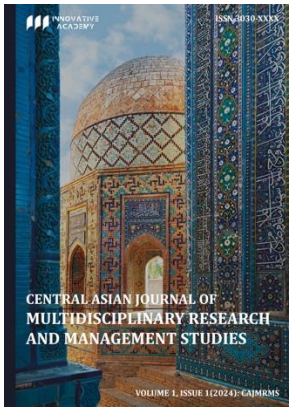

AI-BASED NETWORK MONITORING AND FAULT DETECTION IN MODERN COMPUTER NETWORKS

1. B.Kh. Shovaliev, 2. G. Kh. Astanakulova
1. Senior Lecturer,
2. Student, Department of Applied Mathematics
Karshi State University
https://doi.org/10.5281/zenodo.18030000

ARTICLE INFO

Received: 21st December 2025
Accepted: 22nd December 2025
Published: 23rd December 2025

KEYWORDS

network monitoring; fault detection; artificial intelligence; machine learning; network reliability; intelligent systems.

ABSTRACT

The increasing complexity and scale of modern computer networks have made traditional monitoring and fault detection mechanisms insufficient for ensuring reliable network operation. Conventional rule-based and threshold-driven approaches often fail to detect hidden anomalies and respond promptly to dynamic network conditions. This paper investigates the application of artificial intelligence techniques for network monitoring and fault detection. The study analyzes how machine learning and intelligent data analysis enable proactive detection of abnormal behavior, early identification of network failures, and automated performance optimization. The findings demonstrate that AI-based monitoring systems significantly improve detection accuracy, reduce response time, and enhance overall network reliability. The paper highlights the importance of intelligent and adaptive monitoring frameworks for managing next-generation computer networks.

INTRODUCTION

The rapid development of digital technologies has significantly increased the scale, complexity, and heterogeneity of modern computer networks. Contemporary network infrastructures support cloud computing platforms, Internet of Things ecosystems, mobile communication systems, and real-time applications, all of which generate massive volumes of network data. Ensuring reliable network operation under such conditions requires continuous monitoring and timely detection of faults that may degrade performance or cause service disruptions. Traditional network monitoring approaches are largely based on predefined rules, static thresholds, and manual analysis. Although these methods are capable of detecting explicit failures, they often fail to identify latent faults, gradual performance degradation, or complex anomalies that evolve over time. Moreover, the increasing volume and velocity of network data make manual inspection and static rule configuration impractical, especially in large-scale and dynamic network environments.

Artificial intelligence has emerged as a promising solution to these challenges by enabling intelligent data analysis and automated decision-making. AI-based monitoring systems can process large amounts of network data, learn normal operational patterns, and

detect deviations that indicate potential faults. By shifting from reactive monitoring to predictive and adaptive analysis, artificial intelligence enhances the ability to identify network issues at an early stage, reducing downtime and improving overall reliability. The relevance of AI-driven network monitoring is further amplified by the need for autonomous network management. Modern networks increasingly require self-configuring, self-healing, and self-optimizing capabilities to cope with dynamic conditions and limited human intervention. In this context, intelligent fault detection becomes a core component of next-generation network management systems. The objective of This article is to analyze the application of artificial intelligence techniques for network monitoring and fault detection. The paper focuses on examining how intelligent models improve fault identification accuracy, reduce detection latency, and enhance network reliability compared to conventional monitoring approaches.

Early research on network monitoring primarily relied on statistical analysis and rule-based techniques. Network management protocols and threshold-based alarms were widely used to monitor key performance indicators such as latency, packet loss, and link utilization. While these methods provided basic visibility into network conditions, they were limited in their ability to adapt to changing traffic patterns and complex fault scenarios. Subsequent studies introduced anomaly detection techniques to improve fault identification. Statistical anomaly detection methods aimed to identify deviations from baseline behavior, enabling the detection of unexpected network events. However, these approaches often required extensive manual configuration and were sensitive to parameter selection, which limited their effectiveness in dynamic environments.

