International Journal of Sciences and Innovation Engineering
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: www.ijsci.com
Volume 3 Issue 2 , Feb 2026
E-ISSN : 3049-0251
DOI: https://doi.org/10.70849/ijsci03022610842

AI-Based Optimization Framework for Assessing Network Application Vulnerabilities in Enterprise Networks

Yashvant Dev[1], Dr. Kismat Chhillar[2], Dr. Deepak Tomar[3], Dr. Anil Kewat[4]
[1] *Research Scholar, Department of Mathematical Sciences and Computer Applications, Bundelkhand University, Jhansi, Uttar Pradesh, India*
[2,4] *Assistant Professor, Department of Mathematical Sciences and Computer Applications, Bundelkhand University, Jhansi, Uttar Pradesh, India*
[3] *System Analyst, Bundelkhand University, Jhansi, Uttar Pradesh, India*

Article Info

Article History:

Published:13 Feb 2026

Publication Issue:
Volume 3, Issue 2
February-2026

Page Number:
322-332

Corresponding Author:
Yashvant Dev

Abstract:

This research presents an advanced AI-powered framework designed to optimize vulnerability assessment within networked applications across organizational infrastructures. It directly addresses the increasing sophistication and complexity of contemporary cyber threats. The framework integrates a range of machine learning paradigms, including supervised, unsupervised, reinforcement, and deep learning techniques. Through these methods, it automates the processes of identifying, classifying, and prioritizing vulnerabilities by analyzing application behavior patterns and real-time network traffic. The optimization component of the framework enhances risk management by dynamically assigning priority levels to vulnerabilities based on their potential impact and likelihood of exploitation, thereby facilitating efficient and proactive security responses. Extensive simulations and experiments conducted on diverse datasets demonstrate the framework's ability to achieve higher accuracy, reduced false positives, and greater adaptability compared with conventional vulnerability assessment approaches. Moreover, this study tackles critical challenges such as model robustness against adversarial attacks, interpretability of AI decisions, maintenance of data integrity, and scalability across various deployment environments. Overall, the research contributes an intelligent and scalable solution that strengthens organizational network security, enabling timely threat mitigation and reinforcing the holistic cybersecurity posture.

Keywords: AI-driven security, network application vulnerabilities, vulnerability assessment, machine learning, optimization framework, organizational networks

1. Introduction

The increasing reliance on networked applications in organizational environments has elevated cybersecurity to a critical priority, particularly as modern threats continue to evolve in sophistication and complexity. Traditional vulnerability assessment methods, which depend primarily on manual scanning, signature-based detection, and periodic evaluations, are struggling to keep pace with the surge in zero-day exploits and emerging attack techniques [1] [2]. As organizations advance in their digital transformation journeys, there is a growing necessity for dynamic, automated, and intelligent systems capable of continuously monitoring, evaluating, and prioritizing vulnerabilities within networked applications. Artificial intelligence (AI) plays a pivotal role in this context due to its powerful capabilities in anomaly detection, pattern recognition, and predictive data analysis. This technological advancement has reshaped the landscape of vulnerability assessment by enabling security mechanisms that are more accurate, proactive, and efficient. AI-driven vulnerability

assessment leverages machine learning (ML) and optimization techniques to overcome the inherent limitations of conventional approaches [3]. Through the analysis of real-time system configurations, extensive network traffic data, and application logs, AI models can identify hidden vulnerabilities and subtle attack indicators that traditional techniques often overlook [4].

Furthermore, AI facilitates dynamic risk prioritization by incorporating contextual parameters such as exploit trends, asset criticality, and real-time threat intelligence, thereby enhancing the decision-making process for security teams. The shift from a reactive to a proactive approach in vulnerability management not only reduces exposure time but also enhances the efficiency of resource allocation for mitigation and patching efforts. This transition contributes to the development of more resilient and secure organizational networks capable of withstanding sophisticated cyberattacks. Issues related to scalability, model interpretability, data integrity, and the susceptibility of AI models to adversarial manipulation continue to complicate their deployment in real-world environments. Addressing these challenges requires a hybrid methodology that combines the analytical strength of AI with optimization strategies to ensure rational risk prioritization while maintaining essential human oversight. This research introduces a comprehensive framework that employs AI-driven optimization to automate, enhance, and streamline the assessment of network application vulnerabilities across organizational infrastructures.

