KOMPUTIKA

NEWSLETTER

November 2024
Issue

Harnessing AI for Zero-Day Attack Detection: Advancing Cybersecurity with Hybrid Models and Anomaly Detection

INSIDE

—

TAG

[Artificial Intelligence] [Autoencoders] [Cybersecurity] [Random Forest] [Zero-Day Attacks]

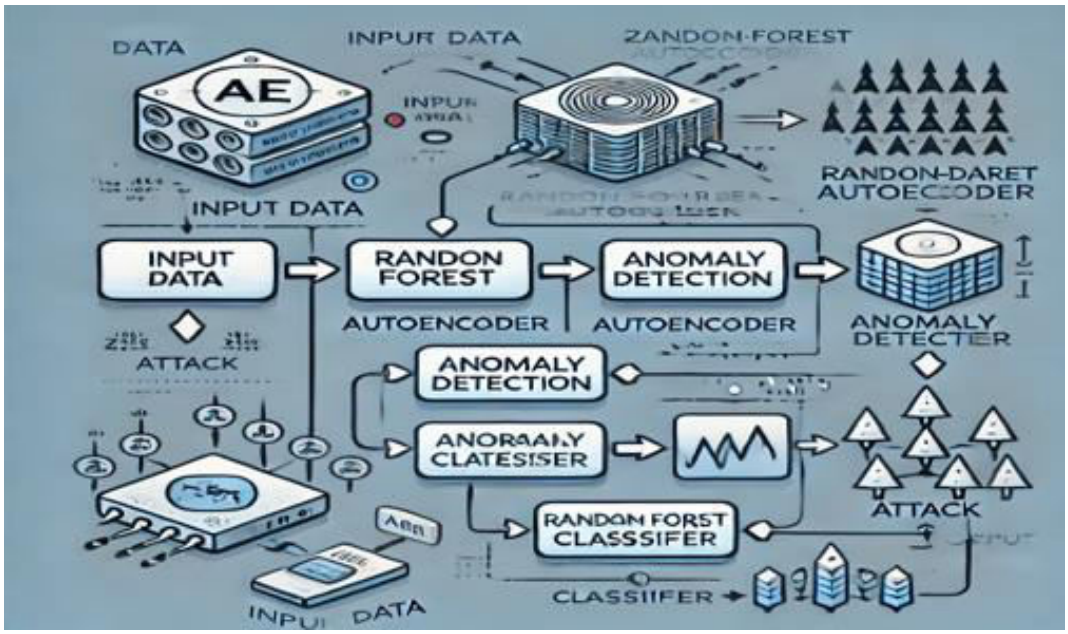
—

AFFILIATION

Department of Computer Systems and Technology,

Faculty of Computer Science and Information Technology,

Universiti Malaya



Conceptual design of an Autoencoder with Traditional Machine Learning Model

Detecting Zero-Day Attacks with AI

– By Prof Dr Por Lip Yee, Yen-Lin Chen, Chin Soon Ku, Koo Yuen Phan, Farid Binbeshr, Roohallah Alizadehsani, Paweł Pławiak, Jing Yang, Siew Juan Leem, Yi Chen, Zhen Dai

Introduction

The escalating threat of cyberattacks has heightened the need for advanced intrusion detection systems, especially against elusive zero-day attacks. Zero-day attacks exploit undiscovered vulnerabilities, leaving systems vulnerable before patches are available. This article reviews and synthesizes cutting-edge AI-based methodologies for detecting zero-day attacks and explores the associated challenges, drawing from a systematic literature review (SLR) by the authors' team. Additionally, the article highlights the integration of anomaly detection techniques, such as autoencoders, with machine learning models to enhance detection performance for previously unseen data.

AI-Driven Detection Methods

Several AI-based techniques are employed for zero-day attack detection, including supervised learning, deep learning, hybrid models, and anomaly detection:

1. Supervised Learning

Machine learning models like Random Forest and Extreme Gradient Boosting (XGBoost) rely on labeled data to detect patterns. However, in zero-day scenarios, the limitation of pre-labeled attack data can reduce their effectiveness. Recent advancements integrate anomaly detectors like autoencoders with these models to improve performance against novel threats. The combination of Random Forest with autoencoders (Random Forest-AE) has demonstrated high accuracy in identifying zero-day attacks in unseen data.

2. Deep Learning

Deep learning models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are increasingly used to detect zero-day attacks. CNNs have shown effectiveness in malware detection using image-based techniques, while RNNs, particularly Long Short-Term Memory (LSTM), can predict malicious behavior over time. The challenge remains the high computational resources these models require.

3. Hybrid Models

Hybrid models combine the strengths of machine learning and deep learning. For instance, models like LightGBM and autoencoders work together to classify data and detect anomalies that traditional methods might overlook. These models enhance detection by learning from both normal and attack patterns.

4. Anomaly Detection

Anomaly-based methods focus on identifying deviations from normal behavior. These methods are particularly suited for zero-day detection as they do not rely on predefined signatures. Systems like Distributed Anomaly Detection (DAD) use statistical models to detect unusual behaviors, enabling real-time identification of unknown threats.

Challenges in Zero-Day Detection

Despite these advancements, significant challenges persist:

1. Data Quality and Processing

The quality of training data is crucial in AI-based detection systems. Incomplete or unrealistic data can result in higher false positives and false negatives. Additionally, imbalanced datasets, where attack data is limited compared to normal traffic, often degrade the model's performance.

2. Computation and Resource Limitations

AI models, particularly deep learning-based approaches, require substantial computational power and memory. For real-time applications, such as edge devices in IoT networks, deploying these models becomes challenging due to limited processing resources.

3. Adaptability and Flexibility

A major concern with current models is their adaptability to new or changing environments. Zero-day attacks evolve rapidly, and models trained on outdated datasets may struggle to detect these novel threats. The lack of real-time adaptability, especially in streaming environments, further complicates their deployment.

4. Real-Time Detection

While anomaly detection techniques excel at identifying unknown threats, the trade-off is often real-time responsiveness. As networks grow more complex, ensuring timely detection of zero-day attacks without sacrificing accuracy is a persistent challenge.

Case Study: Random Forest-AE Model

The integration of autoencoders with traditional machine learning models provides a promising approach to overcoming some of these challenges. In a recent study using the CIC-MalMem-2022 dataset, the Random Forest-AE model achieved remarkable results, with 100% accuracy, precision, recall, and F1 score on unseen data, as presented in our previous research. This highlights the potential of hybrid models in maintaining high detection performance even when encountering novel attack patterns.

Conclusion

AI-based methods, particularly those integrating anomaly detection techniques, offer promising solutions for detecting zero-day attacks. However, challenges related to data quality, computational resources, and adaptability need to be addressed for more robust real-time detection. Future research should focus on enhancing model flexibility and exploring hybrid solutions that combine the strengths of multiple AI approaches.

For more information, contact the author at porlip@um.edu.my from the Department of Computer System and Network at Universiti Malaya.