ISSN 2089-8673 (Print) | 2548-4265 (Online)
Volume 15, Issue 1, 2026, pp. 110-120

TERBIT √A

T4EDR: HYBRID THREAT DETECTION FRAMEWORK FOR EDR BASED ON SEMANTIC RULE EMBEDDING AND CONTEXTUAL NETWORK FLOW ANALYSIS

Muh Dzikri Alfauzan Nuzul[1], Desi Anggreani[1], Muhammad Faisal[1], Abd Rahman Wahid[1,*], Titik Khawa Abd Rahman[2]

[1]Departement of Informatics, Universitas Muhammadiyah Makassar, Indonesia
[2]Department of School of Science and Technology, Asia E University, Malaysia

Abstract

In response to the increasing complexity of cyber threats and attacks, this study proposes an innovative endpoint detection and response (EDR) framework named T4EDR (Transformer for Endpoint Detection and Response). Specifically, it addresses the inefficiencies of traditional systems that rely on static and less adaptive rules. T4EDR integrates semantic analysis methods to interpret security rules and a transformer-based deep learning model to contextually analyze network traffic flows. In the initial phase, thousands of security rules from Wazuh were extracted, embedded, and semantically validated against the MITRE ATT&CK framework, achieving a semantic coherence of 86.43% with a silhouette score of 0.702. Subsequently, the FlowBERT model was designed to classify network traffic flows using the CIC-IDS2018 dataset, achieving 91.1% accuracy, a macro-F1 of 0.79, and a mean Average Precision (mAP) of 0.90, surpassing the quantitative target of 85%. The integration of rule embeddings with FlowBERT hidden states through a linear projector enables adaptive mapping of endpoint activities to relevant security rules, supporting context-based automated responses. The main contribution of this study is an adaptive framework that bridges the gap between traditional rule analysis and deep learning-based detection, thereby enhancing the capability to detect multi-stage threats on modern endpoints.

Keywords: Cyber Security, Deep Learning, Endpoint detection and Response, Transformer, Rule Embedding

Received: 29-09-2025 | **Accepted:** 27-02-2026 | **Available Online:** 31-03-2026
DOI: https://doi.org/10.23887/janapati.v15i1.104059

I. INTRODUCTION

The ability to proactively detect and respond to cyber threats is a key pillar in maintaining the integrity and security of modern technology ecosystems. The increasing complexity of threats and multi-stage attacks specifically targeting endpoints as strategic entry points highlights this urgency [1]. Recent industry reports indicate that more than 70% of cyberattacks originate from endpoint compromise, which then escalate into lateral exploitation and data exfiltration [2]. Under such conditions, signature-based detection proves insufficiently adaptive as it heavily relies on manually updated threat databases [3].

Academic research in the fields of network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS) has leveraged machine learning and deep learning to improve attack classification accuracy [4, 5]. Deep learning methods such as Convolutional Neural Networks (CNN) [6] and Long Short-Term Memory (LSTM) [7] have demonstrated strong performance in detecting temporal anomalies [8]. Nevertheless, further studies reveal that these models struggle when faced with new data distributions (domain shift) and often behave as black-box systems, making it difficult to align their outputs with standard security frameworks [9, 10].

On the other hand, rule-based approaches employed in platforms such as Wazuh provide semantic clarity due to their reliance on explicit rules [11]. However, such systems face limitations in detecting novel attacks, lack scalability, and are prone to generating false positives [12]. This underscores a gap between rule-based methods, which are interpretable but static, and deep learning approaches, which are adaptive but opaque [13].

*Corresponding author: 105841116522@student.unismuh.ac.id (A. R. Wahid)