International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 7965-7971
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Enhancing DevOps with AIOps: Leveraging Artificial Intelligence for Efficient Incident Management

Naveen Kumar Kasarla*

Independent Researcher, USA
* **Corresponding Author Email:** naveenkumarkasarla1@gmail.com - **ORCID:** 0000-0002-5247-7150

Article Info:

DOI: 10.22399/ijcesen.4172
Received : 03 September 2025
Accepted : 20 October 2025

Keywords

AIOps Implementation,
DevOps Automation,
Incident Management Systems,
Machine Learning Operations,
Infrastructure Intelligence

Abstract:

DevOps teams struggle with incident management in distributed systems where traditional monitoring creates more problems than solutions. Alert storms overwhelm operations centers while genuine issues hide among thousands of false positives. Engineers waste time correlating data from dozens of different tools instead of fixing actual problems that impact users. Most organizations handle incidents the hard way. Systems break, alerts fire, and teams scramble to understand what happened while customers complain. This reactive cycle burns through engineering talent and damages business relationships during extended outages. Manual correlation across microservice architectures becomes impossible as systems grow more complex. Intelligent operations platforms address this operational chaos by processing massive data volumes that overwhelm individual engineers during crises. Algorithmic models identify subtle system behaviors that signal developing problems, catching potential failures before they impact end users or cascade across service dependencies. These platforms adapt their detection capabilities based on observed incident histories and changing infrastructure patterns. Organizations deploying intelligent operations report substantial improvements in incident response metrics. Automated correlation eliminates hours of manual investigation, while predictive analytics enable proactive maintenance during scheduled windows rather than emergencies. Teams finally escape the constant firefighting that prevents strategic infrastructure improvements and architectural optimization.

1. Introduction

DevOps changed how teams build software by tearing down walls between developers and operations staff. Yet managing incidents in today's complex systems creates headaches that manual processes can't solve. Modern cloud environments dump enormous amounts of data on engineers who struggle to separate real problems from routine system noise [1]. Most organizations handle incidents badly. Something breaks, alerts flood the operations center, and teams waste hours figuring out what actually happened while customers complain about slow service. Engineers burn out from constant firefighting instead of building better systems that prevent future problems.The situation gets worse as companies adopt microservices and multi-cloud architectures. Applications are spread across hundreds of components in different regions, making it impossible to understand failure patterns manually. When cascading outages occur, teams scramble to correlate events across dozens of monitoring tools while business operations suffer. Traditional monitoring relies on simple rules that generate thousands of useless alerts daily. These systems miss subtle problems while overwhelming teams with false positives about normal system variations. Operations staff spend most of their time investigating alerts that turn out to be nothing rather than focusing on architectural improvements that would prevent real issues [2].Intelligent operations platforms address these problems by automatically processing data volumes that overwhelm human operators. Machine learning algorithms identify patterns indicating genuine problems while filtering out routine system behaviors. These tools learn from past incidents to catch similar issues faster and suggest remediation strategies that worked before. The transformation shifts teams from reactive crisis response to proactive system management. Engineers can plan maintenance

during scheduled windows instead of responding to emergencies at three in the morning. Early adopters report significant improvements in system reliability while reducing the stress and burnout associated with traditional incident response practices.

1.1 AIOps Architecture Framework

Intelligent operations platforms combine several technology components that work together to make sense of complex system data. Collection systems gather information from applications, infrastructure, network devices, and synthetic monitoring tools scattered across different environments. Getting complete visibility requires connecting to dozens of different data sources that use various formats and protocols [6].Processing engines apply algorithms to incoming data streams, looking for patterns that indicate problems developing before they impact users. Computational platforms must process enormous information flows while maintaining response speeds that matter during live incidents. The critical balance involves managing processing capacity against latency requirements in situations where slow detection transforms minor issues into widespread service failures.Storage systems keep historical data needed for training algorithms and providing context during investigations. Time-series databases optimize for the high write volumes typical in monitoring environments while enabling fast queries across long time periods. The architecture must scale as organizations grow their infrastructure and generate more operational data.Integration layers connect intelligent platforms with existing tools that teams already use for monitoring, ticketing, communication, and automation. Rather than replacing everything, successful implementations enhance current workflows with smarter capabilities. Standard APIs ensure compatibility across diverse technology environments without requiring extensive customization work [7].User interfaces present insights through dashboards and alerts that help teams understand what's happening during both normal operations and crises. The design challenge involves showing enough detail for effective troubleshooting while avoiding information overload that slows down response during high-pressure incidents.

