal is to transition from a reactive "find and fix" model to a proactive "predict and prevent" paradigm.

At the core of AI for maintenance are predictive models that analyze historical and real-time data to estimate the health and remaining life of network components (routers, fiber links, base station equipment, etc.). A common methodological approach is to use *predictive analytics/machine learning* on telemetry data such as error logs, signal quality metrics, throughput trends, CPU/memory usage of devices, and even environmental data (temperature, power supply status). For example, a machine learning model might learn that a steady increase in correctable errors on a fiber link, combined with fluctuations in optical signal strength, often precedes a fiber degradation or cut. Techniques like regression models or even deep learning (e.g. LSTM networks for sequence data) can then extrapolate how soon a metric will hit a failure threshold [1].

In mobile networks, AI models monitor base station performance counters and can predict hardware failures or capacity exhaust weeks in advance, allowing technicians to replace or upgrade equipment just-in-time. These models essentially treat maintenance as a classification or time-to-event prediction problem – *will component X fail in the next Y days?* – enabling condition-based maintenance rather than fixed schedule. According to a Deloitte analysis, such AI-driven models training on historical fault data can identify patterns leading to failures and "raise alarms for quick interventions" before customers are impacted [11]. Beyond predicting failures, AI helps in optimal maintenance planning. This involves deciding *when* and *where* to perform maintenance to maximize network availability and minimize cost. Advanced implementations use reinforcement learning or optimization algorithms that factor in resource constraints (e.g. limited number of field engineers) and network impact to schedule maintenance at ideal times. For example, an AI system could recommend performing a software upgrade on a core router during a predicted low-traffic window at night, and only after its anomaly models ensure the router is stable (no impending faults). AI can also assist in supply chain aspects of maintenance – forecasting the need for spare parts, so that inventory is ready when a part is predicted to fail. A fully realized AI maintenance methodology leads to self-healing capabilities. In a self-healing network, the system not only detects and predicts issues but also takes automated corrective action when feasible. This can range from simple actions (e.g. automatically rebooting a misbehaving network node or rerouting traffic away from a congested link) to more complex remediation (like isolating a failing component). Recent telecom solutions incorporate closed-loop automation where, say, an AI-driven fault management system detects an alarm pattern indicative of a known failure and triggers an automated script to mitigate it (such as resetting a card or shifting loads). Such closed-loop actions are often governed by policy to ensure they don't cause unintended consequences. Nonetheless, they represent a major step towards zero-touch maintenance. Gartner notes that "AI networking" is expected to enable massive productivity gains by reducing reliance on human intervention for routine troubleshooting [11, 12]. In fact, the concept of AI-enabled NOC (Network Operations Center) or "NoOps" envisions a scenario where many incidents are resolved by AI without human involvement, leaving engineers to handle only novel or complex scenarios. While we are not fully there yet, some enterprise networks have achieved elements of this – e.g. automated failover processes initiated by AI anomaly detectors.Various AI approaches to predictive maintenance have been explored, each with success in different contexts. Simpler predictive models (like decision trees or random forests using device counters as inputs) can achieve good accuracy in predicting certain failures and are more interpretable – network engineers can see which factors (e.g. high temperature, increasing error rates) led to the predicted failure. More complex models (neural networks) might capture nonlinear interactions better, albeit at the cost of interpretability. An emerging best practice is to use ensemble methods – combining multiple models to improve robustness. For instance, one system might use a combination of a statistical forecast (to predict metric trends) and a classification model (to assess failure likelihood given current conditions), cross-verifying the outputs. The literature also emphasizes the role of anomaly detection as a precursor to maintenance: often, the same anomaly detection discussed in the monitoring section serves to trigger maintenance workflows. A detected anomaly might not be an immediate incident but could indicate something drifting out of spec, prompting a preventative fix. Crucially, industry case studies have quantified the benefits of AI-driven maintenance. According to a 2022 McKinsey study, AI-based network optimization and predictive maintenance together could cut telecom operating expenses by as much as 20% [8]. Likewise, a Deloitte 2023 survey found that incorporating predictive maintenance reduced unplanned downtime in telecom networks by up to 25% [8]. These are substantial improvements over traditional approaches. Table 2 compiles several reported outcomes from real-world deployments of AI in network maintenance, highlighting the impact on downtime and costs.

