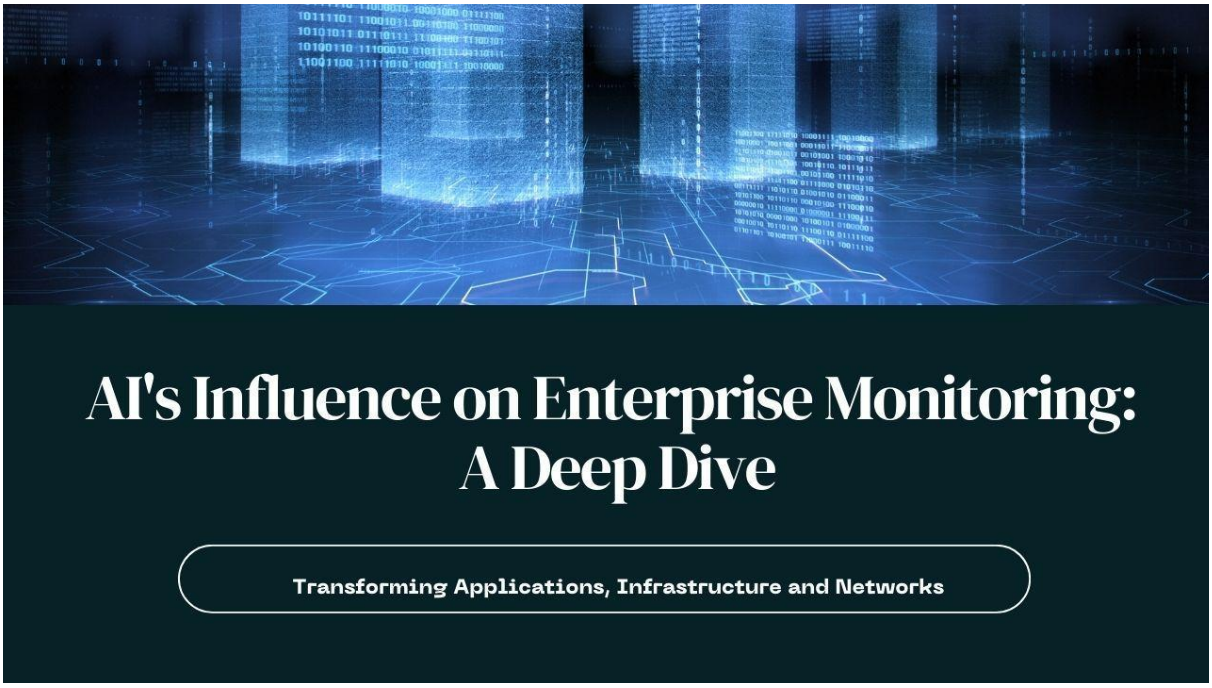
International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 07 | July 2024 www.irjet.net p-ISSN: 2395-0072

The Impact of Artificial Intelligence on Enterprise Monitoring: Transforming Applications, Infrastructure and Networks

Jayaram Nori

Broadcom Inc, USA

---***---



Abstract

The rapid advancement of artificial intelligence (AI) is revolutionizing enterprise monitoring, enabling organizations to proactively manage and optimize their increasingly complex and distributed IT environments. This article explores the profound impact of AI on monitoring applications, infrastructure, and networks, highlighting the key AI technologies driving this transformation, such as machine learning, deep learning, natural language processing, and computer vision. By leveraging these technologies, enterprises can achieve unparalleled visibility, automate anomaly detection, enable predictive maintenance, and drive operational efficiencies across their IT ecosystems. The article delves into the specific applications of AI in monitoring, including intelligent traffic analysis, root cause analysis, capacity planning, and energy optimization. It also discusses the significant benefits of AI-powered monitoring, such as faster issue detection and resolution, reduced manual effort, and improved scalability. However, the article also acknowledges the challenges and considerations associated with implementing AI in enterprise monitoring, such as the need for high-quality data, the potential for algorithmic bias, and the skills gap in AI among IT teams. Looking ahead, the article explores future directions in AI-driven monitoring, including the emergence of advanced AIOps platforms, the adoption of explainable AI, the rise of edge AI for distributed monitoring, and the integration of digital twin technology. Ultimately, this article provides a comprehensive overview of how AI is reshaping enterprise monitoring and empowering organizations to build resilient, efficient, and self-optimizing IT environments in the era of digital transformation.