1.2 Machine Learning Integration Patterns

Different organizations implement machine learning based on their specific needs, data quality, and infrastructure complexity. Supervised learning works well when teams maintain detailed incident records with clear root cause information and resolution outcomes. These models learn from past problems to classify new events and predict potential failures before they happen [3].Unsupervised methods discover operational patterns without requiring labeled training data from past incidents. These algorithms organize similar system behaviors into clusters while identifying unusual activity that differs from established normal operations. The capability proves especially useful for spotting previously unknown failure modes and gaining insights into system performance under varying operational scenarios.Time-series forecasting examines metric trends to predict resource usage and capacity needs. Teams can make scaling decisions proactively and schedule maintenance during low-traffic periods. Accuracy improves as models process longer historical periods and account for seasonal patterns in application usage.Natural language processing converts unstructured log files into information suitable for algorithmic analysis. Text classification sorts log entries by severity and component, while extraction techniques pull out relevant technical details. This enables a comprehensive analysis of application logs that would otherwise require tedious manual review [4].Reinforcement learning optimizes automated response strategies by learning from previous remediation outcomes. Models adapt their recommendations based on which actions succeeded or failed in similar situations. The continuous improvement cycle enables increasingly sophisticated automated responses while maintaining safety controls that prevent potentially harmful actions during critical incidents.

2. Anomaly Detection Mechanisms

Identifying system problems before they escalate requires distinguishing genuine issues from normal operational variations that constantly occur across distributed infrastructure environments. Traditional monitoring generates excessive alerts during routine system changes while missing subtle behavioral shifts indicating serious problems developing beneath surface-level metrics. Teams waste significant time investigating false positives rather than addressing actual threats to system stability [9].Intelligent detection establishes dynamic performance baselines that evolve alongside changing system characteristics, infrastructure modifications, and application deployment patterns. These adaptive mechanisms reduce alert noise by understanding routine maintenance activities, traffic fluctuations, and seasonal usage variations that trigger conventional threshold-based monitoring systems unnecessarily.Correlation engines examine relationships between diverse metrics to identify

complex failure scenarios affecting multiple system components simultaneously. Isolated CPU spikes appear benign until combined with memory pressure, increased network latency, and database connection pool exhaustion patterns. E-commerce platforms naturally experience traffic surges during promotional events, while business applications demonstrate that Cross-dimensional analysis exposes systemic problems that individual metric monitoring misses entirely during operational emergencies. Time-based pattern analysis distinguishes normal cyclical system behaviors from actual anomalies by understanding contextual timing relationships within detection frameworks. Predictable usage patterns during standard working hours. Detection systems account for these expected variations rather than generating unnecessary alerts for normal operational cycles [12].Ensemble methodologies combine multiple detection algorithms to improve accuracy while minimizing false alarm rates. Different techniques excel under varying operational conditions, so aggregated approaches provide more reliable threat identification with confidence scoring mechanisms that help operations teams prioritize their response efforts effectively during high-pressure incident scenarios.

2.1 Automated Root Cause Analysis

Determining failure origins traditionally requires experienced engineers to manually correlate events across numerous systems while working under intense pressure during active service disruptions. This investigative process consumes valuable resolution time while affected services remain degraded, and business operations experience continued impact from ongoing problems. Automated correlation systems eliminate much of this manual detective work through intelligent event analysis [5]. Dependency graph analysis traces failure propagation patterns through complex distributed architectures by mapping interconnections between system components, data flows, and service relationships. When symptoms appear across multiple services simultaneously, correlation algorithms identify originating failure points by analyzing component dependencies and communication pathways.Temporal sequence analysis examines event timing relationships to establish causal connections between initial failures and subsequent system symptoms. Problems typically manifest through predictable progression patterns where root causes trigger related effects across various infrastructure components within specific time intervals. Machine learning models recognize these sequential relationships from historical incident data to automatically identify similar patterns during new operational disruptions [11].Log correlation transforms unstructured error messages and system notifications into actionable diagnostic information by extracting relevant technical details and categorizing problem types. Natural language processing techniques identify recurring error patterns while semantic analysis groups related issues expressed through different terminology but representing identical underlying system failures. Historical pattern matching compares current incident characteristics to previous cases with documented root causes and successful resolution strategies. Knowledge databases maintain comprehensive records of past problems along with proven diagnostic procedures and effective remediation approaches that enable faster problem resolution during similar future incidents.