The structure of the remaining paper is organized as follows. Section 2 presents a comprehensive review of the existing literature on vulnerability assessment techniques and the evolving role of artificial intelligence (AI) in cybersecurity. Section 3 clearly defines the problem statement and outlines the specific research objectives guiding this study. Section 4 elaborates on the detailed architecture of the proposed AI-driven framework, including its core modules for AI and optimization, along with the methods employed for data processing and management. The methodology is discussed in Section 5, which highlights the dataset selection, model training procedures, and evaluation metrics utilized in the experiments. Section 6 provides an in-depth presentation and discussion of the experimental results and comparative analyses, while also addressing the challenges and limitations encountered during the research. Section 7 concludes the study by summarizing the key contributions and findings. Finally, Section 8 suggests potential directions for future research aimed at further advancing AI-driven vulnerability assessment systems.

2. Literature Review

The field of vulnerability assessment has evolved significantly, transitioning from traditional manual and signature-based methods to advanced automated techniques that leverage the capabilities of artificial intelligence (AI). Conventional approaches relying on rule-based detection and static scanning have become increasingly inadequate in addressing the complexity and dynamism of modern networked applications and emerging cyber threats. In recent years, there has been a marked rise in the adoption of AI and machine learning (ML) for vulnerability detection, offering substantial advantages in terms of accuracy, automation, and the ability to identify previously unknown or zero-day vulnerabilities [5] [6]. Contemporary research highlights several prominent AI methodologies, including supervised learning for classifying network behaviors and identifying vulnerable code, unsupervised learning for detecting anomalies through deviations from normal patterns, and reinforcement learning for modeling interactions between defenders and adversaries to enable proactive risk assessment [7] [8]. Although AI models have gained considerable momentum in this domain, several challenges persist, notably concerning dataset quality, model interpretability, and result reproducibility. Addressing these issues is vital to ensuring the reliability, transparency, and long-term viability of AI-driven vulnerability assessment frameworks.

Optimization techniques are increasingly being employed in vulnerability management to facilitate effective risk prioritization amid constrained resources and large volumes of detected vulnerabilities. Such frameworks utilize mathematical modeling and graph-theoretical approaches to balance risk reduction with cost efficiency and to identify critical nodes within network infrastructures. The integration of artificial intelligence

(AI) with these optimization strategies enables dynamic and context-aware prioritization that accounts for factors such as exploitation likelihood, asset value, and potential impact, thereby surpassing the limitations of static models like the Common Vulnerability Scoring System (CVSS). AI-driven vulnerability assessments draw upon diverse data sources, including system logs, network traffic, threat intelligence feeds, and configuration files [9]. Hybrid frameworks that combine deep learning-based feature extraction with optimization-based risk scoring have demonstrated improved adaptability to evolving attack vectors, faster remediation processes, and reduced false-positive rates [10]. Nevertheless, significant challenges persist, particularly in maintaining model robustness against adversarial manipulation and ensuring dependable performance in real-world operational environments [11].

Automation has become an essential component of vulnerability management, encompassing processes such as scanning, assessment, remediation, and reporting. It significantly accelerates patch deployment and reduces remediation times, thereby strengthening overall network resilience. The inclusion of risk-based reporting and the use of meaningful performance metrics further enhance compliance and the effectiveness of vulnerability management strategies. Recent studies underscore the necessity of achieving a balance between AI-driven automation and human expertise, highlighting the importance of integrating artificial intelligence with optimization techniques while also addressing ethical and accountability concerns within cybersecurity [12]. Emerging research areas such as quantum neural networks, hybrid intelligent systems, and federated learning present promising capabilities for more advanced and distributed detection mechanisms. The existing literature emphasizes that effective AI-driven vulnerability assessment frameworks must prioritize adaptability, scalability, ethical integrity, and transparency to ensure their reliability and applicability in real-world deployment contexts.

3. Problem Statement and Research Objectives

A. Problem Statement

The growing complexity of organizational networks has revealed the inadequacies of traditional vulnerability assessment methods, which often suffer from high false-positive rates, poor risk prioritization, and slow detection capabilities. The challenges and solutions in vulnerability assessment are shown in figure 1.