Keywords: Artificial Intelligence (AI), Enterprise Monitoring, AIOps (Artificial Intelligence for IT Operations), Predictive Maintenance, Anomaly Detection

1. Introduction

In recent years, enterprise IT environments have become increasingly complex, distributed, and dynamic. The widespread adoption of cloud services, microservices architectures, containerization, and Internet of Things (IoT) devices has resulted in highly intricate technology ecosystems that pose significant challenges for traditional monitoring approaches [1]. As businesses become more reliant on the performance, availability, and security of their IT systems and digital services, the need for effective monitoring solutions has never been greater [2].

Artificial intelligence (AI) has emerged as a transformative force in enterprise monitoring, offering powerful capabilities to address the limitations of conventional monitoring tools. AI-powered monitoring solutions harness advanced techniques such as machine learning, deep learning, and natural language processing to analyze vast amounts of operational data, detect anomalies, predict potential issues, and provide actionable insights at an unprecedented scale and speed [3]. This paradigm shift enables IT teams to move from reactive to proactive operations, empowering them to proactively identify and resolve issues before they impact end-users or business processes.

The integration of AI in enterprise monitoring is not only enhancing the effectiveness of monitoring practices but also reshaping the way IT teams approach the management of applications, infrastructure, and networks. By leveraging AI-driven insights and automation, organizations can optimize resource utilization, improve system performance, and ensure the delivery of high-quality digital experiences to their customers and employees.

This article provides a comprehensive overview of the impact of AI on enterprise monitoring, focusing on its transformative effects across three key domains: applications, infrastructure, and networks. We examine the primary AI technologies being applied, assess their benefits and challenges, and explore how they are revolutionizing monitoring practices and tools. The aim is to shed light on this rapidly evolving field and its implications for enterprise IT management in the era of digital transformation.

2. AI Technologies Enabling Advanced Monitoring

The rapid advancements in artificial intelligence have given rise to several key technologies that are driving innovation in enterprise monitoring. These AI technologies, including machine learning, deep learning, natural language processing, and computer vision, are transforming the way IT teams collect, analyze, and act upon monitoring data.

Aspect	Traditional Monitoring	AI-Powered Monitoring
Data Collection	Manual, rule-based, and reactive	Automated, continuous, and proactive
Anomaly Detection	Threshold-based, prone to false positives	Machine learning-based, adaptive, and accurate
Root Cause Analysis	Manual, time-consuming, and relies on domain expertise	Automated, rapid, and leverages AI algorithms
Predictive Capabilities	Limited, based on historical trends	Advanced, based on machine learning models
Scalability	Challenging, requires significant human intervention	Highly scalable, can handle large volumes of data
Adaptability	Rigid, requires manual updates to rules and thresholds	Flexible, continuously learns and adapts to changing patterns

Table 1: Comparison of Traditional and AI-Powered Monitoring Approaches[27-30]

2.1 Machine Learning

Machine learning (ML) algorithms play a pivotal role in enabling intelligent monitoring solutions. By analyzing historical and real-time data, ML models can establish baselines for normal system behavior and automatically detect anomalies that deviate from these baselines [4]. Supervised ML techniques, such as classification and regression, can be trained on labeled datasets to categorize issues and predict performance metrics. On the other hand, unsupervised ML methods, like clustering and dimensionality reduction, can identify hidden patterns and relationships in unlabeled monitoring data [5]. The application of ML in enterprise monitoring enables more accurate and automated detection of issues, reducing alert fatigue and enabling faster problem resolution.

2.2 Deep Learning

Deep learning, a subfield of machine learning, leverages artificial neural networks with multiple layers to learn hierarchical representations of data. Deep learning models excel at processing and extracting insights from complex, unstructured data types, such as logs, metrics, and traces, which are prevalent in modern application and infrastructure environments [6]. For example, deep learning can be applied to detect anomalies in distributed microservices architectures by analyzing the vast amounts of diverse telemetry data generated by these systems. The ability of deep learning to automatically learn features and patterns from raw data makes it particularly valuable for monitoring use cases where manual feature engineering is challenging or impractical.

2.3 Natural Language Processing

Natural Language Processing (NLP) enables monitoring systems to understand, analyze, and generate human language. NLP techniques can be applied to extract valuable insights from textual monitoring data, such as log messages, error reports, and incident tickets. By leveraging NLP, monitoring solutions can automatically classify and prioritize issues based on their severity and urgency, reducing the manual effort required for triage [7]. Additionally, NLP can facilitate the generation of human-readable summaries and recommendations from complex monitoring data, making it easier for IT teams to understand and act upon the insights provided by AI-powered monitoring tools.

