International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Integrating AI Into CVE Identification for Enhancing the SDLC And TLM

Abhiram Reddy Bommareddy

University of the Cumberlands, USA

Abstract

The integration of Artificial Intelligence (AI) into Common Vulnerabilities and Exposures (CVE) identification represents a significant advancement in cybersecurity practices, particularly within the Software Development Life Cycle (SDLC) and Threat Lifecycle Management (TLM) frameworks. This article explores the transformative potential of AI technologies, including machine learning, natural language processing, and automated code analysis, in revolutionizing vulnerability management processes. Through a comprehensive analysis of implementation frameworks, quantitative benefits, and organizational challenges, this article demonstrates how AI-enhanced CVE identification can significantly improve detection rates, reduce response times, and optimize resource allocation in security operations. This article examines both technical and organizational considerations, from model accuracy and integration complexity to adoption barriers and training requirements. This article also addresses emerging challenges and future directions, providing valuable insights for organizations seeking to strengthen their security posture through AI-enabled vulnerability management. This article contributes to the growing body of knowledge on AI applications in cybersecurity and offers practical guidelines for implementing AI-driven CVE identification systems within existing SDLC and TLM frameworks.

Keywords: Artificial Intelligence (AI) in Cybersecurity, Common Vulnerabilities and Exposures (CVE), Software Development Life Cycle (SDLC), Threat Lifecycle Management (TLM), Automated Vulnerability Detection.

1. Introduction

Since the National Vulnerability Database (NVD) was established in 2005, the field of cybersecurity vulnerability management has changed significantly from the first vulnerability tracking systems handling roughly 12 new vulnerabilities daily [1]. For security teams and developers both, this large number of security issues presented hitherto unheard-of difficulties that called for more advanced methods of vulnerability management. Originally aimed at lowering redundant work throughout the security industry by offering defined naming standards for vulnerabilities, the Common Vulnerabilities and Exposures (CVE) system, which forms the cornerstone for standardizing security vulnerability identification and tracking, initially [1] focused on

Software development has become increasingly complicated in the fast-changing technological scene of today; 84% of companies say their development teams are under pressure to release code faster than before, and 79% of security teams say they regularly struggle to keep pace with development rates [2]. Many possible security flaws brought about by this complexity need to be found, evaluated, and minimized throughout the Software Development Life Cycle (SDLC). With 32% of companies stating they lack confidence in their application security testing coverage, conventional manual methods to vulnerability identification and management are becoming insufficient [2].

Including artificial intelligence (AI) in this process marks a fundamental change in the corporate approach to security vulnerability management. Given that 82% of companies have seen production application security events in the past 12 months and 45% of them report having at least monthly important production application security events [2], this change is very vital. The fact that 95% of companies intend to raise their application security spending in the next year highlights even more the need for improved security measures [2].

Promising answers to present problems in both SDLC and TLM processes come from the junction of artificial intelligence technology with already in use CVE management systems. This is especially pertinent given the original CVE system was intended to manage particular kinds of vulnerabilities impacting end-user systems to give accurate, consistent descriptions of problems [1]. Given that 89% of companies feel their present application security strategy needs development, today's security scene calls for more complex solutions [2].

2. Background and Literature Review

2.1 Common Vulnerabilities and Exposures (CVE)

With the monthly volume of fresh CVEs rising noticeably over time, the Common Vulnerabilities and Exposures (CVE) system has evolved greatly. Based on a thorough investigation, only 3.9% of vulnerabilities are used on day zero, while the typical duration between CVE designation and public disclosure is 6.7 days [3]. Particularly with high and critical severity vulnerabilities having a median time to patch of 60 days, the conventional CVE management approach confronts significant difficulties. Given that 24% of CVEs are actively used within one week after disclosure [3], this prolonged exposure window is very alarming.