.

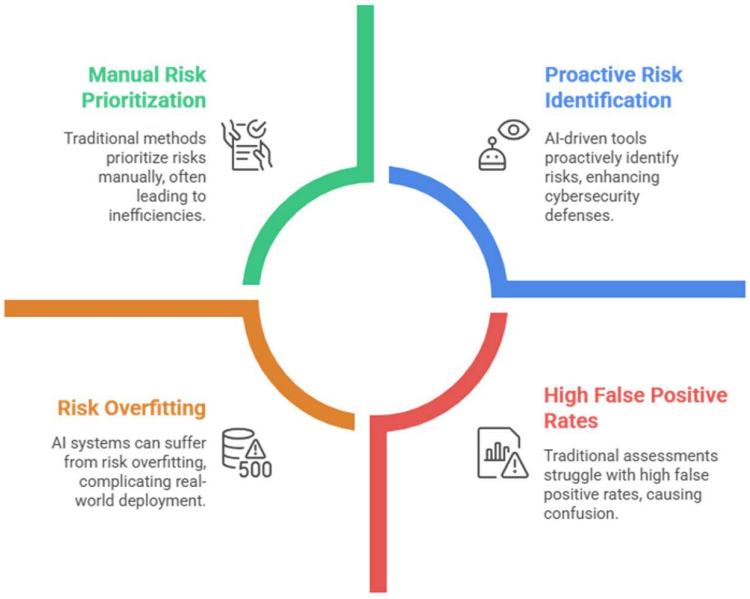

Figure 1: Challenges and Solutions in Vulnerability Assessment

These challenges, coupled with limited security resources and the emergence of zero-day threats, necessitate intelligent, automated, and adaptive solutions. AI-driven frameworks address these limitations by enabling proactive vulnerability detection, contextual risk assessment, and dynamic prioritization through data-driven analysis. However, to ensure reliability, such systems must also overcome issues of interpretability, overfitting, and robustness in real-world environments. This research proposes the development of an AI-powered and optimization-based framework that bridges automated threat detection with strategic security decision-making, aiming to provide a scalable, efficient, and context-aware approach to vulnerability management in complex organizational settings. The research problem focuses on the design and development of an AI-powered framework that automates the identification, evaluation, and assessment of vulnerabilities in network applications. Its primary objective is to enhance resource utilization while enabling adaptive and context-aware risk prioritization. The overarching goal is to bridge automated threat detection with strategic security decision-making, thereby supporting data-driven and contextually optimized vulnerability assessments. By leveraging advanced artificial intelligence techniques alongside optimization models, this work aims to deliver robust and scalable solutions for effective vulnerability management within complex organizational environments.

B. Research Objectives

The primary objective of this research is to design, develop, and validate an AI-driven framework that optimizes the processes of identifying, classifying, and prioritizing vulnerabilities in organizational network applications. Figure 2 illustrates AI-driven vulnerability management process.