2.2 Intelligent Remediation Strategies

Automated problem resolution transforms incident response from manual troubleshooting procedures into systematic remediation using established operational playbooks and adaptive response mechanisms. Standard remediation actions, including service restarts, cache invalidation, and resource scaling, address many routine operational issues without requiring direct human intervention during critical business hours [8]. Procedural automation handles well-documented incident categories with proven resolution workflows that eliminate manual diagnostic steps for common system problems. When specific error conditions match established remediation criteria, automated systems execute appropriate corrective actions immediately rather than waiting for human operators to identify problems and implement solutions manually.Adaptive learning algorithms optimize remediation effectiveness by evaluating historical success rates across different incident scenarios and system configurations. These algorithms continuously refine their response recommendations based on documented outcomes from previous remediation attempts, enabling increasingly sophisticated automated responses while maintaining strict safety boundaries [10]. Progressive escalation implements graduated response strategies beginning with conservative interventions before attempting more aggressive remediation procedures. Initial automated responses focus on low-risk actions such as cache clearing and individual component restarts. When preliminary interventions fail to resolve operational problems, systems escalate to more significant corrective measures, including service failovers and infrastructure scaling operations. Human oversight frameworks ensure automated remediation operates

within acceptable operational risk parameters while providing manual intervention capabilities for complex scenarios requiring contextual judgment. Approval mechanisms require explicit human authorization for high-impact remediation actions while permitting immediate execution of routine corrective procedures during standard operational conditions.

3. Performance Optimization Outcomes

Organizations implementing intelligent operations report substantial improvements in operational metrics that directly impact business performance and customer satisfaction. Mean time to detection decreases dramatically when automated pattern recognition identifies developing problems before they escalate into service disruptions. Teams catch issues during early development phases rather than after customers experience degraded performance or complete service outages [1].Resolution times improve significantly as automated correlation eliminates hours of manual investigation that previously consumed engineering resources during critical incidents. Engineers spend less time hunting through disparate monitoring tools and log files while automated systems provide targeted insights about failure origins and recommended remediation strategies. This efficiency gain allows teams to restore services faster while reducing the business impact associated with extended outages.False positive reduction transforms operational workflows by eliminating alert fatigue that overwhelms monitoring teams with irrelevant notifications. Traditional threshold-based monitoring generates thousands of alerts daily, most representing normal system variations rather than genuine problems requiring immediate attention. Intelligent filtering reduces alert volumes by identifying patterns that distinguish routine operational changes from actual threats requiring investigation.Resource optimization develops naturally when teams transition from emergency response patterns toward strategic capacity management and architectural improvement activities. Engineering staff who previously handled constant operational crises can redirect attention toward system enhancements, performance optimization, and scaling strategies that address root causes of recurring problems. This forward-thinking orientation creates cumulative improvements where systems gain resilience and operational efficiency through sustained development efforts [12].Operational cost reduction occurs through multiple mechanisms, including reduced overtime expenses, decreased infrastructure waste, and improved resource allocation efficiency. Automated incident response eliminates night-shift escalations for routine problems while predictive analytics enable right-sized infrastructure provisioning that avoids both over-provisioning costs and under-provisioning performance problems.Team productivity increases as engineers develop expertise in strategic system design rather than spending careers managing operational crises. Knowledge retention improves when institutional wisdom gets captured in automated playbooks and correlation rules rather than remaining trapped in individual experience. This systematization enables more consistent incident response while reducing dependencies on specific team members during critical operational periods.

Table 1: *AIOps Implementation Components [1,6]*

Component	Description
Data Collection Layer	Aggregates telemetry from applications, infrastructure, and network sources
Processing Engine	Applies machine learning algorithms for real-time pattern analysis
Storage System	Maintains historical operational data for model training and context
Integration APIs	Connects with existing monitoring, ticketing, and automation tools
Visualization Interface	Presents insights through dashboards and alert management systems
Correlation Engine	Identifies relationships between events across distributed components

Table 2: *Machine Learning Detection Methods [3,9]*

Method	Application
Supervised Learning	Classifies incidents using labeled historical data
Unsupervised Clustering	Groups similar system behaviors without training labels

Time-Series Forecasting	Predicts resource utilization and capacity requirements
Anomaly Detection	Identifies outliers deviating from established baselines
Natural Language Processing	Converts unstructured logs into structured information
Ensemble Techniques	Combines multiple algorithms for improved accuracy

