The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.06 Issue 01 2026
PAGE NO. 138-143

Adaptive AI-Driven Frameworks for Dependency Vulnerability Mitigation in Large-Scale Enterprise Systems

Johnathan Meyer

University of Vienna, Austria

Received: 01 January 2026; **Accepted:** 16 January 2026; **Published:** 31 January 2026

Abstract: The rapid evolution of enterprise information systems, coupled with increased reliance on interconnected digital infrastructures, has amplified the complexity and susceptibility of software ecosystems to dependency vulnerabilities. These vulnerabilities, if unaddressed, can propagate across systems, resulting in operational disruption, financial loss, and reputational damage. This research critically examines AI-assisted approaches to identifying, mitigating, and resolving dependency vulnerabilities in large-scale enterprise systems. Building upon the theoretical foundation of machine learning, data analytics, and autonomous system design, the study integrates multiple perspectives from supply chain risk management, cloud-native architectures, cybersecurity protocols, and healthcare informatics to construct a comprehensive model for proactive vulnerability management. The study employs qualitative synthesis of secondary research and extensive case analysis of enterprise systems, emphasizing real-time dependency monitoring, automated patch application, and predictive risk modeling. The findings indicate that AI-powered interventions significantly enhance resilience by reducing detection latency, optimizing resource allocation for remediation, and enabling predictive forecasting of potential vulnerability exploitations. Moreover, the integration of AI within enterprise dependency frameworks facilitates adaptive learning from historical incidents, improves interdepartmental coordination, and provides actionable insights to stakeholders for decision-making under uncertainty. The study highlights critical theoretical debates surrounding ethical AI deployment, explainability, and risk governance, positioning AI-assisted vulnerability resolution as a strategic imperative for sustainable enterprise operations. The research concludes by outlining future directions for hybrid human-AI governance, enhanced interpretability frameworks, and the development of standardized metrics for AI effectiveness in enterprise dependency management.

Keywords: AI-Assisted Vulnerability, Enterprise Systems, Dependency Resolution, Predictive Risk Modeling, Cybersecurity, Cloud-Native Architectures, Resilient Systems

INTRODUCTION

In contemporary enterprise environments, the integration of complex software modules, third-party libraries, and distributed services has created an intricate network of interdependencies that simultaneously offers functional efficiency and exposes systems to heightened vulnerability. Dependency vulnerabilities—flaws originating from software libraries, modules, or interconnected services—pose a formidable challenge to large-scale enterprise systems, given their cascading potential to compromise system stability, data integrity, and operational continuity (Kathi, 2025). Historically, enterprises relied on reactive approaches, such as manual patching or periodic auditing, which often failed to account for the dynamic nature of software evolution and the increasing sophistication of cyber threats (Kolluri, 2024).

The theoretical underpinnings of dependency vulnerability management can be traced to the convergence of multiple disciplines, including software engineering, risk management, and artificial intelligence. The principles of software modularity and dependency inversion dictate that each software component should maintain minimal coupling while maximizing cohesion, thereby mitigating the propagation of defects (Behnam Fahimnia et al., 2015). However, in practice, enterprises rarely achieve such idealized modularity due to legacy constraints, heterogeneous technological stacks, and strategic acquisitions, resulting in complex dependency networks that amplify vulnerability exposure (Vikash

et al., 2020).

The advent of artificial intelligence (AI) and machine learning (ML) introduces transformative capabilities in addressing these challenges. AI-assisted frameworks enable predictive modeling of potential vulnerabilities, dynamic prioritization of patches, and automated resolution workflows, thereby reducing human error and enhancing system resilience (Boppiniti, 2022). The integration of AI also facilitates real-time monitoring and anomaly detection, leveraging historical data patterns, runtime logs, and behavioral analytics to forecast latent vulnerabilities before they manifest as operational disruptions (Gatla, 2020).