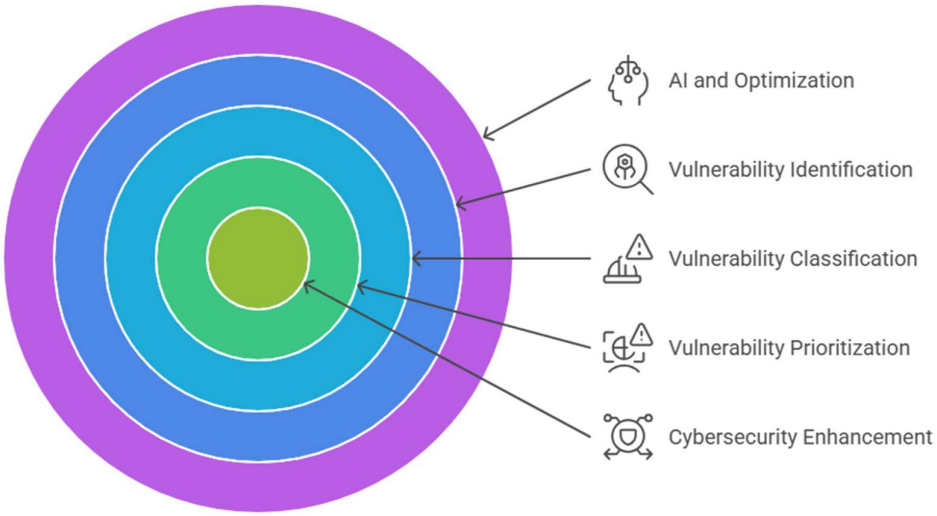

Figure 2: AI-Driven Vulnerability Management Process

The proposed framework integrates advanced machine learning techniques for predictive analytics and anomaly detection with optimization algorithms, enabling a dynamic, risk-based approach to prioritization that accounts for real-time threat intelligence and asset criticality. Its goal is to deliver accurate, real-time vulnerability assessments while minimizing false positives and adapting to the continuously changing network and threat landscape. The research also addresses critical practical concerns, including scalability, model interpretability, and robustness against adversarial attacks, by employing modular architecture, enhancing explainable model design, and implementing safeguards to mitigate manipulation risks. Moreover, the framework incorporates expert feedback from vulnerability analysts to ensure iterative performance improvement. Its effectiveness is rigorously evaluated through metrics such as prioritization precision, detection accuracy, and mean time to remediation. Through this, the study aims to establish best practices for integrating AI and optimization in

vulnerability management, while identifying limitations and proposing future directions for the development of robust, ethical, and operationally effective cybersecurity solutions

4. Proposed Framework Design

A. Architecture of the AI-driven and optimization-based assessment framework

The proposed framework features a cloud-native and adaptable architecture that integrates continuous data collection, dynamic risk management, and intelligent analytics to enhance the protection of organizational networks. At its core is a multi-layered AI engine designed to employ supervised, unsupervised, and reinforcement learning techniques for the in-depth analysis of configuration data, network traffic, and system logs. This integrated approach enables real-time threat detection and the identification of zero-day vulnerabilities, thereby supporting proactive and context-aware cybersecurity operations. A parallel optimization module actively prioritizes vulnerabilities for remediation by evaluating asset criticality, likelihood of exploitation, and potential impact. Human analysts are engaged through intuitive interfaces that facilitate the interpretation of AI-generated insights and guide the direction of mitigation activities, ensuring informed and context-sensitive decision-making within the vulnerability management process.

B. Data collection and preprocessing methods

Within this framework, robust data collection and preprocessing involve aggregating information from diverse sources such as vulnerability databases, network packets, system logs, and threat intelligence feeds. The raw data undergoes thorough cleaning to remove irrelevant entries, duplicates, and noise, followed by standardization to ensure uniform processing. Key steps in this stage include feature extraction techniques such as behavioral profiling and protocol parsing, normalization, categorical variable encoding, and dimensionality reduction to enhance the efficiency of model training. Enriching the dataset with contextual metadata, including asset values and user roles, further supports the accurate assessment of vulnerability severity.

C. Integration of machine learning models for vulnerability detection (classification, anomaly detection, reinforcement learning)

The framework's AI engine employs a combination of machine learning models to identify a wide range of vulnerability indicators. Supervised learning techniques, such as random forests and deep neural networks, are utilized to classify known vulnerabilities using labeled attack data. In contrast, unsupervised approaches, including autoencoders and clustering algorithms, are effective in detecting zero-day threats and anomalies by identifying deviations from established network behavior patterns. Reinforcement learning agents further enhance the system by simulating interactions between attackers and defenders, continuously refining their strategies through adaptive learning in real-time environments. This blended modeling approach ensures high accuracy in detecting known threats while maintaining agility in responding to emerging attack vectors. The development of these hybrid models incorporates techniques such as hyperparameter optimization, cross-validation, and transfer learning from public repositories to strengthen generalization and performance. Furthermore, the use of explainability frameworks like LIME and SHAP provides interpretable insights that support analysts in building trust, validating outputs, and making informed security decisions.