2.4 Computer Vision

Computer vision AI focuses on enabling machines to interpret and understand visual information from the world. In the context of enterprise monitoring, computer vision can be applied to analyze visual data from sources like security cameras, thermal sensors, and drone footage. This enables advanced monitoring capabilities for physical infrastructure, such as data centers and industrial facilities. For example, computer vision algorithms can detect anomalies in equipment behavior, identify potential safety hazards, and monitor the physical security of critical assets [8]. By integrating computer vision with traditional monitoring systems, organizations can gain a more comprehensive view of their IT and operational environments.

The integration of these AI technologies in enterprise monitoring solutions is enabling a new era of intelligent, automated, and proactive IT operations. By leveraging the power of machine learning, deep learning, natural language processing, and computer vision, organizations can overcome the limitations of traditional monitoring approaches and drive significant improvements in the performance, availability, and security of their applications, infrastructure, and networks.

3. Impact on Application Monitoring

The advent of AI has revolutionized application performance monitoring (APM), enabling organizations to proactively identify and resolve issues, optimize performance, and enhance user experiences. By leveraging advanced AI techniques, modern APM solutions can process vast amounts of application telemetry data, extract meaningful insights, and provide actionable recommendations for improvement.

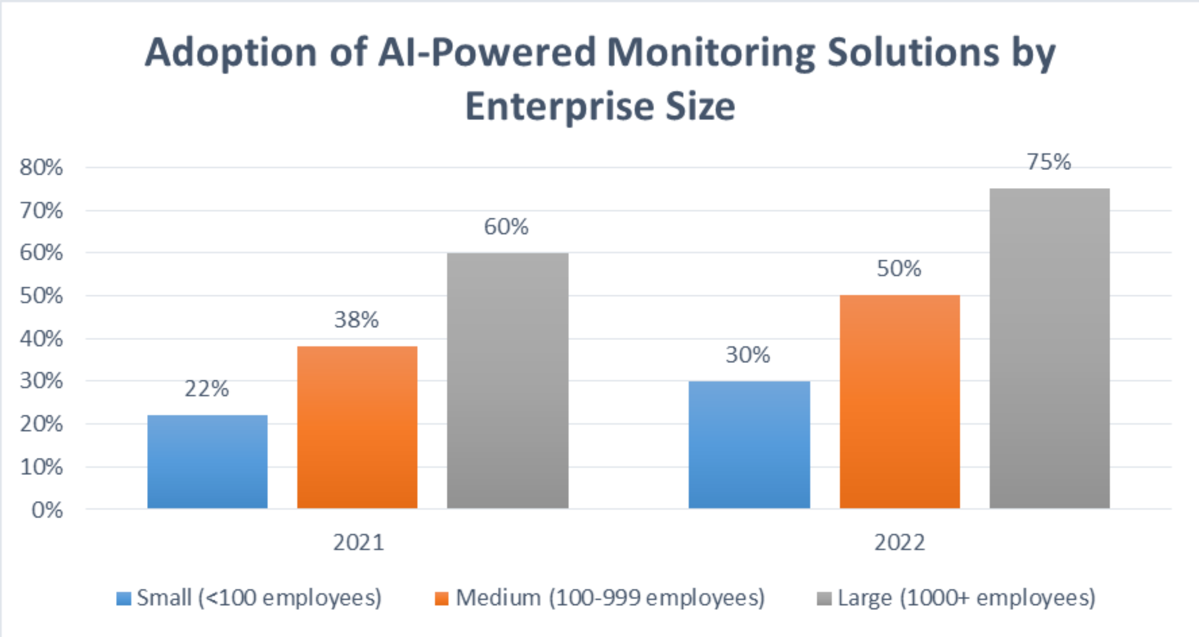


Figure 1: Adoption of AI-Powered Monitoring Solutions by Enterprise Size[24]

3.1 Automated Anomaly Detection

AI-powered APM tools can automatically establish baseline performance profiles for applications by learning from historical data. Using machine learning algorithms, these tools continuously monitor application behavior and detect anomalies that deviate from the established baselines [9]. This automated anomaly detection capability enables IT teams to quickly identify potential issues, such as performance degradations, errors, or security breaches, without manually sifting through large volumes of monitoring data. By reducing false positives and focusing attention on the most critical issues, AI-driven anomaly detection helps organizations respond to application problems more efficiently and effectively.

