Anomaly-Based Intrusion Detection System To Detect Advanced Persistent Threats: Environmental Sustainability

Zahra Oughannou[1], Zakaria EL Rhadiouini[1], Habiba CHAOUI[1], Salmane Bourekkadi[2]

[1] Advanced Systems Engineering Laboratory, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco.
[2] University of Poitiers, France - Ibn Tofail University, Morocco

Abstract. In an evolving digital world, Advanced Persistent Threats (APTs) pose severe cybersecurity challenges. These extended, stealthy cyber-attacks, often elude conventional Intrusion Detection Systems (IDS). To bridge this gap, our research introduces a novel, environmentally conscious, deep learning-based IDS designed for APT detection. The system encompasses various stages from objective definition, data collection and preprocessing, to model development, integration, validation, and deployment. The system, utilizing deep learning algorithms, scrutinizes network traffic to detect patterns characteristic of APTs. This approach improves IDS accuracy and allows real-time threat detection, enabling prompt response to potential threats. Importantly, our system contributes to environmental protection by minimizing power consumption and electronic waste associated with cyberattacks, promoting sustainable cybersecurity practices. Our research outcomes are expected to enhance APT detection, providing robust defense against sophisticated cyber threats. Our environmentally-conscious perspective adds a unique dimension to the cybersecurity domain, underlining its role in sustainable practices.

Index Terms— APT; IDS, anomaly-based Intrusion detection, deep learning; Environmental Sustainability, Sustainable Cybersecurity Practices.

1 Introduction

The proliferation of cyber threats and attacks has made anomaly-based intrusion detection systems (IDS) more important than ever. One of the most insidious types of cyber threats is the Advanced Persistent Threat (APT), which targets end users with access to sensitive data and critical systems within a company or organization [1]. APTs employ various techniques such as social engineering, spear-phishing, and zero-day attacks to gain access to target systems and remain undetected for long periods of time. Anomaly-based intrusion detection systems (IDS) have been developed to detect APTs, but they have

limited capabilities to detect unknown threats. Anomaly- based intrusion detection systems (IDS) have been developed to detect APTs, but they have limited capabilities to detect unknown threats. [2] This research proposes a deep learning-based IDS for detecting APTs, which can analyze the behaviors of malicious codes and classify the threat level of unknown threats. To combat the challenge posed by APT attacks, traditional IDS techniques are no longer sufficient. [3] Deep learning techniques have been proposed as an alternative approach to detect anomalies in network traffic and identify potential APTs. The purpose of this research is to explore the effectiveness of deep learning in detecting APT attacks and to propose a new methodology that improves the accuracy and efficiency of APT detection. Our proposed solution is to develop an anomaly-based Intrusion Detection System to detect APTs using a deep learning approach. The methodology involves defining the scope and objectives, collecting and preprocessing data, developing the deep learning model, evaluating its performance, integrating the model with an anomaly IDS, validating and fine-tuning the model, and finally, deploying the system. By simulating APT attacks in a lab environment and using appropriate NN architecture, we aim to improve the accuracy and effectiveness of APT detection. We anticipate that our proposed methodology will improve the detection accuracy of APT attacks and reduce the false positive rate compared to traditional IDS approaches. By utilizing deep learning, our approach can adapt to new and evolving attack patterns, making it more effective and robust against APTs. We will evaluate the performance of our proposed methodology by comparing it to traditional IDS techniques using a public dataset of network traffic, and report the detection accuracy, false-positive rate, and other relevant metrics.

.

1.1 Related works

Deep Learning (DL) methodologies are increasingly being utilized in anomaly-focused Intrusion Detection Systems (IDS) to enhance their precision and efficiency. DL algorithms have demonstrated significant efficacy in fields such as image analysis and natural language processing, and have recently been extended to network traffic analysis for detecting anomalies. A variety of DL-oriented methods have been introduced in academic research for Advanced Persistent Threat (APT) detection through anomaly-centric IDS. In the study [4], a relatively basic Multilayer Perceptron (MLP) classifier was introduced for a five-category classification, accomplishing an accuracy of 81.43%. In the same study, an Auto-Encoding model was used and achieved an accuracy of 87% on the Test+ dataset. In research [5], a combination of two-dimensional Convolutional Neural Network (CNN) and Bi-directional Long Short-Term Memory (BiLSTM) was utilized to extract spatial and temporal features, respectively, achieving 83.58% accuracy for Test+ using CNN-BiLSTM and 81.75% accuracy for Test+ using CNN alone.
The authors in [6] implemented a set of 122 features to train an LSTM-RNN model for a five-category classification, achieving an accuracy of 82.68% on Test+. In paper [7], models such as CNN, Gated Recurrent Unit (GRU), and Random Forest (RF) were trained for binary classification, reaching accuracies of 82.92%, 83.19%, and 80.14% respectively on Test+ and 68.3%, 68.52%, and 62.34% respectively on Test-21.
In the research [8], the authors boosted the performance of the Auto-Encoder Network for anomaly detection to reach an accuracy of 90.61% on Test+. Similarly, the authors in [9] suggested a Multi-CNN with discrete preprocessing, achieving an accuracy of 83% for classifying the attack type on Test+.
In the study [10], an approach was introduced to address class imbalance prior to applying any training models. Various techniques, including the Difficult Set Sampling Technique