Despite the recognized potential of AI, several theoretical debates persist regarding the scope, ethics, and governance of automated vulnerability mitigation. Scholars argue that the opaque nature of AI decision-making may introduce secondary risks, such as misprioritization of critical patches or inadvertent system incompatibilities (Kolluri, 2015). Additionally, the interplay between AI-driven automation and human oversight raises questions regarding accountability, interpretability, and the trade-offs between operational efficiency and systemic transparency (Boppiniti, 2023). This study engages with these debates, situating AI-assisted dependency management within a broader discourse of risk governance, supply chain resilience, and enterprise cybersecurity.

A critical literature gap exists in the holistic synthesis of AI methodologies for dependency vulnerability resolution, particularly in the context of large-scale, heterogeneous enterprise systems. While studies have examined AI applications in cybersecurity, real-time stream processing, and healthcare informatics individually (Pindi, 2017; Vikash et al., 2020), few analyses provide an integrated framework that addresses the multidimensional nature of dependencies across software, operational processes, and human oversight (Kathi, 2025). Moreover, existing research often emphasizes reactive remediation over predictive resilience, failing to leverage AI's potential for anticipatory risk management (Katsaliaki et al., 2022).

This research addresses this lacuna by developing a comprehensive AI-assisted framework for dependency vulnerability resolution. The study emphasizes three critical dimensions: (1) predictive detection of dependency vulnerabilities through machine learning algorithms and pattern recognition, (2) automated prioritization and resolution of identified vulnerabilities within enterprise architectures, and (3) ethical and governance considerations in deploying AI within high-stakes operational environments. The research builds upon prior insights into cloud-native, cloud-enabled, and cloud-agnostic digital transformation strategies to contextualize AI's role in enterprise resilience (Pratik Jain et al., 2024). The methodology synthesizes cross-disciplinary perspectives, integrating insights from supply chain risk management, cybersecurity, AI in healthcare, and robotics to construct a theoretically rigorous and practically applicable model.

By situating the investigation at the intersection of AI, enterprise systems, and dependency management, this study contributes to both theoretical discourse and operational practice. It addresses the pressing need for predictive, adaptive, and ethically governed solutions in managing dependency vulnerabilities, a domain that has grown exponentially in importance with the proliferation of complex enterprise infrastructures (Gatla, 2018). In doing so, the study positions AI not merely as a technical intervention but as a strategic tool for fostering organizational resilience, ensuring operational continuity, and mitigating systemic risks across digital ecosystems.

Methodology

This study adopts a multi-layered qualitative research design grounded in comprehensive secondary data analysis and interpretive synthesis. The methodology integrates theoretical modeling, comparative literature analysis, and applied case study examination to construct a robust framework for AI-assisted dependency vulnerability resolution. The research framework is structured into three sequential stages: data acquisition and system mapping, AI-driven predictive modeling, and resolution strategy assessment.

The initial stage involves detailed mapping of enterprise dependency networks, leveraging publicly available and proprietary secondary sources, including system architecture reports, vulnerability disclosure databases, and peer-reviewed literature (Kathi, 2025). Each dependency relationship is coded based on component criticality, historical failure frequency, and interconnectivity, providing a granular understanding of vulnerability propagation potential. This mapping process incorporates principles from supply chain risk modeling, emphasizing systemic interdependencies and cascading failure mechanisms (Behnam Fahimnia et al., 2015).

In the predictive modeling stage, machine learning algorithms, including supervised and unsupervised classification techniques, are employed to identify patterns indicative of emerging vulnerabilities (Boppiniti, 2022). Historical incident logs serve as the primary dataset, capturing metrics such as patch application latency, severity scoring, and system downtime. Feature engineering is applied to normalize heterogeneous data types, including categorical dependency classifications, continuous performance metrics, and textual descriptions of system alerts (Vikash et al., 2020). Model evaluation is conducted through cross-validation and sensitivity analysis, ensuring robustness and minimizing the risk of overfitting.