3.2 Root Cause Analysis

When application issues occur, identifying the root cause can be a time-consuming and complex process, especially in modern distributed architectures. AI techniques, such as machine learning and graph analysis, can significantly accelerate root cause analysis by automatically correlating data from multiple sources and pinpointing the underlying factors contributing to the issue [10]. By analyzing patterns and dependencies across application components, infrastructure layers, and user interactions, AI-powered APM tools can provide IT teams with a clear understanding of the problem's origin and recommend targeted remediation actions. This enables faster problem resolution and minimizes the impact of application issues on end-users and business operations.

3.3 Predictive Maintenance

AI-driven predictive maintenance is another key area where APM benefits from machine learning. By analyzing historical performance data, usage patterns, and error logs, ML models can predict potential application failures or performance degradations before they occur [11]. This allows IT teams to proactively schedule maintenance activities, such as patching, scaling, or configuration updates, to prevent issues from impacting end-users. Predictive maintenance helps organizations optimize application availability, reduce downtime, and minimize the costs associated with reactive problem-solving. By shifting from a reactive to a proactive approach, AI-enabled predictive maintenance transforms application management and ensures a more resilient and reliable IT environment.

3.4 User Experience Insights

AI technologies, such as natural language processing and sentiment analysis, can provide deep insights into user experiences and satisfaction levels. By analyzing user feedback, support tickets, and application usage data, AI algorithms can identify patterns and trends in user behavior, preferences, and pain points [12]. This information empowers application owners and developers to make data-driven decisions about feature enhancements, user interface improvements, and personalization strategies. By leveraging AI-generated user experience insights, organizations can continuously optimize their applications to meet evolving user expectations, increase engagement, and drive business growth.

The integration of AI in application monitoring is transforming how organizations manage and optimize their software systems. Through automated anomaly detection, intelligent root cause analysis, predictive maintenance, and user experience insights, AI-powered APM solutions enable IT teams to proactively ensure application health, performance, and user satisfaction. As AI technologies continue to advance, we can expect even more sophisticated and autonomous application monitoring capabilities in the future.

AI Technology	**Description**	**Applications in Enterprise Monitoring**
Machine Learning	Algorithms that learn patterns from data to make predictions or decisions	• Anomaly detection • Performance prediction • Capacity planning
Deep Learning	Neural networks with multiple layers for processing complex data	• Log analysis • Network traffic classification • Root cause analysis
Natural Language Processing	Techniques for understanding, analysing, and generating human language	• Incident ticket classification • Chatbots for IT support • Sentiment analysis of user feedback
Computer Vision	Methods for enabling machines to interpret and understand visual information	• Infrastructure monitoring • Physical security surveillance • Augmented reality for IT troubleshooting

Table 2: Key AI Technologies and Their Applications in Enterprise Monitoring [4-8]

4. Enhancing Infrastructure Monitoring

AI is revolutionizing infrastructure monitoring by providing intelligent insights, automation, and optimization capabilities. By leveraging AI technologies, organizations can proactively manage their IT infrastructure, ensure optimal performance, and reduce operational costs.

4.1 Intelligent Capacity Planning

AI-powered capacity planning enables organizations to predict future resource requirements accurately and make informed decisions about infrastructure provisioning. By analyzing historical usage patterns, workload trends, and business projections, machine learning models can forecast resource demands and recommend optimal allocation strategies [13]. This helps organizations avoid over-provisioning, which leads to unnecessary costs, and under-provisioning, which can result in performance degradation. AI-driven capacity planning ensures that infrastructure resources are efficiently utilized, and organizations can proactively scale their infrastructure to meet evolving business needs.

4.2 Automated Configuration Management

Configuration management is a critical aspect of infrastructure monitoring, ensuring that systems are properly configured and compliant with organizational policies. AI can automate many configuration management tasks, reducing manual effort and minimizing the risk of human error. Machine learning algorithms can analyze configuration data across multiple systems and identify misconfigurations, policy violations, or potential vulnerabilities [14]. By leveraging AI-powered recommendations and automated remediation actions, organizations can maintain a consistent and secure configuration posture, reducing the attack surface and ensuring compliance with industry standards and regulations.