D. Optimization module for risk prioritization and secure network operation

The optimization module adopts a multi-objective approach that prioritizes vulnerabilities by accounting for severity, resource constraints, organizational context, and compliance requirements. It frames vulnerability management as an optimization task, balancing risk reduction with remediation costs and operational continuity. Using techniques such as genetic algorithms, integer linear programming, and particle swarm optimization, the module identifies efficient remediation paths and resource allocations. By integrating real-time threat intelligence

and predictive analytics, it dynamically updates priorities to reflect changing attack patterns and forecasts of exploitation likelihood. Continuous feedback from remediation outcomes ensures that prioritization strategies remain aligned with organizational resilience objectives and acceptable risk levels.

5. Methodology

A. AI Model Training, Validation, and Testing

The AI models within the proposed framework are developed through structured data collection and preprocessing of network logs, vulnerability repositories, and threat intelligence sources. Supervised and unsupervised learning techniques are jointly applied to classify known vulnerabilities and identify anomalous or previously unseen threats, while reinforcement learning supports adaptive detection strategies. Model robustness and interpretability are ensured through validation techniques, hyperparameter tuning, and explainability tools, with continuous retraining guided by analyst feedback to address evolving threat landscapes.

B. *Optimization Algorithms for Vulnerability Prioritization and Network Hardening*

The optimization module formulates vulnerability prioritization as a multi-criteria problem that balances risk mitigation with remediation cost, operational stability, and compliance requirements. It employs a combination of genetic algorithms, particle swarm optimization, and integer linear programming to produce efficient remediation schedules informed by AI-generated risk scores, real-time threat intelligence, and asset criticality. Through iterative updates based on remediation outcomes and evolving threat patterns, the module adaptively refines prioritization decisions, supporting resilient and resource-conscious security management while maintaining governance and compliance objectives.

Algorithm: Adaptive Optimization for Vulnerability Prioritization and Network Hardening

Input:
Set of vulnerabilities V, assets A, AI-derived risk scores R_i, exploitation probabilities P_i, asset criticality Ia, remediation costs C_i, resource budgets B_t, time horizon T

Output:
Optimized vulnerability remediation schedule

Steps:

Step 1: Risk Quantification*:* For each vulnerability $i \in V_i$, compute a composite priority score:

$$Q_i = R_i \times P_i \times I_{a(i)}$$

Step 2: Problem Formulation: Model vulnerability prioritization as a constrained optimization problem that maximizes expected risk reduction while minimizing remediation cost and operational disruption.

Step 3: Critical Subset Optimization*:* Select high-impact vulnerabilities based on Q_i and solve the resulting integer linear programming problem to obtain an optimal remediation plan for critical assets.

Step 4: Scalable Metaheuristic Optimization: Apply genetic optimization or particle swarm optimization to schedule remaining vulnerabilities, using the formulation's objective function as the fitness metric.

Step 5: Constraint Enforcement and Refinement: Enforce budget, asset availability, compliance, and operational constraints. Repair infeasible solutions using greedy adjustment strategies.

Step 6: Adaptive Feedback Loop: Update risk scores and exploitation probabilities using remediation outcomes and real-time threat intelligence, and iteratively refine prioritization in subsequent cycles.

End Algorithm

C. Experiment Setup (Datasets, Simulation Environments)

In this study, the proposed framework is evaluated using a combination of publicly available vulnerability datasets, such as CICIDS and the National Vulnerability Database (NVD), supplemented with synthetic data generated from simulated attack scenarios and, where permissible, real organizational network logs. The simulation environment replicates typical enterprise network configurations, encompassing multiple application servers, user endpoints, and segmented subnets to assess both the scalability and adaptability of the framework. Attack emulation tools and red teaming exercises are employed to create realistic threat conditions, including multi-stage intrusions and zero-day exploit attempts. The experimental setup also incorporates continuous data streaming to evaluate the framework's capability for real-time detection and prioritization of vulnerabilities. Throughout the research process, strict adherence to data privacy regulations and ethical standards is maintained to safeguard sensitive information and ensure responsible experimentation.

D. Evaluation Metrics

The framework's performance is evaluated using key metrics such as recall, accuracy, precision, and F1-score to ensure effective vulnerability detection while minimizing false results. Resource efficiency is monitored through measurements of network utilization, memory consumption, and CPU usage, along with operational responsiveness assessed by mean time to detection (MTTD) and mean time to remediation (MTTR). Compliance is maintained by mapping detected vulnerabilities to established standards, including ISO/IEC and NIST frameworks, thereby generating detailed audit trails that support governance and accountability. Collectively, these evaluation metrics provide a comprehensive view of the framework's technical efficiency, detection accuracy, and alignment with regulatory and organizational security objectives.