The resolution strategy assessment stage examines AI-driven intervention mechanisms, focusing on automated patch deployment, risk prioritization, and decision support integration. AI agents simulate patch application sequences, identifying optimal strategies for mitigating vulnerabilities while preserving system stability (Gatla, 2024). The study also critically evaluates governance mechanisms, including human-in-the-loop oversight, interpretability constraints, and ethical compliance considerations (Boppiniti, 2023). Limitations of the methodology include reliance on secondary datasets, potential biases inherent in publicly reported incidents, and the challenge of generalizing findings across diverse enterprise contexts.

Methodologically, the study employs triangulation by integrating insights from cybersecurity, cloud computing, and healthcare informatics, thereby enhancing internal validity and offering a multi-dimensional perspective on vulnerability management (Kolluri, 2016; Pindi, 2018). Ethical considerations, particularly regarding AI deployment in sensitive operational domains, are explicitly addressed through adherence to contemporary standards for responsible AI, including transparency, fairness, and accountability (Boppiniti, 2023).

Results

The analysis reveals that AI-assisted interventions substantially improve detection, prioritization, and resolution of dependency vulnerabilities in large-scale enterprise systems. Predictive models demonstrate high accuracy in identifying high-risk dependencies before exploitation, with AI-driven classification outperforming traditional rule-based approaches by 34–46% across multiple case studies (Kathi, 2025). The models also reduce response latency, allowing organizations to implement corrective measures within a significantly shortened window compared to manual processes (Kolluri, 2024).

Automated patch management simulations indicate that AI prioritization strategies minimize systemic disruption by identifying the sequence of patches that addresses the highest-risk dependencies while preserving operational continuity (Gatla, 2024). Integration of anomaly detection algorithms facilitates early identification of emerging vulnerabilities, particularly in cloud-native and hybrid cloud environments, where dependency dynamics are highly volatile (Pratik Jain et al., 2024).

The study also observes that AI implementation enhances cross-functional communication and decision-making, as predictive insights are translated into actionable intelligence for IT operations, risk management, and executive governance teams (Boppiniti, 2022). Ethical deployment frameworks, emphasizing explainable AI and human oversight, ensure that autonomous actions do not compromise organizational accountability or stakeholder trust (Kolluri, 2015).

Moreover, comparative analysis indicates that AI-driven approaches outperform conventional methods in reducing downtime and mitigating financial and operational losses associated with dependency vulnerabilities. Specifically, enterprises employing AI frameworks reported a 28% decrease in system outages and a 22% reduction in unplanned maintenance expenditure over a 12-month observation period (Vikash et al., 2020). These outcomes substantiate the theoretical proposition that AI integration fosters adaptive resilience by learning from historical incidents and dynamically adjusting mitigation strategies.

Discussion

The findings underscore the theoretical and practical significance of AI-assisted dependency vulnerability resolution in complex enterprise systems. From a theoretical perspective, the research confirms that AI facilitates predictive risk management by leveraging historical incident data, system performance metrics, and dependency mapping to generate actionable insights (Kathi, 2025). This aligns with the broader discourse on proactive enterprise risk governance, where predictive modeling and real-time analytics are central to resilience-building strategies (Katsaliaki et al., 2022).

Scholarly debates concerning the balance between automation and human oversight are particularly pertinent in this context. While AI algorithms provide rapid, data-driven recommendations, interpretability challenges and ethical considerations necessitate human-in-the-loop mechanisms to validate decisions and ensure accountability (Boppiniti, 2023; Kolluri, 2015). The study's integrated framework addresses this by combining autonomous detection and remediation with human validation, thereby mitigating the risk of erroneous interventions that could exacerbate system vulnerabilities.

The research also highlights the significance of contextualizing AI interventions within broader enterprise digital transformation strategies. Cloud-native, cloud-enabled, and cloud-agnostic architectures exhibit distinct dependency profiles and vulnerability patterns, necessitating adaptive AI models tailored to architectural characteristics (Pratik Jain et al., 2024). By incorporating these nuances, the proposed framework ensures that AI interventions are both context-sensitive and strategically aligned with organizational objectives.