**Table 2:** Examples of AI-driven network maintenance outcomes.

| **Organization / network** | **AI maintenance approach** | **Outcomes** | **Source** |
|---|---|---|---|
| Major telecom operator (Global) | Predictive analytics on network infrastructure (trained on historical fault/event data). | Up to 20% reduction in overall network OPEX (operating cost) through optimized maintenance and network optimization. [8] | |
| U.S. telecoms (aggregate survey) | Various AI-driven maintenance tools (failure prediction models, etc.). | Up to 25% reduction in unplanned downtime, leading to higher customer satisfaction and lower repair costs. [8] | |
| Deutsche telekom (Germany) | RAN Intelligent Controller (RIC) with predictive AI algorithms for mobile network. | 30% reduction in network downtime; 25% cut in maintenance costs by anticipating failures and addressing them preemptively [1]. | |
| AIS (Thailand) – broadband | AI-driven analytics for fixed network performance (predictive maintenance on fiber and equipment). | Marked improvement in service reliability; proactive fixes ensure near zero downtime for customers [2]. | |
| Large data center network | ML models monitoring hardware sensor data (temperatures, fan speeds, error rates) for predictive alerts. | Reduced catastrophic equipment failures by ~40%, by replacing components at-risk before they actually fail (internal KPI report). | |

We see across multiple cases that AI methodologies consistently drive down downtime and maintenance expenses. For instance, Deutsche Telekom's adoption of an AI-powered RIC for its mobile network is reported to have significantly improved reliability [1].

These results validate the practical significance of AI in maintenance – not only as experimental systems but as operational tools saving real money and ensuring uptime. Notably, the RIC example is part of the move towards open RAN architectures, where AI controllers optimize radio networks; this showcases an advanced practice (pioneered in Europe/US).

The ultimate vision (and active research frontier) is fully autonomous network maintenance. Building on successes in predictive alerts, researchers are exploring AI agents that not only predict failures but *take automated corrective action* (with minimal human oversight). In practice, this might involve AI systems that dynamically reconfigure networks to isolate faulty elements or load-balance traffic in anticipation of performance issues. Telecom operators and vendors often call this "self-healing" capability. Cisco, for example, has discussed architectures for self-healing networks where AI monitors network state and automatically executes predefined remedies for known failure scenarios (such as rerouting traffic when a link's error rate skyrockets) [2, 13].

We are seeing early instances of this in cloud data centers and SD-WAN deployments, where policies allow an AI to perform failovers instantly. Importantly, these autonomous actions are kept limited to low-risk scenarios presently – more critical decisions (like shutting down a major router) still require human confirmation. However, as confidence in AI grows, the scope of automation will widen. Gartner's projections reinforce this trajectory: by 2027, an estimated 70% of network operations teams will rely on AI (including generative AI assistants) for day-to-day management, up from less than 5% in 2024 [7]. This points to a near-future state where AI isn't just aiding humans in maintenance, but effectively running the show for many operational tasks.

In summary, AI methodologies in network maintenance are shifting the field from reactive firefighting to proactive and preventive care. Predictive maintenance models catch failures in advance, and automated responses fix certain issues immediately – together these reduce downtime and operational overhead. The next section delves into how organizations can implement these AI solutions, what challenges they face (technology and organizational), and what emerging trends (like generative AI and intent-driven networks) will shape the future of AI-enabled network operations.

## 4. Implementation challenges, best practices, and future trends

Deploying AI in network monitoring and maintenance involves addressing several key challenges—technical, process-related, and cultural. This section outlines the most critical aspects of implementing AI solutions, shares best practices from advanced deployments, and highlights emerging trends.

AI systems depend on high-quality data. Networks generate vast amounts of telemetry (logs, metrics, SNMP traps, NetFlow records), but much of this data may be noisy, incomplete, or isolated in silos. Ensuring data accuracy—through robust collection, time-synchronization, deduplication, and validation—is crucial for reliable AI insights [5]. Unified data lakes and the systematic labeling of historical incidents enhance model training and improve predictive performance, as recommended in Gartner's AIOps guidelines [12].

Once data is in place, AI models must accurately detect anomalies without overwhelming operators with false positives. Iterative tuning and a feedback loop—where network engineers validate AI alerts—can help improve model accuracy over time. Explainable AI (XAI) is essential for building trust; models that clearly indicate which metrics led to an anomaly are preferred [6]. Many implementations use an ensemble approach: a complex model triggers alerts while a simpler, rule-based system provides additional rationale, enabling gradual increased autonomy [12].

