PENINSULA PUBLISHING LLC

SHIFRA
Vol. **(2023)**, 2023, **pp**. 17–25
ISSN: 3078-3186

Research Article

Mitigating Developed Persistent Threats (APTs) through Machine Learning-Based Intrusion Detection Systems: A Comprehensive Analysis

Abdul Samad Bin Shibghatullah [1,*]

[1] *College of Computing & Informatics (CCI), Universiti Tenaga Nasional, Kajang, Selangor, Malaysia.*

ARTICLEINFO

Article History
Received 13 Oct 2022
Revised: 19 Dec 2022
Accepted 20 Feb 2023
Published 16 Mar 2023

Keywords
Mitigating Developed APTs,
Machine Learning,
Intrusion Detection Systems,
Comprehensive Analysis.

ABSTRACT

Persistent threats (APTs) pose a significant challenge to cybersecurity due to their incredible evasive nature. Identification systems often fail to recognize APTs, resulting in significant data breaches and lost revenue. This study aims to solve this problem by developing a machine learning based intrusion detection system (IDS) specifically designed for APT detection This study aims to evaluate the performance of different machine learning algorithms for APT detection, IDS integration of these algorithms are efficient. The system includes integration and evaluation of system performance under real-world conditions. A major contribution of this research includes a comprehensive investigation of machine learning methods for APT recognition, IDS reprogramming, extensive empirical validation using real-world data Findings show that the proposed IDS greatly improves detection accuracy while reducing false positives for.

1. INTRODUCTION

The cybersecurity industry faces an ongoing and growing threat from Advanced Persistent Threats (APTs). APTs are sophisticated, stealthy, and protracted cyberattacks, often carried out and coordinated by highly sophisticated and well-funded adversaries, such as nation-states or organized cybercrime groups, viz as opposed to traditional cyberattacks, which are generally aimed at immediate profit or damage [1] . APTs are designed for long-term deployment, allowing attackers to surreptitiously extract sensitive information, manipulate data, or destroy sensitive long-term APTs that are persistent and stealthy makes it especially dangerous, difficult to detect and mitigate. APTs use a combination of advanced techniques to maintain undetected access to target networks to breach security. These techniques typically include spear phishing, zero-day vulnerabilities, customized malware, and sophisticated social engineering techniques. Once inside the network, APTs move sideways to identify and exploit high-value assets, adapting to maintain visibility [2]. While emphasizing the importance of strengthening security strategies in the fight against APTs, this shifting and changing behavior calls for improved security techniques and similarly adapting APTs detection is critical in cybersecurity. The stealth nature of APTs allows attackers to remain undetected for extended periods of time, during which time they can cause significant damage including theft of intellectual property, economic loss and critical infrastructure a they destroy Traditional security systems often fail to detect these threats due to their reliance on known attack patterns and signatures [3]. Proper detection of APTs can reduce the risk of damage, protect critical information, and ensure the integrity and availability of critical systems . Thus, advanced detection systems that can detect and respond to APTs are critical to cope with cybersecurity. Despite the critical importance of effective APT detection, traditional intrusion detection systems (IDS) are severely limited in addressing this threat [4]. Traditional IDS typically relies on signature-based detection methods, which perform well against known threats but are inadequate against new and evolving APT techniques These systems often do not recognize an APT types are sophisticated and variable, resulting in significant data breaches and economic losses [5].

This figure illustrates the machine learning model workflow for classifying network traffic in a cybersecurity environment . The process begins with data collection, where network traffic data is collected and stored in a network traffic corpus [6].

