ISSN: 2320-5407

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: **IJAR-51865** Date: 25/05/2025

Title: AI-Augmented Security Models for Software Development: Leveraging 1 Machine Learning for Threat Detection and Mitigation

Recommendation:
Accept after minor revision

Rating	Excel.	Good	Fair	Poor
Originality	✓			
Techn. Quality	✓			
Clarity			✓	
Significance	✓			

Originality: The paper presents a novel hybrid security framework that integrates rule-based systems with supervised and unsupervised machine learning algorithms for enhanced threat detection. The multi-layered approach for both known and unknown (zero-day) threat identification is a meaningful advancement over existing isolated techniques. It offers fresh insights into how AI can be embedded throughout the software development lifecycle, making it stand out among current literature.

Technical Quality: The technical depth is robust. The authors present a strong rationale and methodology, leveraging the CRISP-DM framework, appropriate supervised models (SVM, Random Forest, Decision Trees), and unsupervised models (Autoencoders, VAEs). Experimental results show practical performance improvements, and the methodological rigor (e.g., use of real-time traffic data, multiple evaluation metrics) is appropriate for publication in a high-quality journal

Clarity: While the paper is generally well-structured and covers all major components (introduction, literature review, methodology, results, etc.), the text would benefit from professional proofreading. There are minor issues related to repetition, inconsistent figure labelling (e.g., "Figure 1.2" appears without a proper caption), and overly dense blocks of text that could be made more reader-friendly. Paragraph breaks and visual segmentation of key ideas would improve readability.

Significance: The study contributes directly to critical challenges in modern software development particularly the identification of zero-day vulnerabilities and real-time threat mitigation using AI. The work is also aligned with current security demands in cloud-native, microservices, and IoT environments

Reviewer Name: Mr. Aditya Nivas Magdum **Date:** 25/05/2025

Reviewer's Comment for Publication.
(*To be published with the manuscript in the journal*)

The manuscript titled "AI-Augmented Security Models for Software Development: Leveraging Machine Learning for Threat Detection and Mitigation" presents an original and technically sound hybrid framework that integrates traditional rule-based methods with supervised and unsupervised machine learning algorithms. The proposed model effectively addresses known and zero-day threats, offering significant improvements in detection rates and incident response times. The use of the CRISP-DM methodology and real-world datasets enhances the study's rigor and practical relevance. While the paper is well-structured and comprehensive, minor revisions are needed to improve clarity, figure formatting, and language flow. Overall, this is a valuable contribution to the field of AI-driven cybersecurity and is recommended for publication with minor revisions.