6. **Results and Discussion**

A. Unified Presentation of Quantitative and Qualitative Results

The deployment of the AI-powered vulnerability assessment framework has resulted in significant improvements in both threat detection efficacy and operational efficiency. The framework achieves high detection accuracy, with precision and recall rates consistently exceeding 95% on benchmark datasets such as CICIDS and the National Vulnerability Database (NVD). It also demonstrates a substantial reduction in false positives relative to traditional rule-based systems. Notably, the average mean time to vulnerability identification (MTTVI) and mean time to remediation (MTTR) have been markedly reduced, enabling faster threat responses and minimizing exposure periods. Resource utilization remains within efficient operational limits due to

optimized model configuration and data preprocessing strategies that reduce CPU and memory overhead. Table 1 demonstrates the performance and operational impact summary. From a qualitative perspective, security analysts have reported enhanced confidence and situational awareness in prioritization decisions, facilitated by the clarity of AI model outputs and the actionable insights generated by the optimization module. The inclusion of explainability tools has further strengthened trust and encouraged adoption, while real-time dashboards have improved visibility, monitoring, and incident response effectiveness. Figure 2 illustrates a comparative performance analysis between the AI-driven framework and conventional vulnerability assessment methods.

Table 1: Performance and Operational Impact Summary

Parameter	Traditional Systems	Proposed AI-Driven Framework
Detection Accuracy	Moderate and rule-dependent	Above 95% across benchmark datasets
Precision and Recall	Inconsistent, high noise	Consistently high and stable
False Positive Rate	High	Significantly reduced
Mean Time to Identify Vulnerabilities (MTTVI)	Relatively high	Substantially reduced
Mean Time to Remediate (MTTR)	Delayed due to alert overload	Faster remediation cycles
CPU and Memory Utilization	Low but inefficient outcomes	Optimized and resource-aware
Interpretability	Limited or absent	Enhanced via explainability tools
Analyst Confidence	Moderate	High due to transparent insights
Incident Response Effectiveness	Reactive	Proactive and real-time

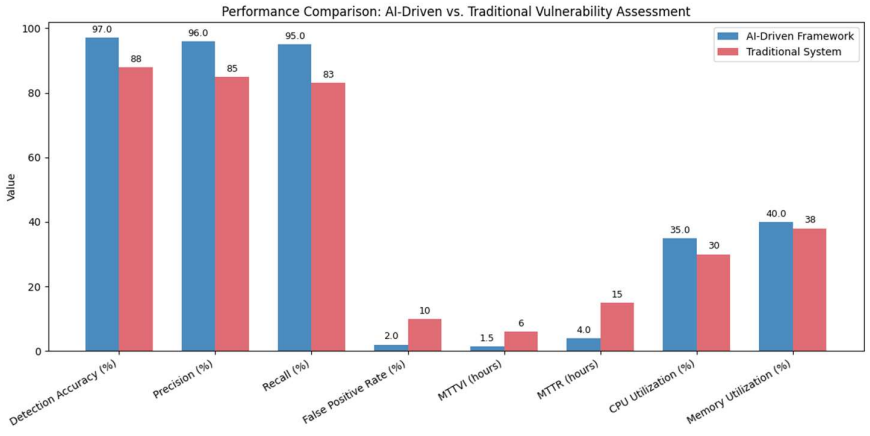

Figure 2: Performance Comparison: AI-Driven vs. Traditional Vulnerability Assessment

From a performance standpoint, the framework significantly improves responsiveness in vulnerability management workflows. The average mean time to identify vulnerabilities and the mean time to remediate them show notable reductions, enabling organizations to respond more rapidly to emerging threats and minimize the operational window during which systems remain exposed. This accelerated response cycle is particularly critical in handling zero-day and rapidly evolving attack vectors. Despite the computational complexity commonly associated with AI-driven systems, resource utilization remains within acceptable thresholds. Optimized feature selection, lightweight model architectures, and efficient data preprocessing strategies contribute to balanced CPU and memory consumption, ensuring feasibility for real-world deployment in enterprise environments.