*Corresponding author email: abdul.samad@uniten.edu.my
DOI: https://doi.org/10.70470/SHIFRA/2023/003

This information is analyzed and interpreted using Arcsight Moloch (Arkime), where normalization, transformation and reduction are performed in preparation for feature extraction and then 83 features are extracted from the processed data using the CICFlowmeter tool. Then, feature selection is performed using analysis of variance (ANOVA), reducing the number of features to 12 for greater accuracy . These selected features are compiled into a dataset, which is used for model training [7]. The model used is the eXtreme Gradient Boosting (XGBoost) model, which has a specific resolution with a learning rate of 0.1, a maximum depth of 10, 100 estimators, a seed value of 7, and a training/test separation of a it is 80% and 20% . , with a batch size of 10 samples, respectively. The trained system then classifies the network traffic information into various categories including long-range traffic, inspection, priority agreement, segment movement, data dump This workflow provides steps for device design details of learning models for developing and implementing network traffic classification [8].

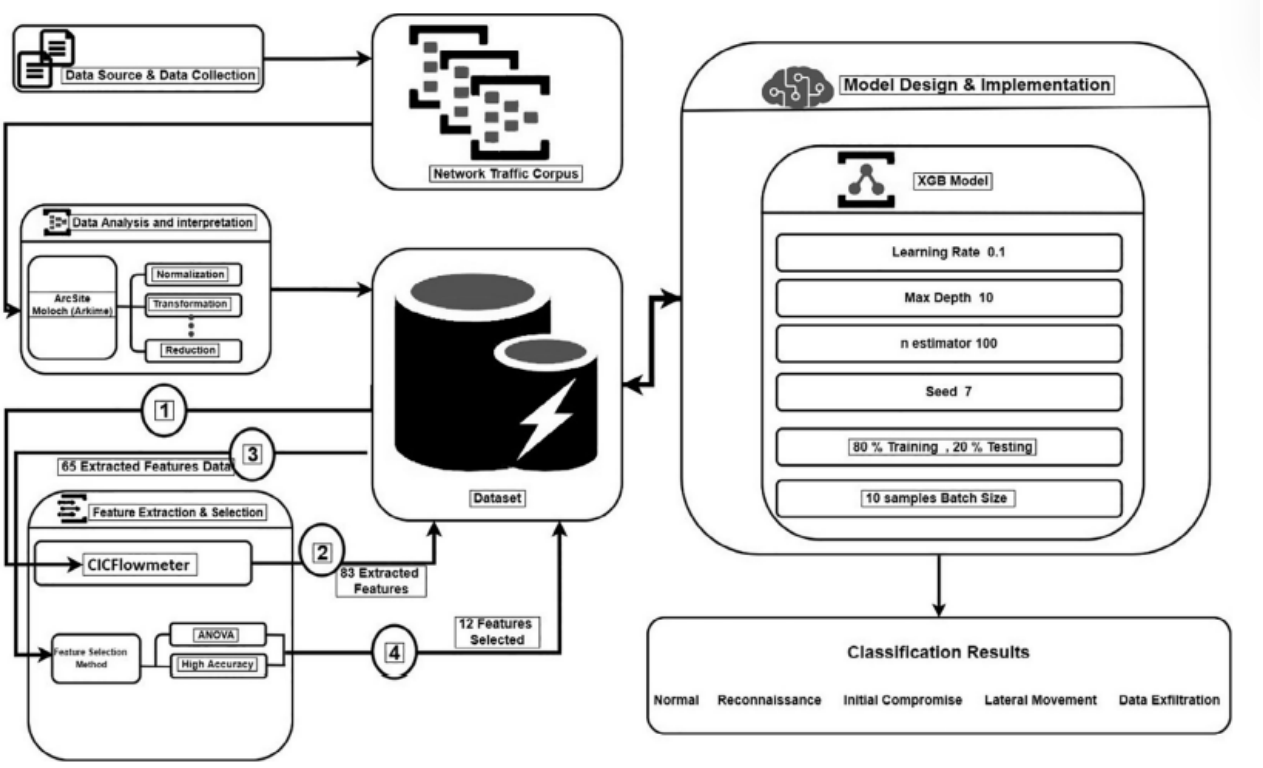

Fig .1. Workflow for Network Traffic Classification Using XGBoost Model in Cybersecurity

Furthermore, traditional IDS generates a high false positive rate, resulting in alert fatigue and making it difficult for security analysts to detect real threats in less threatening alerts To overcome these challenges on, the aim of this research is to develop a machine learning algorithm for intrusion detection [9]. programs to be developed, specifically designed to identify and reduce APTs The main objectives of this review are threefold:

First, the study aims to evaluate the effectiveness of machine learning algorithms in APT detection. It includes detailed analysis of multiple systems, taking into account factors such as detection accuracy, number of false positives, and ability to detect previously unknown threats Through analysis is effectively in these systems upon, the study seeks to determine the most appropriate methods for APT detection .