From a practical standpoint, the study reveals that AI-assisted vulnerability management contributes to operational efficiency, cost reduction, and enhanced resilience. Enterprises implementing predictive dependency monitoring and automated patch deployment report measurable improvements in system reliability and stakeholder confidence (Gatla, 2020; Pindi, 2017). The integration of ethical and explainable AI principles further reinforces trust, particularly in high-stakes domains such as healthcare informatics, financial services, and critical infrastructure (Kolluri, 2016; Boppiniti, 2023).

Counterarguments regarding the overreliance on AI merit attention. Critics contend that excessive dependence on automated systems may obscure latent vulnerabilities, reduce human expertise, and introduce systemic blind spots (Kolluri, 2014). This study addresses these concerns by advocating a hybrid governance model, emphasizing continuous human oversight, scenario-based validation, and periodic audit of AI decision-making processes. Such an approach ensures that AI functions as a strategic augmentation tool rather than an uncritical replacement of human judgment.

The research also contributes to ongoing discussions on supply chain resilience and systemic risk propagation. Drawing analogies between software dependencies and supply chain interdependencies, the study underscores that vulnerabilities in one module can cascade across the enterprise, amplifying potential damage (Behnam Fahimnia et al., 2015). AI frameworks capable of simulating these cascading effects and optimizing intervention sequences offer novel avenues for minimizing systemic risk and enhancing organizational adaptability (Katsaliaki et al., 2022).

Furthermore, the study engages with emerging debates in AI ethics, data governance, and explainable machine learning. By embedding transparency, accountability, and ethical safeguards within AI-assisted frameworks, enterprises can reconcile the tension between operational efficiency and responsible technology deployment (Boppiniti, 2023). The research advocates the development of standardized metrics for evaluating AI performance, including accuracy, interpretability, and alignment with organizational risk thresholds, thereby providing a benchmark for future comparative studies.

Future research directions include the exploration of hybrid AI-human decision systems for real-time vulnerability resolution, advanced predictive modeling incorporating external threat intelligence feeds, and cross-industry comparative analyses to validate the generalizability of AI frameworks. Additionally, longitudinal studies are required to assess the sustainability of AI-assisted interventions and their long-term impact on enterprise resilience, operational costs, and cybersecurity posture (Gatla, 2018; Kolluri, 2024).

Conclusion

This study establishes the theoretical and practical efficacy of AI-assisted frameworks in managing dependency vulnerabilities within large-scale enterprise systems. By integrating predictive analytics, automated remediation, and ethical governance, the research demonstrates that AI significantly enhances system resilience, reduces operational risk, and facilitates proactive decision-making. The proposed framework bridges critical gaps in current literature by offering a holistic model that accounts for technological, organizational, and ethical dimensions of dependency management. The findings underscore the necessity of adopting adaptive, context-aware, and ethically governed AI solutions to ensure sustainable enterprise operations in increasingly complex digital ecosystems. Future investigations should extend this work by incorporating real-time adaptive learning mechanisms, cross-industry benchmarking, and advanced interpretability

frameworks, thereby consolidating AI's role as a strategic enabler of resilient enterprise infrastructures.

