ISSN: 2320-5407

ISSN NO. 2320-5407

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: **51865** Date: 26-05-2025

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

Recommendation:
Accept as it is ………… **YES** ………
Accept after minor revision……
Accept after major revision ………………
Do not accept (*Reasons below*) ………

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

Reviewer Name: Gulnawaz Gani

Reviewer's Comment for Publication.

The paper introduces a novel hybrid framework combining rule-based methods with supervised and unsupervised machine learning for enhanced threat detection, zero-day vulnerability identification, and automated threat response in software development.

Detailed Reviewer's Report

- This paper proposes a hybrid AI-augmented security framework, demonstrating significant improvements in threat detection and response.
- While the reported 30% increase in known threat detection and 40% reduction in incident response time are impressive, the paper could benefit from a more detailed discussion on the computational overhead and resource requirements of deploying such a complex hybrid model in real-world, large-scale software development environments.
- Additionally, further exploration into the explainability of the unsupervised models, especially for identifying zero-day vulnerabilities, would enhance trust and adoption.
- The methodology section, while referencing CRISP-DM, could provide more specific details on dataset sizes, feature engineering processes, and the specific metrics used for evaluating the unsupervised models beyond just "identification."
- The paper is a good contribution to the field.