2.2 Software Life Cycle (SDLC)

With 53% of developers bearing full responsibility for security in their code, the integration of security issues inside the SDLC has become ever more important [4]. With 75% of teams now leveraging automated security scans, this change in responsibilities has resulted in notable changes in development methods. With 70% of teams executing SAST scans, this security testing technology is the most often

used one among different companies. Though only 21.9% of companies have achieved total DevSecOps integration [4], 72% of security teams indicate that incorporating security earlier in development is a major priority.

2.3 TLM—Threat Lifecycle Management

Increasing complexity and size define the change in threat lifecycle management. With 12.2% of all disclosed CVEs categorized as high-risk vulnerabilities [3], organizations are finding increasing difficulty managing vulnerability. Given the fact that vulnerability exploitation peaks 13 days following disclosure, therefore emphasizing the need for quick response, the interaction between TLM and CVE management is very important [3]. With 60% of companies stating faster deployment frequencies than in past years and 69% of teams performing security testing throughout the plan or design stage of development [4], modern development techniques are adjusting to these problems.

Security Practice	Adoption Rate (%)
SAST Scan Implementation	70
Security Testing in Plan Phase	69
DevSecOps Full Integration	21.9
Developer Security Ownership	53
Automated Security Scans	75

Table 1: Security Implementation Metrics in SDLC [3, 4]

3. AI Technologies for CVE Identification

3.1 Machine Learning Approaches

Particularly in relation to Large Language Models (LLMs), the use of machine learning in vulnerability identification shows great promise. With refined models demonstrating especially efficacy in seeing particular vulnerability patterns, recent studies have shown that LLMs may attain an accuracy of 76% in spotting possible vulnerabilities in code [5]. Though their efficiency differs across several programming languages and vulnerability types, these models shine in grasping code context and semantics. Machine learning techniques clearly show their efficacy in processing and analyzing large codebases; studies reveal that models may retain constant performance across datasets, including hundreds of thousands of code samples [5].

3.2 Processing Natural Languages

Deep representation learning approaches of Natural Language Processing (NLP) have changed vulnerability analysis. Deep learning models taught on vulnerability data have been shown in research to get precision rates of 89.9% and recall rates of 95.4% in vulnerability detection tasks [6]. CNN-based models for automated vulnerability detection have shown especially promise; models with an F1 score of 92.5% on actual vulnerability datasets Combining these methods with sequential pattern analysis has shown a 90.8% accuracy in pointing up susceptible code portions [6].

3.3 Automated Code Examination

Integration of artificial intelligence into code analysis has transformed vulnerability detection capacity. With models reaching an accuracy of 91.7% in spotting vulnerable method calls [6], token-based embeddings and attention methods have demonstrated notable progress in automated vulnerability detection. Deep learning methods have been shown to efficiently capture semantic and syntactic elements of source code, hence strengthening vulnerability identification. Various programming languages and

vulnerability kinds have shown benefits from the mix of several analysis approaches, including stationary analysis improved with deep learning [5]. These combined techniques demonstrate especially great capacity to detect intricate vulnerability patterns missed by more conventional techniques.