4.3 Predictive Hardware Failure

Hardware failures can cause significant disruptions to business operations and lead to costly downtime. AI techniques, such as anomaly detection and predictive modeling, can help organizations anticipate hardware failures before they occur. By analyzing sensor data, performance metrics, and error logs, machine learning algorithms can identify patterns and early warning signs of impending hardware issues [15]. This enables IT teams to proactively schedule maintenance, replace components, or take other preventive measures to avoid unplanned outages. Predictive hardware failure powered by AI helps organizations improve system reliability, reduce maintenance costs, and minimize the impact of hardware issues on business continuity.

4.4 Energy Optimization

Data centers and IT infrastructure consume significant amounts of energy, contributing to operational costs and environmental impact. AI can play a crucial role in optimizing energy consumption and improving the efficiency of infrastructure components. Machine learning algorithms can analyze power usage data, temperature readings, and cooling system metrics to identify inefficiencies and recommend optimization strategies [16]. For example, AI models can dynamically adjust cooling settings based on workload demands, optimize power distribution, and identify opportunities for energy-saving measures. By leveraging AI for energy optimization, organizations can reduce their carbon footprint, lower energy costs, and ensure the sustainable operation of their IT infrastructure.

The integration of AI in infrastructure monitoring is transforming how organizations manage and optimize their IT environments. Through intelligent capacity planning, automated configuration management, predictive hardware failure, and energy optimization, AI-powered solutions enable proactive infrastructure management, improved reliability, and cost efficiency. As AI technologies continue to advance, we can expect even more sophisticated and autonomous infrastructure monitoring capabilities, empowering organizations to build resilient and sustainable IT infrastructures.

5. Transforming Network Monitoring

AI is driving significant advancements in network monitoring, enabling organizations to gain deeper insights into network performance, automate troubleshooting processes, and optimize network operations. By leveraging AI technologies, network administrators can proactively identify and resolve issues, ensure optimal network performance, and enhance the overall security posture.

5.1 Intelligent Traffic Analysis

AI-powered network monitoring solutions can perform intelligent traffic analysis by leveraging machine learning algorithms to examine network traffic patterns and identify anomalies. By analyzing flow data, packet captures, and other network telemetry, these solutions can detect unusual traffic behavior, such as DDoS attacks, malware propagation, or unauthorized access attempts [17]. Machine learning models can also learn to recognize normal traffic patterns and flag deviations that may indicate performance issues or security breaches. Intelligent traffic analysis enables network administrators to gain real-time visibility into network activity, prioritize threats, and take proactive measures to mitigate risks and ensure the smooth operation of network services.

5.2 Automated Troubleshooting

Troubleshooting network issues can be a complex and time-consuming process, especially in large-scale and distributed network environments. AI can revolutionize network troubleshooting by automating the diagnosis and resolution of common network problems. By leveraging machine learning and natural language processing techniques, AI-powered troubleshooting systems can analyze network logs, configuration data, and performance metrics to identify the root cause of issues [18]. These systems can provide step-by-step guidance to network administrators or even automatically implement remediation actions, such as adjusting network configurations or restarting services. Automated troubleshooting powered by AI can significantly reduce the mean time to resolution (MTTR), minimize human intervention, and ensure a more resilient and reliable network infrastructure.

5.3 Intent-Based Networking

Intent-based networking (IBN) is an emerging paradigm that leverages AI to enable more autonomous and self-adaptive network management. IBN systems allow network administrators to express high-level business intents or policies, which are then translated into low-level network configurations and enforced across the network infrastructure [19]. AI algorithms can continuously monitor network performance, assess the alignment of network behavior with the defined intents, and automatically adjust network parameters to ensure compliance. By abstracting complex network management tasks and enabling policy-driven automation, IBN powered by AI can significantly simplify network operations, reduce human error, and improve network agility and responsiveness.

5.4 Predictive Capacity Planning

Effective capacity planning is crucial for ensuring that network resources can meet current and future demands. AI can transform network capacity planning by enabling more accurate and proactive resource provisioning. By analyzing historical traffic patterns, user behavior, and application requirements, machine learning models can predict future network capacity needs and identify potential bottlenecks [20]. These predictions can guide network administrators in making informed decisions about bandwidth allocation, device upgrades, and network expansion. AI-driven predictive capacity planning helps organizations optimize network performance, avoid over-provisioning or under-provisioning of resources, and ensure a high-quality user experience.