Second, the research focuses on a collaborative IDS framework that integrates a highly effective machine learning framework. This design will be designed in order to exploit different algorithm capabilities, to ensure optimal threat detection with robust capabilities. The goal is to create a system that can robustly deal with the changing landscape of APTs, providing improved protection against this sophisticated threat [10].

Third, the study aims to assess the performance of the developed IDS system in a real-world setting. It involves testing using real-world data to assess system performance and reliability. By testing the IDS framework in a real scenario, the study seeks to ensure that APT recognition is effective and applicable in a variety of communication scenarios .

This review aims to make many important contributions to cybersecurity:

First, it will provide a comprehensive review of machine learning techniques for APT detection, providing insights into their strengths, weaknesses, and applicability in various contexts This review will be a valuable resource for computing so security professionals and researchers looking to understand the potential of machine learning to improve APT detection .

Second, the research will lead to the development of a new IDS framework that integrates multiple machine learning frameworks. The system is expected to provide improved detection and flexibility compared to traditional IDS. Utilizing the

strengths of different algorithms, the proposed IDS framework aims to provide a robust and effective solution for APT detection and mitigation.
The research will include extensive empirical validation using real-world data. This validation process will demonstrate the efficiency of the proposed IDS algorithm, and highlight its potential to improve detection accuracy while reducing false positives. The findings will lead to robust solutions to mitigate APT in complex networks, help advance cybersecurity practices and develop more flexible security strategies [11].

