© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1718202

Development Of An AI-Enhanced Intrusion Detection System for Detecting Zero-Day Attacks in Enterprise Networks

EMMANUEL UDEME EDET[1], DR. NELSON OGBOGU[2]
[1, 2]*University of Portharcourt*

Abstract- ***Zero-day attacks pose a significant threat to modern enterprise networks because they can exploit previously unknown vulnerabilities before security patches or signatures are available. Traditional intrusion detection systems (IDS), which rely primarily on signature-based detection, are inadequate for identifying such emerging threats. This paper presents the development of an AI-enhanced hybrid intrusion detection system designed to improve the detection of zero-day attacks in enterprise environments. The proposed system integrates machine learning and deep learning techniques within a hybrid framework that combines anomaly-based and misuse-based detection mechanisms. Network traffic data are subjected to preprocessing operations including feature extraction, normalization, and dimensionality reduction before classification using supervised and unsupervised learning models. Experimental evaluation demonstrates that the proposed IDS achieves higher detection accuracy and lower false positive rates compared to conventional IDS approaches. The results confirm that artificial intelligence significantly enhances enterprise security by enabling adaptive and real-time threat detection. This study contributes a practical and scalable framework for deploying intelligent intrusion detection systems capable of responding effectively to evolving cyber threats.***

Keywords: Intrusion Detection System, Zero-Day Attacks, Artificial Intelligence, Machine Learning, Deep Learning, Enterprise Networks, Cybersecurity.

I. INTRODUCTION

The rapid digital transformation of enterprise environments has led to increased reliance on interconnected information systems, cloud computing platforms, and Internet of Things (IoT) devices. While these technologies improve operational efficiency and scalability, they also expand the attack surface available to cyber adversaries. As a result, cyberattacks have become more sophisticated, with zero-day exploits representing one of the most severe security challenges.

Zero-day attacks exploit previously unknown vulnerabilities, allowing attackers to bypass traditional security controls. Intrusion Detection Systems (IDS) play a critical role in monitoring network traffic and identifying malicious activities. However, conventional IDS solutions are largely based on signature matching, which requires prior knowledge of attack patterns. Although effective against known threats, signature-based IDS are incapable of detecting zero-day attacks due to the absence of predefined signatures. Anomaly-based IDS offer an alternative by identifying deviations from normal behavior, but they often suffer from high false positive rates.

Recent advancements in artificial intelligence (AI) and machine learning (ML) have introduced new possibilities for enhancing intrusion detection. AI-driven IDS solutions can learn complex traffic patterns, adapt to evolving threats, and detect anomalies indicative of zero-day exploits. This research focuses on the development of an AI-enhanced hybrid IDS that integrates machine learning and deep learning models to improve detection accuracy and reduce false alarms in enterprise networks.

The objectives of this study are to design a comprehensive IDS framework, implement AI-based detection mechanisms, and evaluate the system's effectiveness in detecting zero-day attacks.

II. RELATED WORK

Numerous studies have investigated the application of machine learning techniques to intrusion detection. Early research focused on traditional classifiers such as Decision Trees, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Naïve Bayes. While these approaches improved detection rates compared to purely signature-based systems, their performance depended heavily on manual feature engineering and the availability of labeled datasets.

More recent research has explored deep learning techniques, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models. These models demonstrate strong capabilities in automatically learning hierarchical and temporal features from network traffic data, making them suitable for detecting sophisticated and evolving attacks.

Hybrid IDS architectures that combine misuse-based and anomaly-based detection have also gained attention. Such systems aim to leverage the precision of signature-based detection while maintaining the adaptability of anomaly-based approaches. Despite these advances, challenges such as high false positive rates, scalability limitations, and concept drift in dynamic enterprise environments remain unresolved. This study addresses these limitations by proposing a practical AI-enhanced hybrid IDS architecture tailored for enterprise networks with a focus on zero-day attack detection.

III. SYSTEM ARCHITECTURE

The proposed AI-enhanced IDS adopts a layered architecture consisting of data acquisition, preprocessing, feature engineering, AI-based detection, and response modules.