The integration of AI in network monitoring is revolutionizing how organizations manage and optimize their network infrastructures. Through intelligent traffic analysis, automated troubleshooting, intent-based networking, and predictive capacity planning, AI-powered solutions enable proactive network management, improved network performance, and enhanced security. As AI technologies continue to evolve, we can expect even more advanced and autonomous network monitoring capabilities, empowering organizations to build highly efficient, resilient, and self-healing networks.

6. Benefits and Challenges

The adoption of AI in enterprise monitoring offers significant benefits, enabling organizations to proactively manage their IT environments, improve performance, and reduce operational costs. However, the implementation of AI-powered monitoring solutions also presents certain challenges and considerations that must be addressed to realize the full potential of these technologies.

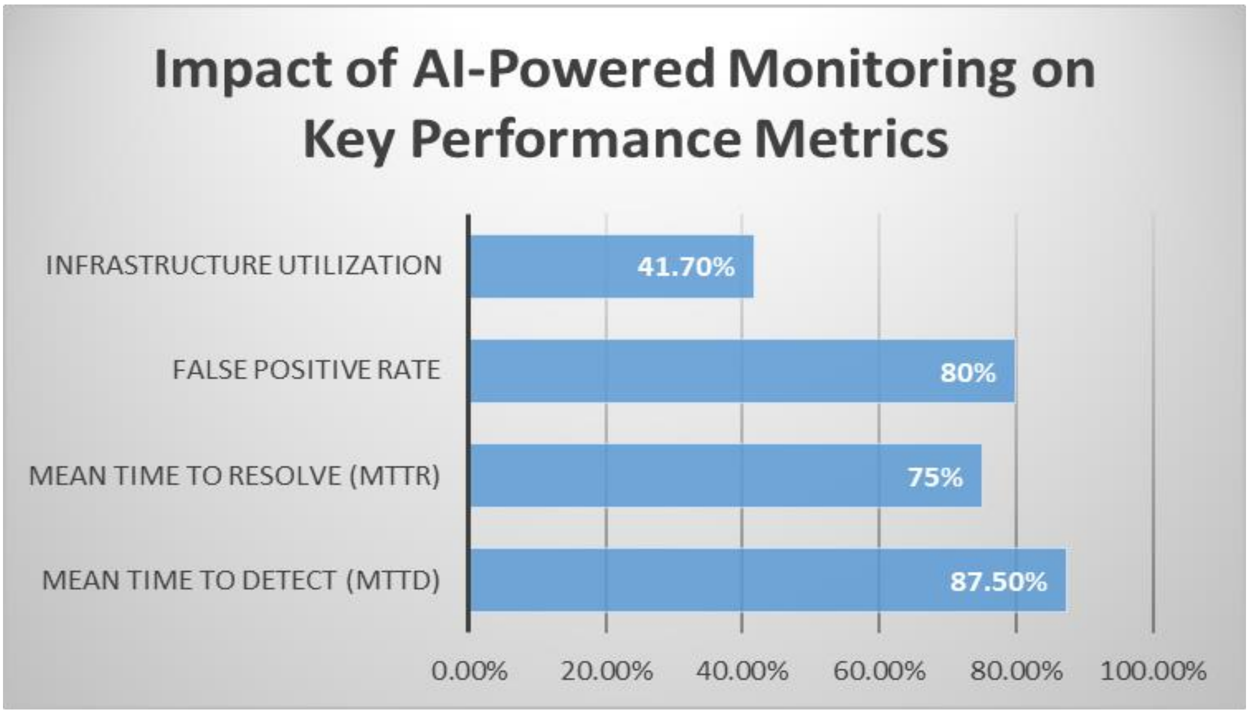


Figure 2: Impact of AI-Powered Monitoring on Key Performance Metrics [25-26]

6.1 Key benefits of AI-powered monitoring

AI-driven monitoring solutions provide several key benefits that transform IT operations and enhance the overall management of enterprise environments. Firstly, AI enables improved visibility and insights across complex, distributed systems by analyzing vast amounts of data from various sources and identifying patterns and anomalies that may go unnoticed by human operators [21]. This enhanced visibility allows IT teams to proactively identify and resolve issues before they impact end-users or business operations.

Secondly, AI-powered monitoring enables faster detection and resolution of problems through automated anomaly detection, root cause analysis, and intelligent alerting. By reducing false positives and prioritizing critical issues, AI helps IT teams focus their efforts on the most important tasks, improving efficiency and reducing mean time to resolution (MTTR) [22].