Table 3: *Root Cause Analysis Techniques [5,11]*

Technique	Purpose
Dependency Mapping	Traces failure propagation through system components
Temporal Correlation	Examines timing relationships between related events
Log Pattern Analysis	Extracts technical details from unstructured error messages
Similarity Matching	Compares incidents to historical cases with known solutions
Graph-Based Analysis	Maps the interconnections between distributed services
Sequence Recognition	Identifies recurring failure progression patterns

Table 4: *Automated Remediation Approaches [8,10]*

Approach	Implementation
Rule-Based Automation	Executes predefined actions for known incident patterns
Progressive Escalation	Starts with conservative fixes before aggressive interventions
Adaptive Learning	Optimizes strategies based on historical success outcomes
Safety Controls	Requires human approval for high-impact remediation actions
Rollback Mechanisms	Automatically reverses failed remediation attempts
Context-Aware Actions	Considers business hours and system criticality levels

4. Conclusions

Intelligent incident management fundamentally changes DevOps operations by automating the tedious correlation work that consumes most operational effort. Teams implementing these technologies achieve faster problem resolution while escaping the reactive cycle that prevents meaningful infrastructure improvements. The shift reaches beyond faster incident resolution to reshape how engineering teams operate and plan strategically. Operations staff can dedicate attention to architectural improvements and failure prevention rather than spending entire shifts investigating alerts and troubleshooting emergencies. Intelligent platforms manage repetitive data processing tasks while engineers apply experience and judgment to design decisions that strengthen system resilience over time. Successful deployment requires distinguishing between tasks where algorithms perform reliably and scenarios demanding human oversight. Model accuracy depends entirely on the quality of historical data available for training, forcing organizations to establish comprehensive monitoring before expecting dependable automated responses.

Computational systems excel when processing predictable patterns within structured datasets, but encounter serious limitations during unusual incidents that require understanding business context and operational constraints beyond pure technical metrics. Unusual incidents frequently involve the most serious operational challenges where human expertise becomes essential for resolution. Technological capabilities advance continuously, but the basic relationship between automated data processing and human decision-

making stays unchanged across various operational contexts. Platforms handle massive information volumes that overwhelm individual cognitive capacity, while experienced engineers provide strategic thinking and institutional knowledge required for complex decisions involving technical specifications alongside business objectives and regulatory requirements. AI applied in different fields as reported in the literature [13-24].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Osinaka Desmond, "Transforming DevOps with artificial intelligence: A deep dive into intelligent automation, predictive analytics, and resilient system design," World Journal of Advanced Research and Reviews, ResearchGate, Jul. 2023. https://www.researchgate.net/publication/388215586_Transforming_DevOps_with_artificial_intelligence_A_deep_dive_into_intelligent_automation_predictive_analytics_and_resilient_system_design

[2] Sumanth Tatineni, "AIOps in Cloud-native DevOps: IT Operations Management with Artificial Intelligence," Journal of Artificial Intelligence & Cloud Computing, ResearchGate, Mar. 2023.https://www.researchgate.net/publication/377614566_AIOps_in_Cloud-native_DevOps_IT_Operations_Management_with_Artificial_Intelligence

[3] Syed Imran Abbas and Ankit Garg, "AIOps in DevOps: Leveraging Artificial Intelligence for Operations and Monitoring," in 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), ResearchGate, Mar. 2024.https://www.researchgate.net/publication/382580085_AIOps_in_DevOps_Leveraging_Artificial_Intelligence_for_Operations_and_Monitoring

[4] Subrahmanyasarma Chitta et al., "AIOps: Integrating AI and Machine Learning into IT Operations," ResearchGate, Jan. 2024.https://www.researchgate.net/publication/389136333_AIOps_Integrating_AI_and_Machine_Learning_into_IT_Operations#

[5] Arturo Peralta et al., "Intelligent Incident Management Leveraging Artificial Intelligence, Knowledge Engineering, and Mathematical Models in Enterprise Operations," MDPI, Mar. 2025.https://www.mdpi.com/2227-7390/13/7/1055

[6] Răzvan Daniel Zota et al., "A Practical Approach to Defining a Framework for Developing an Agentic AIOps System," MDPI, Apr. 2025.https://www.mdpi.com/2079-9292/14/9/1775

[7] Romina Eramo et al., "An architecture for model-based and intelligent automation in DevOps," ScienceDirect, Aug. 2024.https://www.sciencedirect.com/science/article/pii/S0164121224002255

[8] Jithendra Prasad Reddy Baswareddy, "Intelligent CI/CD Pipelines: Leveraging AI for Predictive Maintenance and Incident Management," European Journal of Computer Science and Information Technology, Apr. 2025.https://eajournals.org/ejcsit/wp-content/uploads/sites/21/2025/04/Intelligent-CI-CD-Pipelines.pdf