Successful AI deployment goes beyond the technology—it requires seamless integration into existing workflows. AI outputs should feed directly into incident management and change management systems. For example, automated ticket creation based on AI predictions ensures accountability and traceability. Establishing an AI-assisted Network Operations Center (NOC) where operators work alongside AI-generated insights can further streamline operations. Additionally, ensuring scalability and reliability through distributed AI services (e.g., edge analytics combined with central processing) is critical, along with securing the data pipeline to prevent adversarial manipulation [6].

Adopting AI in network management necessitates upskilling staff and fostering a culture of collaboration between network engineers and data scientists. Training programs and cross-disciplinary teams help bridge the knowledge gap, ensuring that AI augments rather than replaces human expertise. Early pilot projects demonstrating quick wins can build the necessary trust and drive wider organizational acceptance [8].

Cutting-edge practices such as intent-based networking (IBN) and generative AI are emerging in technologically mature markets. IBN allows operators to define high-level intents (e.g., "maximize service uptime") which AI systems then translate into optimized network configurations. Generative AI is beginning to assist in tasks like writing configuration scripts and simulating network scenarios, with Gartner predicting its growing role in SD-WAN management [7]. Future trends include deeper integration of real-time edge analytics, cross-domain AI for a 360° view of network performance, energy optimization, and the development of digital twins to simulate network behavior under various conditions [1].

To recap the key methodological best practices for implementing AI in network monitoring and maintenance:

- Invest in comprehensive data management: Ensure data quality and integration across diverse sources.
- Start with clear use-cases: Focus on anomaly detection and targeted maintenance challenges; prove value through pilot projects.
- Employ a combination of AI techniques: Integrate complex models with explainable, rule-based systems to maintain operator trust.
- Integrate AI outputs into existing workflows: Automate ticketing and incorporate AI insights into daily operations.
- Upskill the workforce: Create cross-functional teams to bridge the gap between network engineering and data science.

- Plan for continuous improvement: Treat AI models as dynamic systems that require regular updates and refinements.

By following these practices, organizations can overcome key challenges and steadily advance toward more autonomous and efficient network operations.

## 5. Discussion

The quantitative evidence consolidated in Sections 1–3 confirms that AI-enabled operations deliver material, repeatable gains across diverse network domains. Field deployments report a 35–60 % reduction in mean-time-to-repair (MTTR)and 20–30 % cuts in unplanned downtime and OPEX, aligning with longitudinal findings from large-scale backbones [14-16]. By juxtaposing fixed broadband (AIS, Thailand) and mobile RAN (Deutsche Telekom) cases, this study extends prior work that had focused on single-domain scenarios, demonstrating that closed-loop AI produces technology-agnostic benefits. Moreover, integrating energy-optimisation modules lowered carrier power bills by an additional ≈ 5 % of OPEX, compressing the pay-back horizon for AI investments to ≈ 18 months—significantly shorter than the 24–30 months projected in earlier cost-benefit models.

Heterogeneity in effect sizes across operators highlights a pivotal insight: data granularity outweighs model complexity. Networks that stream high-resolution telemetry (sub-second counters, enriched flow records) achieve F1-scores 10 percentage-points higher than peers relying on coarse SNMP polling, even when both employ comparable deep architectures. This observation reinforces the claim that "better bits beat better algorithms." Practically, operators should thus prioritise unified data-lake ingestion, time-synchronisation, and lossless compression before experimenting with more sophisticated models.

Finally, the comparative synthesis clarifies the incremental value of AI over rule-based automation. Traditional heuristics still excel at deterministic fault signatures (e.g., link-down alarms), but they fail under compound or incipient anomalies. AI fills that gap by learning multivariate patterns and—even more critically—by delivering probabilistic confidence scores that can be threshold-tuned to the risk posture of each service tier. This capability is decisive for mission-critical slices (e-health, autonomous-vehicle backhaul) where false positives carry high operational cost.

## 6. Limitations

1. Data-source bias. Most empirical metrics originate from Tier-1 communications-service providers; small enterprise or campus networks may not reproduce identical ROI because of lower event density and simpler topologies.
2. Short evaluation windows. Several cited pilots were monitored for fewer than twelve months, limiting visibility into concept-drift resilience and long-run maintenance savings.
3. Vendor-supplied measurements. A subset of case studies relies on reports issued by solution vendors, which may introduce positive-reporting bias despite independent KPI audits.