References

1. Kolluri, V. (2024). Cybersecurity challenges in telehealth services: Addressing the security vulnerabilities and solutions in the expanding field of telehealth. International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, 1(1), 23-33.
2. Gatla, T. R. (2018). Enhancing customer service in banks with AI chatbots: The effectiveness and challenges of using AI-powered chatbots for customer service in the banking sector. TIJER–TIJER–INTERNATIONAL RESEARCH JOURNAL, ISSN 2349-9249.
3. Kathi, S. R. (2025). AI-Assisted Dependency Vulnerability Resolution in Large-Scale Enterprise Systems. International Research Journal of Advanced Engineering and Technology, 2(07), 8-18.
4. Boppiniti, S. T. (2022). Exploring the Synergy of AI, ML, and Data Analytics in Enhancing Customer Experience and Personalization. International Machine Learning Journal and Computer Engineering, 5(5).
5. Vikash, et al. (2020). Performance evaluation of real-time stream processing systems for Internet of Things applications. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167739X20302636
6. Gatla, T. R. (2024). A next-generation device utilizing artificial intelligence for detecting heart rate variability and stress management. Journal Name, 20.
7. Kolluri, V. (2015). A comprehensive analysis on explainable and ethical machine: Demystifying advances in artificial intelligence. TIJER–TIJER–INTERNATIONAL RESEARCH JOURNAL, ISSN 2349-9249.
8. Pratik Jain, et al. (2024). A Comparative Analysis of Cloud-Native, Cloud-Enabled, and Cloud-Agnostic Digital Transformation. Available: https://www.researchgate.net/publication/381301192_A_Comparative_Analysis_of_Cloud-Native_Cloud-Enabled_and_Cloud-Agnostic_Digital_Transformation
9. Gatla, T. R. (2020). An in-depth analysis of towards truly autonomous systems: AI and robotics: The functions. IEJRD-International Multidisciplinary Journal, 5(5), 9.
10. Boppiniti, S. T. (2023). Data ethics in AI: Addressing challenges in machine learning and data governance for responsible data science. International Scientific Journal for Research, 5(5), 1-29.
11. Pindi, V. (2017). AI in rehabilitation: Redefining post-injury recovery. International Numeric Journal of Machine Learning and Robots, 1(1).
12. Kolluri, V. (2021). A comprehensive study on AI-powered drug discovery: Rapid development of pharmaceutical research. International Journal of Emerging Technologies and Innovative Research, ISSN 2349-5162.
13. Kolluri, V. (2016). An innovative study exploring revolutionizing healthcare with AI: Personalized medicine: Predictive diagnostic techniques and individualized treatment. International Journal of Emerging Technologies and Innovative Research, ISSN 2349-5162.
14. Gatla, T. R. (2018). Machine learning in detecting money laundering activities: Investigating the use of machine learning algorithms in identifying and preventing money laundering schemes. TIJER–TIJER–INTERNATIONAL RESEARCH JOURNAL, ISSN 2349-9249.
15. Yarlagadda, V. S. T. (2024). Machine learning for predicting mental health disorders: A data-driven approach to early intervention. International Journal of Sustainable Development in Computing Science, 6(4).
16. Katsaliaki, K., et al. (2022). Supply chain disruptions and resilience: a major review and future research agenda. Available: https://link.springer.com/article/10.1007/s10479-020-03912-1
17. Pindi, V. (2018). Natural language processing (NLP) applications in healthcare: Extracting valuable insights from unstructured medical data. International Journal of Innovations in Engineering Research and Technology, 5(3), 1-10
18. Behnam Fahimnia, et al. (2015). Quantitative models for managing supply chain risks: A review. Available: https://www.sciencedirect.com/science/article/abs/pii/S0377221715003276
19. Kolluri, V. (2024). Revolutionary research on the AI sentry: An approach to overcome social engineering attacks using machine intelligence. International Journal of Advanced Research and Interdisciplinary Scientific Endeavours, 1(1), 53-60.
20. Gatla, T. R. (2024). A next-generation device utilizing artificial intelligence for detecting heart rate variability and stress management. Journal Name, 20.
21. Boppiniti, S. T. (2022). Exploring the Synergy of AI, ML, and Data Analytics in Enhancing Customer

Experience and Personalization. International Machine Learning Journal and Computer Engineering, 5(5).

22. Kolluri, V. (2015). A comprehensive analysis on explainable and ethical

23. machine: Demystifying advances in artificial intelligence. TIJER–TIJER–INTERNATIONAL RESEARCH JOURNAL, ISSN 2349-9249.