link; https://ijaas.iaescore.com/index.php/IJAAS/article/view/22175

# Stacking architecture-endpoint detection: a hybrid multi layered architecture for endpoint threat detection

*Abd Rahman Wahid, Desi Anggreani, Muhyiddin A. M. Hayat, Aedah Abd Rahman, Muhammad Faisal*

## Abstract

Modern endpoint threat detection systems face persistent challenges in balancing detection accuracy, resilience against zero-day attacks, and the interpretability of artificial intelligence (AI) models. Although deep learning (DL) approaches often achieve high accuracy on benchmark datasets, they remain vulnerable to adversarial perturbations and operate as opaque "black boxes," thereby reducing trust and limiting practical adoption in critical infrastructures. This research introduces stacking architecture-endpoint detection (STACK-ED), a hybrid multi-layered architecture for endpoint threat detection. STACK-ED integrates three complementary paradigms: supervised learning for known attack patterns, self-supervised Fgraph-based learning for structural relationships, and unsupervised anomaly detection for emerging or unknown threats. The outputs are consolidated by a meta learner, followed by a post-hoc correction (PHC) mechanism to minimize false negatives. The framework was evaluated on a combined benchmark dataset (CSE-CIC-IDS2018 and UNSW-NB15, hereafter referred to as HIDS-Set). Experimental results demonstrate state-of-the-art performance, achieving an F2-score of 98.89% after hybrid integration and active learning, with the primary optimization objective being the reduction of undetected attacks. Furthermore, the Shapley additive explanations (SHAP) method enhances interpretability by revealing feature contributions, while the PHC successfully recovered 62.64% of missed zero-day candidates. The findings position STACK-ED not only as a highly accurate detection model but also as an adaptive, resilient, and transparent framework, offering practical implications for enterprise-grade endpoint defense and future zero-trust cybersecurity systems.