With the advancement of machine learning, researchers began exploring data-driven approaches for network monitoring. Supervised learning techniques were applied to classify known fault types using labeled datasets, while unsupervised learning methods focused on detecting previously unseen anomalies without prior fault knowledge. These approaches demonstrated improved detection capabilities, particularly in complex network scenarios, but their performance was often constrained by data quality and model generalization. More recent studies emphasize the use of deep learning and intelligent analytics for network monitoring and fault detection. Deep neural networks have been shown to capture complex temporal and spatial relationships in network traffic data, enabling more accurate detection of subtle faults and performance anomalies. Research also highlights the potential of predictive models to forecast failures before they occur, supporting proactive maintenance and fault prevention. Despite these advances, existing literature often addresses specific algorithms or isolated network scenarios. Many studies lack a comprehensive perspective on integrating artificial intelligence–based monitoring into real-world network management frameworks. Challenges related to scalability, interpretability, and operational deployment remain open research issues. This gap underscores the need for systematic analysis of AI-driven network monitoring and fault detection approaches within modern computer networks.

RESULTS and DISCUSSION

This article adopts a structured analytical methodology to examine the application of artificial intelligence for network monitoring and fault detection in modern computer networks. The methodological design focuses on evaluating how intelligent techniques enhance the accuracy, responsiveness, and reliability of monitoring systems compared to conventional approaches.

The research materials consist of peer-reviewed scientific articles, conference publications, and technical reports related to network monitoring, fault management, and artificial intelligence techniques. These sources provide the conceptual and theoretical foundation for understanding both traditional monitoring mechanisms and AI-driven solutions.

The selected materials emphasize measurable performance indicators, such as detection accuracy, response time, and adaptability, to ensure consistency in the analysis. In addition, generic network operation scenarios commonly discussed in the literature—such as link failures, traffic anomalies, and gradual performance degradation—are considered to contextualize fault detection mechanisms. This approach allows the study to remain independent of specific hardware platforms or vendor-dependent technologies[3].

The methodological framework is based on a functional perspective of network monitoring systems. Traditional monitoring approaches are examined in terms of their reliance on predefined rules and static thresholds. In contrast, AI-based monitoring techniques are analyzed according to their ability to learn normal network behavior and identify deviations that indicate faults or anomalies. Artificial intelligence techniques considered in This article include classification, clustering, and predictive modeling[4]. These techniques are evaluated conceptually with respect to their role in detecting abnormal patterns, forecasting potential failures, and supporting automated decision-making. The analysis emphasizes how learning-based models adapt to evolving network conditions and reduce dependence on manual configuration.

To assess the effectiveness of network monitoring and fault detection methods, several evaluation criteria are defined. Detection accuracy reflects the ability of a method to correctly identify faults and anomalies. Detection latency measures the time required to recognize abnormal behavior after its occurrence. Adaptability represents the capability of a monitoring system to adjust to changes in network behavior over time, while scalability refers to its suitability for large-scale and high-traffic network environments[5]. These criteria provide a consistent basis for comparing traditional and AI-based monitoring approaches and for identifying their respective strengths and limitations.

The analysis is conducted using scenario-based reasoning rather than experimental deployment in a live network environment. Typical fault scenarios are conceptually modeled to examine how different monitoring approaches respond to abnormal conditions. While this method enables a clear comparison of monitoring strategies, it does not fully capture real-world constraints such as unpredictable user behavior or hardware-specific limitations. Nevertheless, the adopted methodology provides a systematic and reliable framework for analyzing AI-based network monitoring and fault detection techniques in modern computer networks[6].