3.1 Data Acquisition Layer

Network traffic is captured using packet sniffers and flow exporters deployed at strategic locations within the enterprise network, including core switches and network gateways. Both packet-level and flow-level data are collected to ensure comprehensive traffic visibility.

3.2 Preprocessing Layer

Raw network traffic often contains noise, redundancy, and incomplete records. Preprocessing operations include the removal of corrupted data, normalization of numerical features, encoding of categorical attributes, and handling of missing values. Dimensionality reduction techniques such as Principal Component Analysis (PCA) are applied to reduce computational complexity while preserving essential information.

3.3 Feature Engineering

Relevant features such as packet size, protocol type, flow duration, byte count, and connection frequency are extracted. Statistical and temporal features are also generated to capture behavioral patterns commonly associated with zero-day attacks.

3.4 AI-Based Detection Engine

The detection engine employs a hybrid approach combining multiple learning paradigms:

- Supervised Learning: Random Forest and Support Vector Machine models are trained on labeled data to identify known attack patterns.
- Deep Learning: LSTM networks analyze sequential traffic behavior to detect subtle temporal anomalies.
- Unsupervised Learning: Autoencoders identify deviations from learned baseline network behavior, enabling the detection of previously unseen attacks.

Model outputs are fused using ensemble techniques to enhance robustness and accuracy.

3.5 Alerting and Response Module

Detected threats are categorized based on severity and forwarded to the Security Operations Center (SOC). Automated response actions, such as blocking malicious IP addresses or isolating compromised hosts, can be triggered for high-risk events.

IV. METHODOLOGY

4.1 Dataset Preparation

Publicly available intrusion detection datasets and simulated enterprise traffic are used for training and evaluation. The dataset includes normal traffic and various attack categories, with an emphasis on novel

and modified attack patterns to emulate zero-day behavior.

4.2 Model Training

The dataset is divided into training, validation, and testing subsets. Supervised models are trained using labeled data, while unsupervised models learn baseline behavior from benign traffic. Hyperparameters are optimized using cross-validation techniques.

4.3 Evaluation Metrics

System performance is evaluated using accuracy, precision, recall, F1-score, false positive rate, and detection latency to provide a balanced assessment of detection effectiveness and operational efficiency.

4.4 Implementation Environment

The IDS is implemented using Python with machine learning libraries including TensorFlow and Scikit-learn. The system is evaluated in a simulated enterprise network environment to assess real-time performance.

V. RESULTS AND ANALYSIS

Experimental results show that the proposed AI-enhanced IDS significantly outperforms traditional signature-based systems. The ensemble detection framework achieves high detection accuracy while maintaining a low false positive rate. Deep learning models effectively capture temporal dependencies in traffic flows, enabling early detection of anomalous behavior.

Dimensionality reduction and feature selection techniques substantially reduce processing time, making the system suitable for real-time enterprise deployment.

VI. DISCUSSION

The findings confirm that artificial intelligence enhances IDS effectiveness, particularly for zero-day attack detection. The hybrid integration of supervised, unsupervised, and deep learning models provides a balance between accuracy and adaptability. However, challenges related to model interpretability and dataset bias remain and must be addressed in future deployments.

VII. CONCLUSION AND FUTURE WORK

This study presented an AI-enhanced hybrid intrusion detection system for detecting zero-day attacks in enterprise networks. The proposed architecture demonstrates improved detection accuracy and reduced false positives compared to conventional IDS solutions. Future work will focus on integrating explainable AI techniques, evaluating performance using live enterprise traffic, and implementing automated incident response mechanisms. Further research will also explore federated learning approaches to support collaborative threat intelligence while preserving data privacy.

REFERENCES

[1] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, 305–316. https://doi.org/10.1109/SP.2010.25

[2] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[3] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066

[4] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

[5] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

[6] Zhang, J., & Zulkernine, M. (2006). Anomaly based network intrusion detection with

unsupervised outlier detection. Proceedings of the IEEE International Conference on Communications, 2388–2393. https://doi.org/10.1109/ICC.2006.255060

[7] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.