

Agentic AI for Autonomous Incident Prioritization and Intelligent Alert Correlation in Enterprise Monitoring Systems

Subodh Jain

Computer Science

RKDF IST Bhopal

DR. GIRDHAR GOPAL LADHA

Computer Science

RKDF IST Bhopal

Abstract

Modern enterprise monitoring environments generate enormous volumes of alerts, telemetry streams, logs, and operational events from distributed infrastructure, cloud-native workloads, middleware services, virtualization platforms, and enterprise applications. This paper proposes an Agentic AI Framework for Autonomous Incident Prioritization and Intelligent Alert Correlation in Enterprise Monitoring Systems. The framework introduces specialized AI agents responsible for alert ingestion, noise reduction, telemetry aggregation, dependency correlation, severity classification, business impact assessment, escalation recommendation, and autonomous operational reasoning.

Keywords

Agentic AI, Alert Correlation, Incident Prioritization, AIOps, Enterprise Monitoring, Multi-Agent AI, Intelligent Operations

1. Introduction

Enterprise monitoring systems generate massive operational telemetry across hybrid cloud infrastructure, Kubernetes platforms, middleware ecosystems, APIs, and enterprise applications. Traditional monitoring approaches struggle with alert fatigue, duplicate incidents, and fragmented telemetry. AI-driven operational intelligence presents opportunities for intelligent incident prioritization and autonomous alert correlation.

2. Literature Review

Traditional enterprise monitoring relies on threshold-based alerting and manually configured escalation workflows. AIOps systems introduced anomaly detection and operational analytics; however, many existing systems still require substantial human intervention. Multi-agent AI architectures enable collaborative operational reasoning and adaptive orchestration.

3. Problem Statement

Modern monitoring environments face operational challenges including excessive alert volumes, fragmented telemetry, slow incident prioritization, weak dependency awareness, and reactive workflows. These issues increase operational overhead and delay remediation activities.

4. Proposed Agentic AI Framework

The proposed framework introduces specialized AI agents including Alert Ingestion Agent, Noise Reduction Agent, Dependency Correlation Agent, Severity Classification Agent, Business Impact Assessment Agent, Incident Reasoning Agent, Escalation Recommendation Agent, and Governance Agent.

5. Methodology

The research adopts a conceptual comparative evaluation methodology using enterprise operational scenarios including Kubernetes failures, middleware degradation, distributed application outages, and API gateway instability.

6. Autonomous Incident Prioritization Algorithm

Step 1: Collect telemetry. Step 2: Filter duplicate alerts. Step 3: Correlate incidents using dependency intelligence. Step 4: Classify severity. Step 5: Determine business impact. Step 6: Generate escalation recommendations. Step 7: Monitor incident progression.

7. Comparative Evaluation

The conceptual evaluation indicates reductions in alert noise, faster incident prioritization, improved dependency awareness, and lower Mean Time to Resolution (MTTR) when compared with traditional monitoring workflows.

8. Benefits

Key advantages include improved operational efficiency, intelligent alert grouping, reduced alert fatigue, standardized escalation, and enhanced enterprise resilience.

9. Challenges and Limitations

Challenges include hallucination risk, incomplete telemetry, governance concerns, integration complexity, and trust barriers in autonomous operational systems.

10. Future Scope

Future work includes predictive incident prevention, reinforcement learning optimization, AI-driven SRE automation, and self-healing infrastructure integration.

11. Conclusion

The proposed agentic AI framework demonstrates strong potential for transforming enterprise monitoring systems into intelligent autonomous operational ecosystems capable of advanced alert correlation and autonomous incident prioritization.

References

- [1] Russell, S., & Norvig, P. Artificial Intelligence: A Modern Approach.
- [2] Wooldridge, M. An Introduction to MultiAgent Systems.
- [3] Gartner Research on AIOps.
- [4] The DevOps Handbook.
- [5] Research papers on AI-driven incident management.

Architecture Diagram