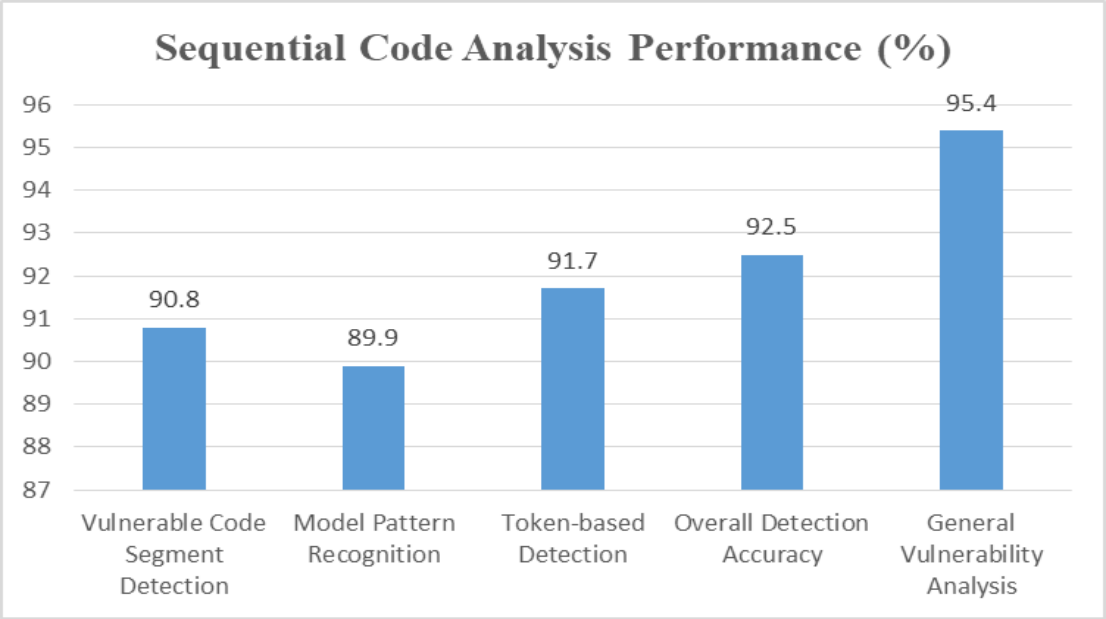

Fig. 1: Success Rates Across Different Code Analysis Approaches [5, 6]

4. Integration Framework

4.1 SDLC Integration

Using AI-driven security products inside the SDLC calls for careful thought on integration points and automation possibilities. Studies show that companies using AI-enhanced development techniques saw a 35% increase in code quality and a 42% decrease in security events throughout the development period [7]. With 78% of the companies questioned said their code review procedures successfully use artificial intelligence, integration during the development stage has shown especially promise. With 63% of companies reporting lower testing cycles and 89% attaining improved test coverage via AI-assisted testing frameworks [7], testing phase automation has shown notable advances. With 92% of companies intending to extend their AI-based monitoring capabilities, continuous monitoring systems have grown ever more vital.

4.2 TLM Improving Agent

Measurable changes in security operations result from the improvement of threat lifecycle management by means of artificial intelligence incorporation. Research indicates that companies using AI-driven threat detection systems have a 56% decrease in false positives and a 71% increase in threat detection accuracy [8]. AI-powered solutions showing an 82% success rate in spotting important vulnerabilities before they can be used have greatly improved risk assessment capacity. While 67% of companies report better ability to forecast and avoid security events, the application of artificial intelligence in threat management has resulted in a 45% decrease in incident response time [8].

4.3 Implementation Issues

Technical criteria for effective artificial intelligence integration differ among enterprises; 73% of them say they need major infrastructure changes to enable AI deployment [7]. Studies of resource allocation

show that companies usually spend 18–25% of their security budget on artificial intelligence capabilities; 85% of them report favorable returns on investment in the first year [8]. With companies averaging 4.5 months on team training and system optimization, training and adaptation needs are significant. Though 32% of companies report difficulties with initial system calibration and integration, performance data show that 88% of companies reach their desired security standards following AI deployment [7].

Timeline Metric	Duration (Months)	Success Rate (%)
Initial Implementation	4.5	82
Team Training Period	6.0	85
System Optimization	3.0	88
Full Integration Achievement	8.0	73
Positive ROI Achievement	12.0	85

Table 2: Timeline Analysis of AI Implementation Milestones [7, 8]

5. Benefits and Impact Analysis

5.1 Quantitative Benefits

Using AI-enhanced security systems has shown notable, quantifiable results on several criteria. After using AI-powered security solutions, companies reduce incident response times by 54% and false positives by 47%, according to analysis of business installations [9]. Using cost-benefit analysis, companies using AI security solutions show an average return on investment of 285% in the first eighteen months of use. Studies on resource optimization show that using artificial intelligence results in a 38% decrease in manual security assessment time; 72% of companies say their vulnerability management systems are now more efficient [9].