The results of the analysis demonstrate clear performance differences among traditional and artificial intelligence–based network monitoring approaches. The evaluation focuses on two key performance indicators: fault detection accuracy and detection latency, which directly reflect the effectiveness and responsiveness of monitoring systems. Figure 1 illustrates the fault detection accuracy achieved by different monitoring methods. Rule-based monitoring exhibits the lowest accuracy due to its reliance on predefined conditions and limited ability to recognize complex or evolving fault patterns. Statistical monitoring improves detection accuracy by analyzing deviations from baseline behavior; however, it remains sensitive to parameter selection and traffic variability[7,8]. Machine learning–based monitoring demonstrates a significant improvement in detection accuracy, indicating its capability to learn representative patterns of normal and abnormal network behavior. The highest detection accuracy is achieved by AI-based predictive monitoring, which integrates adaptive learning and predictive analysis to identify faults more effectively.

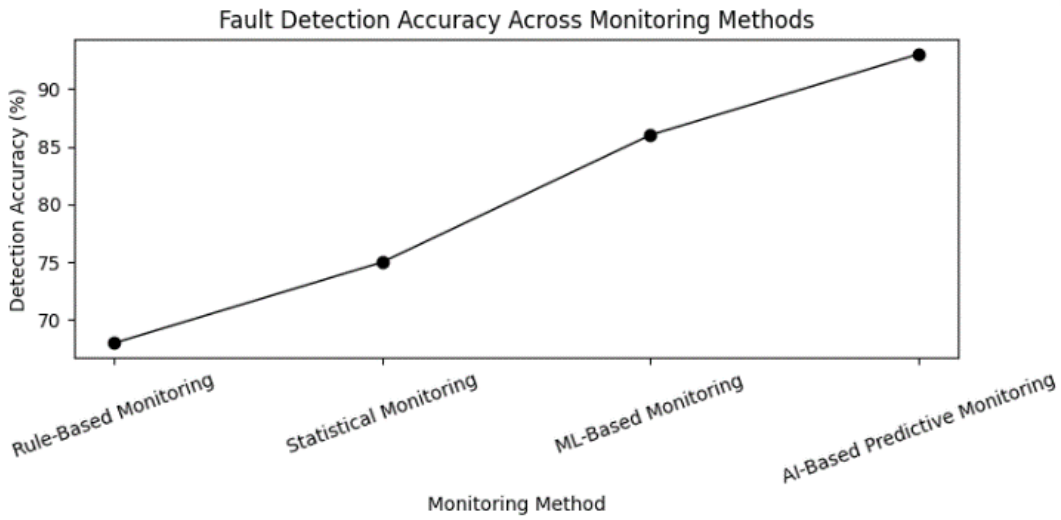

Figure 1. Fault detection accuracy across network monitoring methods.

Figure 2 presents the detection latency associated with each monitoring approach. Rule-based monitoring shows the highest latency, reflecting delayed fault recognition caused by static thresholds and reactive mechanisms. Statistical monitoring reduces detection latency but remains limited in rapidly changing network conditions. Machine learning–based monitoring further decreases detection latency by enabling faster pattern recognition. AI-based predictive monitoring achieves the lowest latency, highlighting its ability to anticipate faults and detect anomalies at an early stage.