Addressing these constraints requires multi-year, vendor-agnostic benchmarking across heterogeneous networks and publishing of anonymised telemetry corpora to facilitate reproducibility.

## 7. Conclusion

In this research, we conducted a comprehensive analysis of how artificial intelligence is being applied to network monitoring and maintenance, focusing on methodological aspects relevant to modern network operations. The key findings are multifold.

First, AI techniques (machine learning, deep learning, etc.) have proven highly effective in network monitoring: they can automatically detect anomalies in vast streams of network data with greater speed and accuracy than traditional methods. Through adaptive learning, AI-based monitors address the challenges of dynamic network conditions and reduce false alarms by learning what "normal" looks like for a given network environment. This leads to faster incident detection and resolution, as evidenced by case studies where AI systems flagged issues hours before they would have been caught manually.

Second, AI-driven approaches to network maintenance are enabling a shift from reactive break-fix models to a proactive maintenance strategy. Predictive maintenance models analyze patterns to forecast faults and performance degradation, significantly cutting down unplanned downtime. Real-world telecom deployments (e.g., those by Deutsche Telekom and others) have demonstrated substantial improvements – up to 20–30% reduction in downtime and costs – by employing AI to anticipate and prevent failures.

In some instances, networks are inching towards self-healing capabilities, where AI not only predicts issues but also initiates automated mitigation (such as re-routing traffic or scheduling a component replacement) without waiting for human intervention.

## References

[1]. Intelligent network management in telecoms - UltiHash. [Electronic resource] – URL: https://www.ultihash.io/use-cases/intelligent-network-management-in-telecommunications

[2]. AI-Powered Telecom Networks: The Road to Full Automation and Intelligence - Telecom Review. [Electronic resource] – URL: https://www.telecomreview.com/articles/reports-and-coverage/8922-ai-powered-telecom-networks-the-road-to-full-automation-and-intelligence

[3]. Gepperth, A., & Rieger, S. (2020). A Survey of Machine Learning applied to Computer Networks. In *ESANN* (pp. 241-250).

[4]. Clemm, A. (2006). *Network management fundamentals*. Cisco press.

[5]. Benefits of AI and Machine Learning in Network Monitoring. [Electronic resource] – URL: https://www.extnoc.com/blog/benefits-of-ai-and-machine-learning-in-network-monitoring/

[6]. Roy, S. A comprehensive Survey on Network Traffic Anomaly Detection using Deep Learning. DOI:10.13140/RG.2.2.32071.30884

[7]. Gartner Report: Generative AI Taking Over SD-WAN Management -- THE Journal. [Electronic resource] – URL: https://thejournal.com/Articles/2024/10/04/Gartner-Report-Generative-AI-Taking-

Over-SD-WAN-Management.aspx

[8]. AI's Role in Revitalizing U.S. Telecoms: Transforming an Industry in Need - TLC Creative Technology. [Electronic resource] – URL: https://www.tlciscreative.com/ais-role-in-revitalizing-u-s-telecoms-transforming-an-industry-in-need/

[9]. The Future of Network Monitoring: AIOPS Trends to Watch in 2025. [Electronic resource] – URL: https://infraon.io/blog/the-future-of-network-monitoring/

[10]. Definition of AIOps (Artificial Intelligence for IT Operations) - Gartner. [Electronic resource] – URL: https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations

[11]. AI in Telecommunications for CSPs | Deloitte US. [Electronic resource] – URL: https://www2.deloitte.com/us/en/pages/consulting/articles/ai-telecommunications-csp.html

[12]. Gartner - AI Networking Report. [Electronic resource] – URL: https://insights.nilesecure.com/ppc-gartner-ai-networking-research

[13]. self-healing networks - Cisco Blogs. [Electronic resource] – URL: https://blogs.cisco.com/tag/self-healing-networks

[14]. Mekrache, A., Ksentini, A., & Verikoukis, C. (2024). Machine Reasoning in FCAPS: Towards Enhanced Beyond 5G Network Management. *IEEE Communications Surveys & Tutorials*.

[15]. Rossi, D., & Zhang, L. (2022). Landing AI on networks: An equipment vendor viewpoint on autonomous driving networks. *IEEE Transactions on Network and Service Management*, *19*(3), 3670-3684.

[16]. Mehmood, K., Kralevska, K., & Palma, D. (2023). Intent-driven autonomous network and service management in future cellular networks: A structured literature review. *Computer Networks*, *220*, 109477.