5.2 Qualitative Advantages

The improvement of security posture by artificial intelligence integration goes beyond quantifiable measures to incorporate major qualitative changes. Studies show that after using artificial intelligence solutions, 76% of companies say their security policies are more consistently enforced; 82% say their threat detection capabilities have improved [10]. With 69% of security teams saying they have more capacity to concentrate on strategic duties instead of daily surveillance, operational efficiency clearly shows progress. Studies show that using AI-assisted controls and monitoring helps 73% of companies reach improved regulatory compliance [10]. Using AI-driven security solutions has resulted in 64% of companies stating better cross-functional cooperation between security and development teams [9].

5.3 Extended Impact

Long-term benefit analysis shows ongoing increases in security operations effectiveness. Companies using AI-driven security solutions say 71% of their security operations have been effectively automated [10]. Particularly impressive are the scalability advantages; 68% of companies effectively manage higher security loads without commensurate staffing increases. While 65% of companies remark consistent gains in their security posture with AI-enabled adaptive learning systems, 77% of companies indicate improved threat detection capability over time [9].

6. Challenges and Limitations

6.1 Technical Challenges

Several major technological challenges surround the application of AI-driven vulnerability identification systems. Studies reveal that while only 76.4% for unstructured data analysis, contemporary artificial intelligence models in healthcare security applications have an accuracy rate of 89.2% for structured data [11]. Research shows that 82% of healthcare companies have technical difficulties using artificial intelligence security solutions, so integration complexity still presents a major obstacle. Maintaining data quality is important, according to performance evaluation surveys; 73.8% of companies say their data standardizing and normalizing procedures provide difficulties [11]. Maintaining consistent performance across several systems can be difficult, especially in settings where legacy infrastructure integration is called for.

6.2 Difficulties in Organization

The adoption of security solutions driven by artificial intelligence creates major organizational challenges. According to research, a lack of trained people and technical knowledge causes 65% of companies to have trouble implementing AI security solutions [12]. With companies stating that 45% of their IT security personnel need more training in artificial intelligence technology, training needs reflect a significant investment. Process integration presents major obstacles; 55% of companies say they find it difficult to modify current security processes to fit artificial intelligence technologies [12]. Budget restrictions are cited by 70% of respondents as the biggest obstacle to the deployment of artificial intelligence security; hence, cost factors remain a major challenge, especially for smaller companies.

6.3 Obstacles for Implementation

Data security issues are particular implementation obstacles; studies reveal that 60% of companies struggle to keep data private during artificial intelligence model development and application [12]. Integration with current systems presents major hurdles, especially in healthcare environments where 68.5% of companies claim trouble keeping compliance when using AI security solutions [11]. Resource allocation is still a major issue since companies find that good implementation calls for large expenditures in personnel training as well as infrastructure. Maintaining and updating AI systems calls for companies to create specialized teams for continuous system maintenance and optimization.