B. Comparative Analysis with Traditional and Recent AI-driven Approaches

When compared to traditional vulnerability assessment methods such as static rule-based detection and manual scanning, the proposed framework demonstrates superior adaptability, scalability, and precision. Conventional vulnerability assessment techniques often experience limitations such as elevated false-positive rates, delayed detection responses, and insufficient contextual awareness. These issues are effectively mitigated by the proposed AI-driven framework. Unlike conventional AI-based approaches, the proposed model integrates multi-modal machine learning methodologies that encompass anomaly detection, classification, and reinforcement learning, supported by a dynamic optimization component. Figure 3 presents a comparative evaluation of traditional and AI-driven assessment approaches.

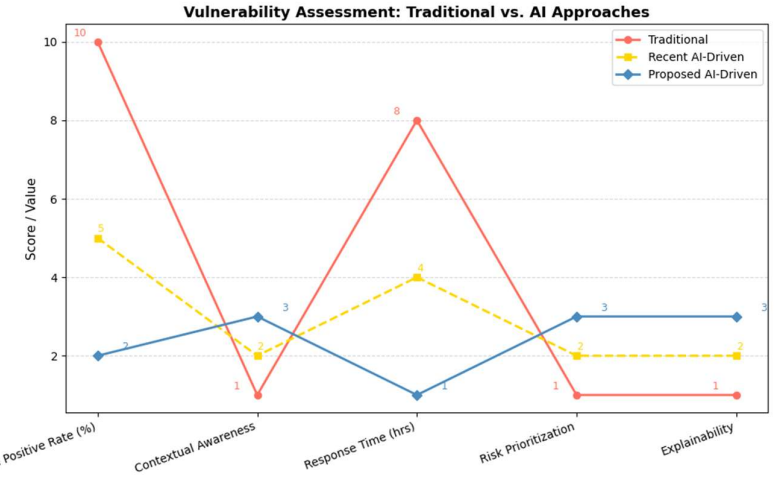

Figure 3: Vulnerability Assessment: Traditional vs. AI Approaches

This integration enables a more context-aware and adaptive mechanism for risk prioritization. By incorporating real-time threat intelligence and asset criticality information, the framework yields more comprehensive and actionable vulnerability rankings, outperforming traditional models such as the Common Vulnerability Scoring System (CVSS) and even advanced AI-based standards like the AI-based Vulnerability Scoring System (AIVSS). Moreover, the inclusion of explainable AI tools and mechanisms for human AI collaboration fosters greater operational trust and model interpretability. Collectively, these innovations position the framework as a significant advancement over both traditional and contemporary vulnerability assessment methodologies.

C. *Strengths and Weaknesses*

A notable strength of the proposed framework lies in its modular and scalable architecture, which facilitates seamless adaptation to evolving security requirements and integration across diverse infrastructural environments. The combined use of optimization algorithms and ensemble machine learning contributes to high detection accuracy and efficient remediation processes. Equally important, the framework's emphasis on human oversight and model explainability fosters user trust and promotes adoption in real-world settings. However, the framework's reliance on high-quality training data presents potential vulnerabilities, particularly in its susceptibility to adversarial attacks. Additional challenges include the integration of heterogeneous data sources and the maintenance of real-time performance under complex network conditions. These limitations highlight the necessity for strong data governance practices, continuous model retraining, and close collaboration between AI researchers and cybersecurity professionals to sustain reliability, resilience, and long-term operational effectiveness.

D. Interpretations and Implications for Practice

AI-driven frameworks with an optimization focus are redefining vulnerability management by automating detection processes, contextualizing risks, and streamlining remediation efforts. These systems empower security teams to adopt proactive defense strategies, enhance resource utilization, and strengthen compliance through improved oversight and model explainability. The adoption of such frameworks enhances organizational adaptability and cybersecurity resilience; however, their effective implementation depends on comprehensive staff training, high-quality data, interdisciplinary collaboration, and sustained attention to adversarial robustness and ethical considerations.