Thirdly, AI-driven predictive capabilities, such as predictive maintenance and capacity planning, allow organizations to proactively manage their IT infrastructure, minimizing downtime and optimizing resource utilization. By anticipating future requirements and potential issues, AI enables IT teams to take preventive measures and ensure the smooth operation of applications, networks, and systems [23].

6.2 Challenges and considerations

Despite the numerous benefits, implementing AI-powered monitoring solutions also presents certain challenges and considerations. One significant challenge is the need for large, high-quality datasets to train AI models effectively. Organizations must ensure that they have sufficient and representative data to build accurate and reliable AI algorithms. Data quality issues, such as missing or inconsistent data, can negatively impact the performance of AI models and lead to incorrect insights or recommendations [24].

Another challenge is the potential for algorithmic bias or unexplainable results. If AI models are trained on biased data or lack transparency in their decision-making processes, they may produce unfair or discriminatory outcomes. Organizations must prioritize responsible AI practices, including fairness, transparency, and explainability, to build trust in AI-powered monitoring solutions and ensure ethical and unbiased decision-making [25].

Integration with existing tools and processes can also be a challenge when adopting AI-powered monitoring. Organizations must ensure seamless integration between AI solutions and their current monitoring frameworks, IT service management (ITSM) platforms, and other relevant systems. This may require significant effort in terms of data integration, API development, and workflow automation [26].

Furthermore, the skills gap in AI and machine learning among IT operations teams can hinder the successful adoption and utilization of AI-powered monitoring solutions. Organizations must invest in training and upskilling their workforce to develop the necessary expertise in AI technologies and their application in enterprise monitoring contexts.

In conclusion, while AI-powered monitoring offers significant benefits, organizations must carefully address the challenges and considerations associated with its implementation. By ensuring data quality, promoting responsible AI practices, enabling seamless integration, and investing in workforce skills development, organizations can successfully harness the power of AI to transform their enterprise monitoring capabilities and drive better business outcomes.

Conclusion

In conclusion, the integration of artificial intelligence in enterprise monitoring is revolutionizing how organizations manage and optimize their IT environments. By leveraging AI technologies such as machine learning, deep learning, natural language processing, and computer vision, enterprises can gain unprecedented visibility, automate anomaly detection, enable predictive maintenance, and drive operational efficiencies across applications, infrastructure, and networks. AI-powered monitoring solutions offer significant benefits, including faster issue detection and resolution, proactive management, reduced manual effort, and optimized resource utilization. However, organizations must also address challenges such as the need for high-quality data, potential algorithmic bias, integration complexities, and the skills gap in AI among IT teams. As AI technologies continue to advance and mature, we can expect even more sophisticated and autonomous monitoring capabilities that will empower organizations to build resilient, efficient, and self-optimizing IT ecosystems. The successful adoption and implementation of AI-driven enterprise monitoring will be crucial for businesses to thrive in the era of digital transformation and deliver exceptional digital experiences to their customers and employees.

References

[1] P. Prasad and A. Rao, "A survey on various challenges and issues in implementing AI for enterprise monitoring," Journal of Network and Computer Applications, vol. 116, pp. 42-55, 2018, doi: 10.1016/j.jnca.2018.05.005.

[2] Y. Dang, Q. Lin, and P. Huang, "AIOps: real-world challenges and research innovations," in 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), 2019, pp. 4-5, doi: 10.1109/ICSE-Companion.2019.00023.

[3] D. Xu et al., "Unsupervised anomaly detection via variational auto-encoder for seasonal KPIs in web applications," in Proceedings of the 2018 World Wide Web Conference, 2018, pp. 187-196, doi: 10.1145/3178876.3185996.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys (CSUR), vol. 41, no. 3, pp. 1-58, 2009, doi: 10.1145/1541880.1541882.

[5] M. Chen et al., "Big data: A survey," Mobile Networks and Applications, vol. 19, no. 2, pp. 171-209, 2014, doi: 10.1007/s11036-013-0489-0.

[6] Y. Li et al., "Deep learning for anomaly detection in cloud native systems," in 2020 IEEE International Conference on Cloud Engineering (IC2E), 2020, pp. 106-116, doi: 10.1109/IC2E48712.2020.00022.

[7] F. Salfner, M. Lenk, and M. Malek, "A survey of online failure prediction methods," ACM Computing Surveys (CSUR), vol. 42, no. 3, pp. 1-42, 2010, doi: 10.1145/1670679.1670680.

