Annals of the University of Petroşani, Electrical Engineering, 25 (2023)

ARTIFICIAL INTELLIGENCE APPLIED IN NETWORK SECURITY

MATEI-VASILE CĂPÎLNAŞ[1]

Abstract: The purpose of this paper is to analyze methods for the development of a system capable of recognizing potential attacks and/or preventing cyberattacks, which have become increasingly prominent in recent years. The overall objective of the system is to assist qualified individuals in the field, optimizing their analysis processes and providing as precise reports as possible to combat cybercrimes. To achieve this goal, artificial intelligence techniques will be used, particularly focusing on deep learning techniques due to their success in addressing similar problems in recent years.

Key words: artificial intelligence, cyberattacks, cybersecurity.

1. INTRODUCTION

According to [1], starting from the 19th century, researchers have studied anomaly detection and produced numerous works using various techniques, from statistical models to evolutionary computation approaches. However, it is not easy to identify and classify all existing anomaly detection techniques because various factors must be considered, such as the type of anomaly, the system, the techniques and algorithms used, as well as technical dilemmas like processing costs and network complexity. Consequently, the available literature today is fragmented, and many works attempt to summarize everything but fail to present the complete picture of the anomaly detection spectrum.

Network anomalies can be caused by a variety of factors, including network attacks, infections with malware programs, improperly configured network devices, or even legitimate user behavior that falls within normal activity limits. Detecting and identifying network anomalies is an important aspect of network security because it can help organizations identify and respond to potential threats promptly. Various tools and techniques, such as Intrusion Detection Systems (IDS), network monitoring software, and machine learning algorithms, can be used to detect and analyze network anomalies.

[1]*Ph.D. Student, Assist. Prof. Eng., University of Alba Iulia, capilnas.matei@uab.ro*

2. INTRUSION DETECTION IN IOT NETWORKS USING DEEP LEARNING ALGORITHM

In the study by [2], researchers utilized a dataset to classify attacks. They employed machine learning techniques (specifically Random Forest: RF) as well as deep learning methods, including Convolutional Neural Network (CNN) and Multi-Layer Perceptron (MLP). The anticipated outcome of this research is the implementation of results into a Network Intrusion Detection System (NIDS), enabling anomaly detection in an IoT network.

Their study investigated various machine learning and deep learning algorithms within an IoT network. Specifically evaluating RF, CNN, and MLP algorithms, they found that RF and CNN provided the highest accuracy and Area Under the Curve (AUC) for multiclass classification. Experiments were conducted with different batch sizes, noting that including epochs in trials with 32 and 64 batches slightly decreased accuracy, while trials with 128 batches slightly increased accuracy.

Moreover, it was discovered that increasing batch size could expedite the computation process. Doubling the batch size in MLP resulted in computation 1.4-2.6 times faster, while CNN led to a process 1.8-2.4 times faster.

3. NETWORK ANOMALY DETECTION: A MACHINE LEARNING PERSPECTIVE

Bayesian networks are often used in conjunction with statistical methods, offering several advantages for data analysis. They can handle missing data, represent causal relationships, and merge prior knowledge with data. In the article by [3] a system based on this network is proposed. In the field of anomaly detection in networks, several variations of the basic Bayesian network technique have been suggested. These techniques can capture conditional dependencies between different attributes using complex Bayesian networks. Bayesian techniques have been commonly used for classification and false alarm suppression.

A multisensor fusion approach has been proposed where outputs from different IDS sensors are aggregated to produce a single alarm. This approach assumes that no anomaly detection technique can classify a set of events as an intrusion with enough confidence.

The advantages of using Bayesian networks for anomaly detection in networks are numerous. They allow the representation of interrelationships among dataset attributes, are easily understood by human experts, and can be easily modified as needed. Bayesian networks permit explicit characterization of uncertainty, quick and efficient computation, and fast training. Their high adaptability, ease of construction, and ability to explicitly represent domain-specific knowledge make Bayesian networks attractive for anomaly detection in networks. However, it's essential to consider the method's limitations.