(DSSTE), were utilized, with the best performance (82.84% accuracy) obtained using AlexNet for categorical classification.
On the other hand, the authors of [11] utilized a CNN in conjunction with TSODE, a novel variant of the Transient Search Optimization (TSO) algorithm. This algorithm used Differential Evolution (DE) to balance between exploitation and exploration, thereby achieving an accuracy of 75.75% in categorical classification and 77.38% in binary classification.
Lastly, in the paper [12], a two-stage DL structure was proposed, with GRU being used in the first stage and Denoising Auto-Encoder (DAE) in the second stage, resulting in an accuracy of 90.21% on Test+ for intrusion detection.
From these studies, it is evident that deep learning has played a substantial role in enhancing the accuracy and efficiency of anomaly-centric IDS. Machine learning models like MLP, CNN, GRU, and RF have been utilized to extract spatial and temporal features, classify attacks, and enhance anomaly detection.

Table 1. Comparative analysis of detection methods, algorithms, and their accuracy rates for advanced persistent threats (APTs)

References	Model(s) Used	Classification type	Accuracy on Test+
[4]	MLP	Five-class	81.43%.
	Auto-Encoding model	-	87%
[5]	CNN	Spatial feature extraction	83.58%
	CNN-BiLSTM	Spatial and temporal feature extraction	82.68%
[6]	LSTM-RNN	Five-category classification	82.68%
[7]	CNN	Binary classification	82.92%
[7]	GRU	Binary classification	83.19%
	RF		80.14%
[8]	Auto-Encoder Network	Anomaly detection	90.61%
[9]	Multi-CNN with discrete preprocessing	Attack type classification	83%
[10]	Difficult Set Sampling Technique (DSSTE)	Class imbalance handling	82.84%
[11]	CNN	Categorical and binary classification	75.75%
	TSODE (with DE)		77.38%
[12]	GRU, Denoising Auto-Encoder (DAE)	-	90.21%

2 Problem statement

The problem of accurately detecting Advanced Persistent Threats (APTs) using anomaly-based Intrusion Detection Systems (IDS) remains a challenge. Anomaly-based IDS rely on identifying deviations or patterns of atypical behavior in network traces and host logs, but the complex and evolving nature of APTs often leads to inaccurate detections, including false positives and false negatives.[13] To improve the accuracy of anomaly based IDS in detecting APTs, there is a need for advanced techniques such as deep learning. The focus of this research is to propose a novel approach that leverages deep learning to enhance the accuracy of anomaly-based IDS in detecting APTs.

3 Methodology

Our solution is to develop an anomaly-based Intrusion Detection System to detect APT's using deep learning approach to solve the challenges discussed in the Problem Statement, using the following steps: 1. Define the scope and objectives: Define the scope of the project by identifying the network or system to be monitored and the type of APTs to be detected. Establish the objectives of the project by identifying the expected outcomes and success metrics. 2. Collect and preprocess data: Collect network or system logs, network traffic, and other relevant data. Preprocess the data by cleaning, normalizing, and transforming it to ensure its suitability for use in a deep learning model. Since the dataset is not available and private on the web, we must simulate those attacks by creating a lab to do so. 3. Develop the deep learning model: After the data preprocessing and selecting the best features to train the model with we get to choose an appropriate NN architecture to give the best result. 4. Evaluate the model: Evaluate the performance of the deep learning model by measuring metrics, such as precision, recall, and F1-score. Use techniques, such as cross validation to ensure the model's accuracy and generalizability. And we will compare our results to the result of the previous work of the other researchers. 5. Integrate the model with an anomaly IDS: Integrate the trained deep learning model with an anomaly IDS to detect APTs in real-time. Configure the IDS to trigger alerts when anomalies are detected. By designing an architecture of (NIDS or HIDS) 6. Validate and fine-tune the model: Validate the performance of the deep learning- based anomaly IDS by testing it against a range of APT scenarios. Fine-tune the model and the IDS based on the results of the testing. 7. Deploy the system: Deploy the deep learning-based anomaly IDS to the production environment. Monitor the system's performance and refine it over time to ensure its effectiveness in detecting APTs.