[9] Bhanu Prakash Kolli, "AI-Powered DevOps: Enhancing Cloud Automation with Intelligent Observability," European Journal of Computer Science and Information Technology, Apr. 2025.https://eajournals.org/ejcsit/wp-content/uploads/sites/21/2025/04/AI-Powered-DevOps.pdf

[10] Sai Prasad Veluru, "Leveraging AI and ML for Automated Incident Resolution in Cloud Infrastructure," International Journal of Artificial Intelligence, Data Science and Machine Learning, May 2025. https://ijaidsml.org/index.php/ijaidsml/article/view/143

[11] Youcef Remil et al., "AIOps Solutions for Incident Management: Technical Guidelines and A Comprehensive Literature Review," arXiv, Apr. 2023. https://arxiv.org/html/2404.01363v1

[12] Qian Cheng et al., "AI for IT Operations (AIOps) on Cloud Platforms: Reviews, Opportunities and Challenges," arXiv, 2023. https://arxiv.org/pdf/2304.04661

[13] García, R., Carlos Garzon, & Juan Estrella. (2025). Generative Artificial Intelligence to Optimize Lifting Lugs: Weight Reduction and Sustainability in AISI 304 Steel. International Journal of Applied Sciences and Radiation Research , 2(1). https://doi.org/10.22399/ijasrar.22

[14] Chui, K. T. (2025). Artificial Intelligence in Energy Sustainability: Predicting, Analyzing, and Optimizing Consumption Trends. *International Journal of Sustainable Science*

and Technology, *3*(1). https://doi.org/10.22399/ijsusat.1

[15] ttia Hussien Gomaa. (2025). From TQM to TQM 4.0: A Digital Framework for Advancing Quality Excellence through Industry 4.0 Technologies. *International Journal of Natural-Applied Sciences and Engineering*, *3*(1). https://doi.org/10.22399/ijnasen.21

[16]M.K. Sarjas, & G. Velmurugan. (2025). Bibliometric Insight into Artificial Intelligence Application in Investment. *International Journal of Computational and Experimental Science and Engineering*, *11*(1). https://doi.org/10.22399/ijcesen.864

[17] Attia Hussien Gomaa. (2025). Value Engineering in the Era of Industry 4.0 (VE 4.0): A Comprehensive Review, Gap Analysis, and Strategic Framework. *International Journal of Natural-Applied Sciences and Engineering*, *3*(1). https://doi.org/10.22399/ijnasen.22

[18]Ibeh, C. V., & Adegbola, A. (2025). AI and Machine Learning for Sustainable Energy: Predictive Modelling, Optimization and Socioeconomic Impact In The USA. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.19

[19]ZHANG, J. (2025). Artificial intelligence contributes to the creative transformation and innovative development of traditional Chinese culture. *International Journal of Computational and Experimental Science and Engineering*, *11*(1). https://doi.org/10.22399/ijcesen.860

[20]Olola, T. M., & Olatunde, T. I. (2025). Artificial Intelligence in Financial and Supply Chain Optimization: Predictive Analytics for Business Growth and Market Stability in The USA. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.18

[21] Kumari, S. (2025). Machine Learning Applications in Cryptocurrency: Detection, Prediction, and Behavioral Analysis of Bitcoin Market and Scam Activities in the USA. *International Journal of Sustainable Science and Technology*, *3*(1). https://doi.org/10.22399/ijsusat.8

[22] S. Menaka, & V. Selvam. (2025). Bibliometric Analysis of Artificial Intelligence on Consumer Purchase Intention in E-Retailing. *International Journal of Computational and Experimental Science and Engineering*, *11*(1). https://doi.org/10.22399/ijcesen.1007

[23] Harsha Patil, Vikas Mahandule, Rutuja Katale, & Shamal Ambalkar. (2025). Leveraging Machine Learning Analytics for Intelligent Transport System Optimization in Smart Cities. *International Journal of Applied Sciences and Radiation Research* , *2*(1). https://doi.org/10.22399/ijasrar.38

[24]G. Prabaharan, S. Vidhya, T. Chithrakumar, K. Sika, & M.Balakrishnan. (2025). AI-Driven Computational Frameworks: Advancing Edge Intelligence and Smart Systems. *International Journal of Computational and Experimental Science and Engineering*, *11*(1). https://doi.org/10.22399/ijcesen.1165