The accuracy of the method relies on certain assumptions based on the behavioral model of the target system, and deviation from these assumptions will decrease its precision.

4. THE ANALYSIS OF FIREWALL POLICY THROUGH MACHINE LEARNING AND DATA MINING

An interesting approach can be observed in the study by [4]. To conduct this study, researchers extracted data from a firewall. However, they encountered an issue - a single log file containing a large amount of data would have used up the entire firewall memory. To overcome this problem, the researchers decided to save the data in smaller chunks using the firewall's own interface. Specifically, they saved the data in 48 pieces, each of which could be used as training data for the study.

By using smaller data chunks, the researchers managed to avoid overwhelming the firewall's memory and conduct the study more efficiently. This approach also allowed them to gain a better understanding of the firewall's behavior as they could analyze each data chunk in detail. Overall, the decision to save the data in 48 pieces proved to be a smart move and helped the researchers achieve their research objectives.

12 training data chunks were analyzed using 6 different classifiers (Naive Bayes, kNN, DecisionTable, HyperPipes, OneR, and ZeroR) to identify the most efficient machine learning algorithms.

Despite the availability of a large number of algorithms, only 6 were selected for further analysis based on their performance in preliminary tests. These 6 algorithms were chosen for their ability to produce the best results and employed different approaches in machine learning.

5. ANALYSIS OF TRAFFIC FROM A SOCIAL MEDIA PLATFORM NETWORK

The study [5] serves as a good starting point in approaching network traffic analysis. With the onset of the COVID-19 pandemic in 2020 and last year in 2022, coinciding with the outbreak of the conflict in Ukraine, there has been a noticeable increase in user activity on social networks. For many, this virtual environment serves as a refuge during challenging times, a space where they can express their feelings through images or comments. Building on this aspect, in 2022, within a research project, we decided to develop a web application to collect comments in Romanian regarding specific images with different emotional impacts.

Starting from the developed application, I believe that improving it to transform it into a social media platform (where users can upload their own photos and interact with each other) could lead to creating an optimal environment for network traffic analysis. Gathering logs generated when a user performs a normal action (e.g., uploading a photo) or when someone attempts an attack on an account or the entire application could yield a dataset usable in developing an intrusion detection and prevention system.

A major issue that might arise in creating such an environment is developing the application in a way that inadvertently introduces security vulnerabilities. This could jeopardize the entire network, and to mitigate risks, the concept of a DMZ (demilitarized zone) must be considered.

6. CONCLUSIONS

The amalgamation of cybersecurity and artificial intelligence heralds a promising frontier, as recent studies vividly illustrate. The symbiotic relationship between these realms promises groundbreaking solutions, from robust threat detection to adaptive defense mechanisms. However, amidst this potential lies a landscape riddled with challenges. Existing problems persist, spanning from the ethical implications of AI-powered security to the vulnerability of AI systems to sophisticated attacks. Bridging these gaps demands a concerted effort, leveraging innovation while navigating the ethical and security pitfalls. As these fields evolve, a balanced synergy between cybersecurity and AI becomes not just a necessity but a pivotal determinant of our digital resilience in an increasingly complex threat landscape.

REFERENCES

[1]. Bhattacharyya D.K., Kalita J.K., *Network anomaly detection: A machine learning perspective*, Crc Press, 2013.

[2]. Fernandes G., et al., *A comprehensive survey on network anomaly detection*, Telecommunication Systems 70, pp. 447–489, 2019.

[3]. Salloum S.A. et al., *Machine learning and deep learning techniques for cybersecurity: a review*", Proceedings of the International Conference on Artificial Intelligence and Computer Vision, Springer, pp. 50–57, 2020.

[4]. Susilo B., Sari R.F., *Intrusion detection in IoT networks using deep learning algorithm*, Information 11.5, p. 279, 2020.

[5]. Ucar E., Ozhan E., *The analysis of firewall policy through machine learning and data mining*", Wireless Personal Communications 96, pp. 2891–2909, 2017.