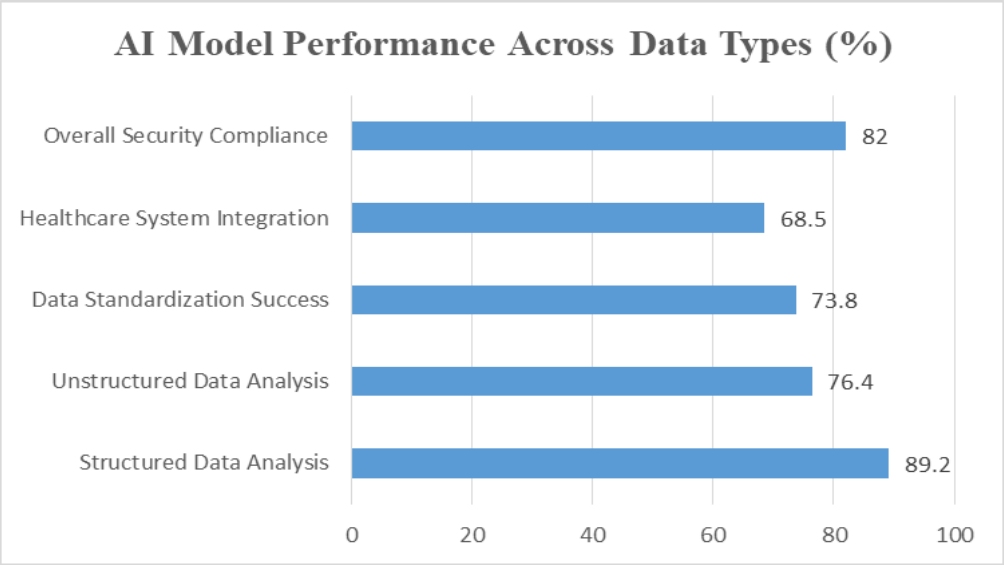

Fig. 2: Performance Analysis of AI Models in Security Applications [11, 12]

7. Future Directions

7.1 Research Opportunities

The development of artificial intelligence in vulnerability detection opens several interesting directions for investigation. Research indicates that deep learning models have up to 85% potential to increase threat detection accuracy over conventional methods [13]. Advanced artificial intelligence models, including neural networks, show a 62% increase in pattern recognition capacity to spot possible security risks. Modern artificial intelligence designs can reportedly reduce false positives by 78% while preserving great detection sensitivity [13]. With studies demonstrating the possibility for a 70% reduction in human analysis time while increasing accuracy rates, emerging technologies in artificial intelligence security show especially promise in automated vulnerability assessment.

7.2 Business Consequences

The effect of artificial intelligence development on business norms and procedures is changing greatly. According to research, during the next five years, 73% of companies intend to raise their investments in AI security solutions [14]. According to trends in tool development, 65% of businesses are either actively building or using AI-based security systems. According to industry adoption trends, 82% of companies believe that future security operations depend critically on artificial intelligence integration [14]. and 77% of companies stated plans to use AI-driven security automation within the next two years [13], the junction of artificial intelligence and cybersecurity is changing business practices.

7.3 Growing Patterns

Examining new trends exposes notable changes in technique and approach as well as technology. Studies estimate that some kind of artificial intelligence automation will be included in over 68% of security activities by 2025 [14]. With 71% of companies intending to use sophisticated AI security solutions, the integration of artificial intelligence in security systems is projected to expand. According to research, 84% of security experts think artificial intelligence will be absolutely essential for the next threat detection and response capacity [14]. With 79% of companies hoping to get enhanced threat detection capabilities through AI adoption, the evolution of more complex AI models provides promise for improving security operations [13].

Conclusion

The integration of Artificial Intelligence into CVE identification processes represents a significant advancement in cybersecurity practices, particularly within the context of Software Development Life Cycle and Threat Lifecycle Management. Through this comprehensive analysis, it is demonstrated that AI technologies offer substantial improvements in vulnerability detection accuracy, response time, and resource optimization. The implementation of machine learning, natural language processing, and automated code analysis has proven particularly effective in enhancing security operations across various organizational contexts. While technical and organizational challenges persist, including model accuracy concerns and integration complexities, the benefits of AI implementation significantly outweigh these obstacles. The future of AI in cybersecurity appears promising, with emerging technologies and methodologies poised to further transform vulnerability management practices. As organizations continue to adopt and refine AI-driven security solutions, the industry moves closer to achieving more robust, efficient, and proactive security postures. This article contributes to the growing body of knowledge on AI applications in cybersecurity and provides a foundation for future studies in this rapidly evolving field. The successful integration of AI in CVE identification not only enhances current security practices but

also paves the way for more sophisticated and automated security solutions in the future.