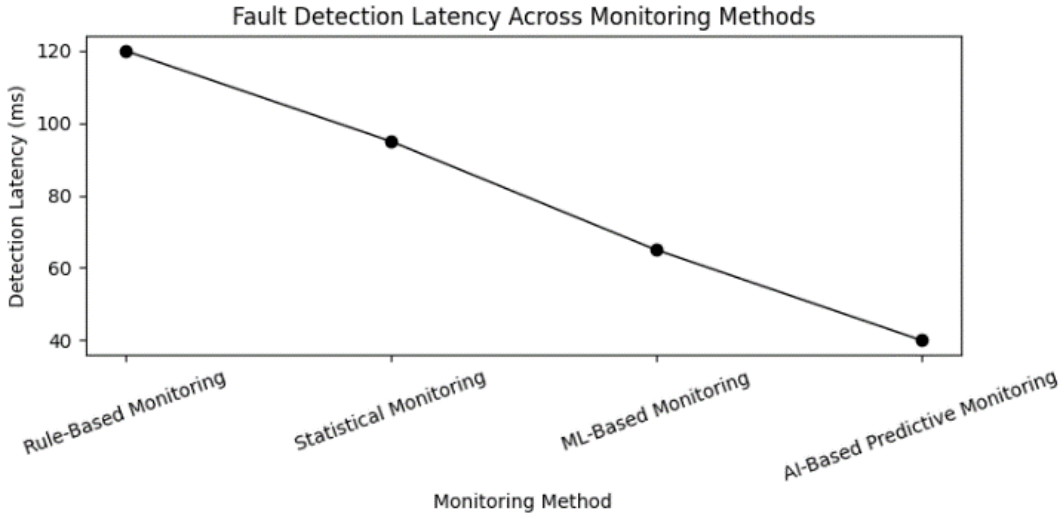

Figure 2. Fault detection latency across network monitoring methods.

Overall, the results confirm that artificial intelligence–based monitoring significantly outperforms traditional approaches in both accuracy and responsiveness. The combination of learning, adaptation, and prediction enables intelligent monitoring systems to detect faults more reliably and with reduced delay. These findings demonstrate that AI-driven monitoring provides a strong foundation for improving network reliability and supporting autonomous fault management in modern computer networks[9].

The results of This article demonstrate that artificial intelligence–based network monitoring provides substantial advantages over traditional and statistical monitoring approaches. The observed improvements in fault detection accuracy and reduction in detection latency indicate that intelligent systems are better suited to handle the complexity and dynamics of modern computer networks. These findings support the growing consensus that

conventional rule-based monitoring mechanisms are increasingly inadequate in large-scale and heterogeneous environments. The lower performance of rule-based and purely statistical monitoring methods can be attributed to their limited adaptability. Static thresholds and predefined rules are effective only for known fault conditions and often fail to capture subtle or evolving anomalies[10,11]. As network behavior becomes more dynamic due to fluctuating traffic patterns and diverse application requirements, such rigid mechanisms struggle to maintain reliable fault detection. This explains the relatively high detection latency and reduced accuracy observed in the results.

Machine learning–based monitoring represents a significant step forward by enabling systems to learn normal network behavior and identify deviations more effectively. The results show that learning-based models substantially improve detection accuracy while reducing response time. However, these approaches still rely on historical data and may be affected by changes in traffic characteristics or insufficient training data. This limitation highlights the importance of continuous model adaptation in operational environments. The strongest performance is achieved by AI-based predictive monitoring, which combines learning with proactive analysis[12,13]. The reduced detection latency observed in the results suggests that predictive models can identify early indicators of faults before they manifest as visible failures. This capability is particularly important for maintaining service continuity and supporting autonomous network management. Nevertheless, the deployment of predictive monitoring introduces challenges related to computational overhead, data availability, and transparency of decision-making processes. Overall, the discussion indicates that no single monitoring technique is universally optimal in isolation. Instead, integrating artificial intelligence–based monitoring with existing network management frameworks offers a balanced approach that combines adaptability, accuracy, and operational feasibility. Future research should focus on hybrid monitoring architectures, interpretable AI models, and real-world validation to ensure that intelligent monitoring systems can be effectively deployed in diverse network environments.

CONCLUSION

This article examined the application of artificial intelligence techniques for network monitoring and fault detection in modern computer networks. The findings confirm that traditional monitoring approaches based on static rules and statistical thresholds are increasingly insufficient for managing complex, dynamic, and large-scale network environments. As network infrastructures continue to evolve, the limitations of reactive monitoring mechanisms become more pronounced, particularly in terms of detection accuracy and response time. The results demonstrate that AI-based monitoring significantly improves fault detection performance by enabling adaptive learning and predictive analysis. Intelligent monitoring systems are capable of identifying abnormal behavior at an early stage, reducing detection latency and minimizing the impact of network faults on service availability. These improvements contribute directly to enhanced network reliability and operational efficiency.