4 Potential Research Contributions

The objective of this study is to investigate the potential of deep learning in improving the accuracy and effectiveness of network intrusion detection systems (IDSs) for the purpose of enhancing data protection. Our research will contribute to this domain by exploring the following aspects: 1. Improved Detection Accuracy: Deep learning models can learn complex patterns and relationships in data, enabling more accurate detection of anomalous network behavior and potential APTs. 2. Early Detection: APTs are designed to operate stealthily and can evade traditional IDSs for extended periods. Deep learning-based IDSs

can detect suspicious network activity early, enabling rapid response to potential threats. 3. Adaptability: Deep learning models can adapt to changes in network traffic patterns and identify new and emerging threats, making the IDS more effective in detecting APTs that are constantly evolving. 4. Improved Incident Response: Deep learning-based anomaly detection can provide detailed insights into network activity, which can help security teams respond more effectively to incidents and minimize the damage caused by APTs.

5 Conclusion & Future Works

In this research proposal, we have proposed a deep learning based anomaly intrusion detection system that aims to improve the accuracy and efficiency of APT detection. By leveraging the power of deep learning, our proposed approach can detect new and evolving APT attack patterns, making it more robust and effective than traditional IDS approaches. Through extensive experimentation and analysis, we aim to demonstrate the potential of our approach in detecting APT attacks with higher accuracy and fewer false positives. The proposed research is just the beginning of the development of deep learning-based anomaly intrusion detection systems. In the future, we aim to further refine our approach and explore other avenues of research in this field. Some possible directions for future work include: ▪ Validation: Conducting further experimentation and validation of the proposed approach using real-world APT attack scenarios to measure its effectiveness. ▪ Performance Optimization: Improving the efficiency of our proposed approach by optimizing its computational resources, such as reducing the computational complexity and optimizing hardware configurations. ▪ Integration: Integrating the proposed approach into existing network security infrastructure to enhance the overall cybersecurity of organizations. ▪ Extension: Extending the proposed methodology to other types of cyber threats, such as malware and ransomware, to enhance the overall cybersecurity of organizations. By exploring these directions of research, we believe that our proposed approach can be improved and extended to address the challenges of APT detection and network security in the future.

References

[1]. Seresht, N. A., & Azmi, R. (2015). MAIS-IDS: a distributed intrusion detection system using multi-agent AIS approach. Engineering Applications of Artificial Intelligence, 35, 286-298.
[2]. Gaur, M. S., Sharma, M., & Pant, B. (2015). Trusted and secure clustering in mobile pervasive environment. Human-centric Computing and Information Sciences, 5(32), 19.
[3]. D. Fraunholz, S. D. Anton, C. Lipps, D. Reti, D. Krohmer, F. Pohl, M. Tammen, and H. D. Schotten, "Demystifying Deception Technology: A Survey," 2018.
[4]. C. Ieracitano, A. Adeel, M. Gogate, K. Dashtipour, F. C. Morabito, H. Larijani, A. Raza, and A. Hussain, "Statistical analysis driven optimized deep learning system for intrusion detection," in International conferenceon brain inspired cognitive systems. Springer, 2018, pp. 759–769.
[5]. K. Jiang, W. Wang, A. Wang, and H. Wu, "Network intrusion detection combined hybrid sampling with deep hierarchical network," IEEE Access, vol. 8, pp. 32 464–32 476, 2020.
[6]. P. Muhuri, P. Chatterjee, X. Yuan, K. Roy, and A. Esterline, "Using a long short-term memory recurrent neural network (lstm-rnn) to classify network attacks," Information, vol. 11, p. 243, 05 2020.
[7]. A. Andalib and V. T. Vakili, "An autonomous intrusion detection system using an ensemble of advanced learners," in 2020 28th Iranian Conference on Electrical Engineering (ICEE), 2020, pp. 1–5.

[8]. W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, "Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset," IEEE Access, vol. 9, pp. 140 136–140 146, 2021.
[9]. J. Yoo, B. Min, S. Kim, D. Shin, and D. Shin, "Study on network intrusion detection method using discrete preprocessing method and convolution neural network," IEEE Access, vol. 9, pp. 142 348–142 361, 2021.
[10]. L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning," Ieee Access, vol. 9, pp. 7550– 7563, 2020.
[11]. A. Fatani, M. Abd Elaziz, A. Dahou, M. A. Al-Qaness, and S. Lu, "Iot intrusion detection system using deep learning and enhanced transient search optimization," IEEE Access, vol. 9, pp. 123 448–123 464, 2021.
[12]. M.-T. Kao, D.-Y. Sung, S.-J. Kao, and F.-M. Chang, "A novel two-stage deep learning structure for network flow anomaly detection," Electronics, vol. 11, p. 1531, 05 2022.
[13]. M. H. Almeshekah and E. H. Spafford, "Planning and integrating deception into computer security defenses," in Proceedings of the 2014 New Security Paradigms Workshop, 2014, pp. 127–138.