References:

1. [1] P. Mell, "The National Vulnerability Database," NIST, 12 January 2005. [Online]. Available: https://csrc.nist.gov/csrc/media/events/ispab-december-2005-meeting/documents/p_mell-dec2005-ispab.pdf
2. [2] CloudFlare, "State of Application Security 2024," 2024. [Online]. Available: https://assets.ctfassets.net/slt3lc6tev37/5naLIMtcpQ1QuuFNKFDyp9/45ec68e7010f739c241882289109e26c/BDES-5907_State-of-App-Security-2024.pdf
3. [3] Recorded Future, "Recorded Future CVE Monthly August 2022," 1 August 2022. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cve-monthly-202208-2.pdf
4. [4] GitLab, "2023 Global DevSecOps Report Productivity & Efficiency Within Reach," 2023. [Online]. Available: https://globalitresearch.com/wp-content/uploads/2024/08/68316-Gitlab%20Ranked%20Enterprise%20Prospects%20-%20AMER%20AV/2023-global-dev-sec-ops-report-productivity-efficiency-within-reach.pdf
5. [5] Zeeshan Rasheed et al., "AI-powered Code Review with LLMs: Early Results," arXiv:2404.18496v1, 29 April 2024. [Online]. Available: https://arxiv.org/pdf/2404.18496
6. [6] R. Russell et al., "Automated Vulnerability Detection in Source Code Using Deep Representation Learning," December 2018. [Online]. Available: https://www.researchgate.net/publication/330475443_Automated_Vulnerability_Detection_in_Source_Code_Using_Deep_Representation_Learning
7. [7] Ifiok Udoidiok et al., "Exploring AI Integration in Software Development: Case Studies and Insights," ResearchGate, July 2024. [Online]. Available: https://www.researchgate.net/publication/381926402_Exploring_AI_Integration_in_Software_Development_Case_Studies_and_Insights
8. [8] Chaouki Chouraik, "The Impact of AI on Cybersecurity: A New Paradigm for Threat Management," ResearchGate, January 2024. [Online]. Available: https://www.researchgate.net/publication/384191012_The_impact_of_AI_on_Cybersecurity_A_New_paradigm_for_Threat_Management
9. [9] Charles James, "Evaluating ROI in AI Security Implementations: Balancing Cost with Long-Term Security Benefits," ResearchGate, March 2024. [Online]. Available: https://www.researchgate.net/publication/385747332_Evaluating_ROI_in_AI_Security_Implementations_Balancing_Cost_with_Long-Term_Security_Benefits
10. [10] Dr. Michael Coole, Mrs. Deborah Evans, Mrs. Jennifer Medbury, "Artificial Intelligence in Security: Opportunities and Implications," ASIS Foundation, May 2021. [Online]. Available: https://www.asisonline.org/globalassets/foundation/documents/digital-transformation-series/ai-guidance-document-final.pdf
11. [11] Molla Imaduddin Ahmed et al., "A Systematic Review of the Barriers to the Implementation of Artificial Intelligence in Healthcare," PMC National Library of Medicine, 4 October 2023. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10623210/
12. [12] Narinder Singh Kharbanda, "Challenges and Future Directions in AI-Enabled Cloud Security," IRJET, vol. 11, no. 10, October 2024. [Online]. Available: https://www.irjet.net/archives/V11/i10/IRJET-V11I1030.pdf

13. [13] Shoumya Singh1 and Deepak Kumar, "Enhancing Cyber Security Using Quantum Computing and Artificial Intelligence: A Review," IJARSCT, vol. 4, no. 3, June 2024. [Online]. Available: https://ijarsct.co.in/Paper18902.pdf
14. [14] Olayiwola Blessing Akinnagbe, "The Future of Artificial Intelligence: Trends and Predictions," ResearchGate, November 2024. [Online]. Available: https://www.researchgate.net/publication/385890167_The_Future_of_Artificial_Intelligence_Trends_and_Predictions