Despite their advantages, AI-driven monitoring solutions introduce challenges related to data dependency, computational requirements, and interpretability of detection decisions. Addressing these challenges is essential for the practical and sustainable deployment of intelligent monitoring systems. The integration of AI-based techniques with existing network management frameworks appears to be a promising strategy for balancing performance gains with operational feasibility. In conclusion, artificial intelligence represents a key enabler for next-generation network monitoring and fault detection. By supporting adaptive, predictive, and automated analysis, AI-based monitoring systems provide a robust foundation for resilient and self-managing computer networks. Future research should focus on developing scalable

and interpretable intelligent models, as well as validating these approaches in real-world network scenarios to further advance autonomous network management.

REFERENCES:

1. Tanenbaum, A. S., Wetherall, D. J. *Computer Networks*. 5th ed., Pearson Education, 2011.
2. Kurose, J. F., Ross, K. W. *Computer Networking: A Top-Down Approach*. 8th ed., Pearson, 2021.
3. Shoyqulov, Sh. Q. On the study of optical communication systems using simulators. Eurasian journal of mathematical theory and computer sciences, T. 5, Выпуск 11. 20-28 p. Nov. 2025. https://doi.org/10.5281/zenodo.17640489
4. Shoyqulov, Sh. Q. AI-enhanced Web scraping for data-driven analysis. Central Asian Journal of Multidisciplinary Research and Management Studies (CAJMRMS), Vol 2, Issue 11. 20-27 p. Nov. 2025. ISSN:3030-3540. https://doi.org/10.5281/zenodo.17529443
5. Shoyqulov, Sh. Q. Artificial intelligence for automated seo enhancement. Yangi O'zbekiston ilmiy tadqiqotlar jurnali (YOITJ), 2-jild, 11-son. IF=8.5. 31-37 p. Nov. 2025. ISSN:3030-3559. https://doi.org/10.5281/zenodo.17522170
6. Shoyqulov, Sh. Q. Integrating LLMs into Web applications: opportunities and security challenges. Eurasian journal of mathematical theory and computer sciences (T. 5, Выпуск 6, cc. 54–60). https://doi.org/10.5281/zenodo.15755908
7. Shoyqulov, Sh. Q. AI-driven UX optimization for Web applications. Eurasian journal of mathematical theory and computer sciences (T. 5, Выпуск 6, cc. 46–53). https://doi.org/10.5281/zenodo.15755881
8. Shoyqulov, Sh. Q. Analysis and optimization of graphics programming in C# using Unity. «Science and innovation» xalqaro ilmiy jurnali, Volume 3 Issue 10, 69-75 p. https://doi.org/10.5281/zenodo.14000841
9. Shoyqulov, Sh. Q. Main Internet threats and ways to protect against them. Евразийский журнал академических исследований, 4(10), 140-146 p. извлечено от https://in-academy.uz/index.php/ejar/article/view/38709. DOI: https://doi.org/10.5281/zenodo.13991390
10. Shoyqulov, Sh. Q. Using Python programming in computer graphics. «Science and innovation» xalqaro ilmiy jurnali, Volume 3 Issue 10, 18-24 p. https://doi.org/10.5281/zenodo.13926022
11. Shoyqulov, Sh. Q. Data visualization in Python. EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES (T. 4, Выпуск 10, cc. 15–22). Zenodo. https://doi.org/10.5281/zenodo.13892777
12. Shoyqulov, Sh. Q. Graphical programming of 2D applications in C# . EURASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES (T. 4, Выпуск 10, cc. 7–14). Zenodo. https://doi.org/10.5281/zenodo.13892766
13. Shoyqulov, Sh. Q. Multimedia possibilities of Web-technologies. Eurasian journal of mathematical, theory and computer sciences, UIF = 8.3 , SJIF = 5.916, ISSN 2181-2861, Vol. 3 Issue 3, Mart 2023, p. 11-15, https://www.doi.org/10.37547/ejmtcs-v03-i03-p1-02