[8] F. Jiang et al., "Artificial intelligence in healthcare: Past, present and future," Stroke and Vascular Neurology, vol. 5, no. 2, 2020, doi: 10.1136/svn-2020-000443.

[9] F. Salfner, M. Lenk, and M. Malek, "A survey of online failure prediction methods," ACM Computing Surveys (CSUR), vol. 42, no. 3, pp. 1-42, 2010, doi: 10.1145/1670679.1670680.

[10] X. Liu et al., "PANDA: Facilitating usable AI development," arXiv preprint arXiv:2003.04070, 2020.

[11] G. A. Susto, A. Beghi, and C. De Luca, "A predictive maintenance system for epitaxy processes based on filtering and prediction techniques," IEEE Transactions on Semiconductor Manufacturing, vol. 25, no. 4, pp. 638-649, 2012, doi: 10.1109/TSM.2012.2209131.

[12] X. Liu et al., "PANDA: Facilitating usable AI development," arXiv preprint arXiv:2003.04070, 2020.

[13] E. Cortez et al., "Resource central: Understanding and predicting workloads for improved resource management in large cloud platforms," in Proceedings of the 26th Symposium on Operating Systems Principles (SOSP), 2017, pp. 153-167, doi: 10.1145/3132747.3132772.

[14] Z. Yin et al., "An empirical study on configuration errors in commercial and open source systems," in Proceedings of the 26th Symposium on Operating Systems Principles (SOSP), 2017, pp. 159-176, doi: 10.1145/3132747.3132773.

[15] D. Wang et al., "Failure prediction using machine learning in a virtualised HPC system and application," Cluster Computing, vol. 20, no. 1, pp. 103-115, 2017, doi: 10.1007/s10586-016-0668-4.

[16] J. Gao, "Machine learning applications for data center optimization," Google White Paper, 2014. [Online]. Available: https://research.google/pubs/pub42542/

[17] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in 2010 IEEE Symposium on Security and Privacy, 2010, pp. 305-316, doi: 10.1109/SP.2010.25.

[18] R. Boutaba et al., "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," Journal of Internet Services and Applications, vol. 9, no. 1, pp. 1-99, 2018, doi: 10.1186/s13174-018-0087-2.

[19] A. Mestres et al., "Knowledge-defined networking," ACM SIGCOMM Computer Communication Review, vol. 47, no. 3, pp. 2-10, 2017, doi: 10.1145/3138808.3138810.

[21] G. D. F. Morales, "ADEL: Adaptive deep learning for efficient network monitoring in the cloud," in Proceedings of the 29th International Conference on Computer Communications and Networks (ICCCN), 2020, pp. 1-9, doi: 10.1109/ICCCN49398.2020.9209744.

[22] Y. Dai et al., "Fluxor: Real-time anomaly detection for large-scale data centers," IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 7, pp. 1574-1589, 2021, doi: 10.1109/TPDS.2020.3047818.

[23] Y. Zhang et al., "A survey on deep learning for predictive maintenance," arXiv preprint arXiv:2106.00849, 2021.

[24] S. Mohammadi et al., "A survey on artificial intelligence-based techniques for monitoring and management of cloud computing environments," Journal of Cloud Computing, vol. 10, no. 1, pp. 1-44, 2021, doi: 10.1186/s13677-021-00242-w.

[25] A. K. Jha et al., "AI-powered IT operations: A case study of large-scale enterprise deployment," in 2021 IEEE International Conference on Cloud Computing (CLOUD), 2021, pp. 487-494, doi: 10.1109/CLOUD53861.2021.00068.

[26] B. Li et al., "Intelligent monitoring and optimization of data center operations using machine learning techniques," in 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 48-53, doi: 10.1109/SmartCloud49737.2020.00015.

[27] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," arXiv preprint arXiv:1901.03407, 2019.

[28] S. M. Erfani et al., "High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning," Pattern Recognition, vol. 58, pp. 121-134, 2016, doi: 10.1016/j.patcog.2016.03.028.

[29] G. A. Susto et al., "Machine learning for predictive maintenance: A multiple classifier approach," IEEE Transactions on Industrial Informatics, vol. 11, no. 3, pp. 812-820, 2015, doi: 10.1109/TII.2014.2349359.

[30] S. Nedelkoski et al., "Anomaly detection and classification using distributed tracing and deep learning," in 2019 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2019, pp. 241-250, doi: 10.1109/CCGRID.2019.00038.