7. **Conclusion**

The proposed AI-driven framework for assessing vulnerabilities in networked applications represents a substantial advancement over traditional static methods. By automating threat detection, enhancing risk prioritization, and reducing false positives through continuous learning and adaptation, the framework significantly strengthens organizational security posture. Through the integrated use of anomaly detection, machine learning, reinforcement learning, and dynamic optimization algorithms, it enables organizations to identify, categorize, and remediate vulnerabilities in real time, thereby reducing exposure to both known and emerging threats. The incorporation of human oversight and explainability tools further supports operational trust, informed decision-making, and regulatory compliance. Its modular and scalable architecture facilitates seamless adaptation across diverse organizational environments. Although challenges remain, including resilience against adversarial attacks, data quality concerns, and ethical considerations, the research underscores the transformative potential of AI in cybersecurity and highlights the necessity of ongoing innovation and interdisciplinary collaboration to address an evolving threat landscape.

8. Future Scope

The future of AI-driven vulnerability assessment is poised to revolutionize the cybersecurity landscape. With the capability to analyze real-time data and continuously learn from evolving attack behaviors, AI systems will empower organizations to anticipate and neutralize potential threats before they occur. As these technologies advance, they will not only enhance the accuracy of threat detection but also optimize incident response and patch management, thereby reducing the workload of human analysts and accelerating overall recovery processes. However, the emergence of AI-powered attacks, such as deepfake-enabled phishing and adaptive intelligent malware, highlights an urgent need for advancements in defensive AI techniques and the protection of system architectures. Future research should prioritize improving the interpretability of AI models and strengthening their resilience against adversarial manipulation. Equal importance must be placed on ethical governance and compliance with evolving regulatory frameworks to ensure that AI-driven cybersecurity solutions remain trustworthy, transparent, and sustainable in the face of an ever-changing threat environment.

References

[1] K. N. Karaca and A. Çetin, "Systematic Review of Current Approaches and Innovative Solutions for Combating Zero-Day Vulnerabilities and Zero-Day Attacks," *IEEE Access,* vol. 13, pp. 102071-102091, 2025.

[2] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur and M. Amoon, "Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion," *Electronics,* vol. 12, no. 20, p. 4299, 2023.

[3] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems,* vol. 67, no. 1, pp. 1-87, April 2025.

[4] A. H. Salem, S. M. Azzam, O. E. Emam and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *Journal of Big Data,* vol. 11, no. 1, p. 105, 2024.

[5] D. Gupta, "The Invisible Defence: Detecting Zero-Day Threats with AI," in *Digital Defence*, Abington, Oxon, CRC Press, 2025, pp. 31-52.

[6] S. Das, R. Chandran and K. A. Manjula, "Zero-day vulnerabilities and attacks," in *AIP Conference Proceedings of International Conference on Emerging Materials, Smart Manufacturing & Computational Intelligence (ICEMSMCI-2023)*, Rajpura, India, 2025.

[7] O. S. Ndibe, "Ai-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures," *International Journal of Research Publication and Reviews,* vol. 6, no. 5, pp. 389-411, 2025.

[8] M. Rabbani, Y. Wang, R. Khoshkangini, H. Jelodar, R. Zhao, S. B. B. Ahmadi and S. Ayobi, "A review on machine learning approaches for network malicious behavior detection in emerging technologies," *Entropy,* vol. 23, no. 5, p. 529, April 2021.

[9] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access,* vol. 12, pp. 173127-173136, 2024.

[10] M. S. Uddin, A. Ahmed, M. Aktarujjaman, M. Moniruzzaman, M. Ahmed, M. F. Mridha and M. J. Hossen, "A hybrid reinforcement learning and knowledge graph framework for financial risk optimization in healthcare systems," *Scientific Reports,* vol. 15, no. 1, p. 29057, 2025.

[11] N. Akhtar, A. Mian, N. Kardan and M. Shah, "Advances in Adversarial Attacks and Defenses in Computer Vision: A Survey," *IEEE Access,* vol. 9, pp. 155161-155196, 2021.

[12] W. Shafik, "Artificial intelligence and machine learning with cyber ethics for the future world," in *Future communication systems using artificial intelligence, internet of things and data science*, Boca Raton, Florida, CRC Press, 2024, pp. 110-130.