2. RELATED WORK

Advanced Persistent Threats (APTs) are a class of cyberattacks characterized by their sophisticated techniques, stealthy nature, long lasting and unlike conventional cyberattacks aimed at quick profit or damage is immediately disabled, APTs are designed to gain unauthorized network access and remain undetected for extended periods of time [12]. alter data, or disrupt long-term critical functions. The main characteristics of APTs are advanced strategies to exploit their vulnerabilities, the ability to evade detection through covert operations, and consistency, including ongoing effort to maintain and control damaged systems. The concept of APTs has grown exponentially over the past decades, and several high-profile events have highlighted their impact. One of the first confirmed APT cases was the Titan Rain attack, attributed to Chinese hackers, who targeted the US [13]. defense contractors and government agencies in the early 2000s followed by the Stuxnet worm in 2010, with Iran primarily targeting nuclear facilities, and demonstrating APT capabilities to disrupt critical infrastructure Recent examples include APT29 (2010). Cozy Bear) attacks on government and non-governmental organizations, and the SolarWinds attack in 2020 by the US. a number of government agencies, private And agencies were confused. These events underscore the ongoing threat posed by APTs and their potentially devastating impact on industries. Intrusion detection systems (IDS) are important components of the cybersecurity infrastructure, designed to monitor network traffic and detect malicious activity[14]. Traditional IDS techniques are mainly based on two approaches: signature detection and anomaly-based. Signature-based IDS uses pre-defined patterns or signatures of known threats to detect malicious activity. While effective against known threats, this approach fails to detect new or evolving threats that do not match existing signatures. In other words, an anomaly-based IDS establishes baselines for normal network behavior and flags deviations from these baselines as potential risks. While this approach can detect new attacks, it often generates a lot of false alarms, leaving security analysts with vigilant fatigue[15]. Both methods face severe limitations in APT detection, which are designed to act as stealth and avoid traditional detection methods by using sophisticated listening techniques to mimic fraudulent behavior relevant to Devices learning has emerged as a promising tool in the fight against cyber threats Offers Cybersecurity uses machine learning algorithms to analyze large amounts of data, identify patterns and predict potential threats [16]. Current applications include spam filtering, malware detection, anomaly detection, and behavior analysis. Success stories in this area include advanced threat detection systems with services such as Darktrace, which uses machine learning to identify and respond to threats in real time, and Cylance, which uses artificial intelligence used to analyze file types and predict malware infection. This application demonstrates the potential of machine learning to enhance cybersecurity defenses and identify adaptive and dynamic threats[17].
Despite its potential, the use of machine learning in APT recognition presents several challenges. A key challenge is the need for large and diverse data sets to effectively train machine learning models. APTs are rare and highly targeted, making it difficult to obtain adequate training data. Furthermore, APT is constantly evolving, requiring models to adapt rapidly to new techniques, techniques, and new processes (TTPs). Another challenge is balancing detection accuracy with false positive rates. High false positive rates can overwhelm security units and reduce the effectiveness of detection schemes [18]. However, these challenges also present opportunities for innovation. Improvements in unsupervised learning and anomaly detection can help solve the problem of limited label data by deviating from normal behavior without the need for a prescribed attack signature date on the Additionally, the integration of threat intelligence and context can increase the accuracy and usefulness of machine learning models [19]. The use of ensemble methods combining multiple algorithms can also improve search performance by leveraging the strengths of different methods. Combining machine learning with APT detection offers tremendous potential for enhancing cybersecurity defenses, provided the challenges are addressed with continued research and development The main problem with traditional intrusion detection systems (IDS), especially those that rely on anomaly detection, is the high number of false positives they generate These systems tend to give unnecessary warnings overwhelm security analysts, causing warning fatigue. When analysts are consistently desensitised to false alarms, the likelihood of overlooking real threats increases. This high rate of false positives compromises both the reliability and effectiveness of the IDS, making it difficult to maintain strong security [20].
Another important limitation is the insufficient training data for machine learning models. Effective machine learning models require large and diverse datasets for efficient training. However, due to the rarity and widespread targeting of persistent threats (APTs), it is difficult to collect sufficient data to train these models. This lack of training data prevents the model from detecting and responding accurately to new evolving APT processes, methods, and procedures (TTPs), and limits the effectiveness of the IDS.

The evolution of APTs presents a significant new challenge. As APTs continue to evolve and become more sophisticated, it is imperative that research programs rapidly adapt to new TTPs. Traditional IDS approaches often struggle to keep up with these changes. Constantly updating and optimizing machine learning models is needed to effectively counter the latest threats, which can be resource intensive and complex [21].

Balancing detection accuracy with false positive rates is also an important challenge. Increased false-positive accuracy generally occurs, whereas false-positive reduction can reduce detection accuracy. This balance is important to ensure that IDS are reliable and useful in real-world situations. The optimal balance reduces false positives without compromising detection accuracy, and ensures that the IDS remains effective in detecting real threats [22].

Designing an effective IDS system requires the integration of multiple machine learning algorithms, an inherently complex process. But this integration is necessary to take advantage of the strengths of different algorithms, thus enhancing robust and adaptable threat detection capabilities Effective integration enhances the overall performance of the IDS, and enhances its control Properly address the characteristics of the APT [23].

Many current studies also lack comprehensive empirical evidence using real-world data. Such validation is important for the evaluation of the usefulness and reliability of the IDS system. Without rigorous empirical validation, it is difficult to determine whether the developed systems can perform well in different network environments. This highlights the need for more practical, real-world testing to ensure that IDS can provide reliable protection against APTs. Adaptation of IDS programs to real-world conditions is often poorly considered [24]. Realistic test scenarios are necessary to capture the effectiveness of the system and to understand the practical challenges it may face. Ensuring that an IDS can operate effectively in complex dynamic networks is important for strong defense against APTs. This requires continuous research and development to maintain a high level of safety in real-world applications [25]. These problems and limitations highlight the ongoing challenges in developing machine learning-based IDS for APT mitigation and highlight areas where research and innovation are critical as shown in Table I.

TABLE I. CHALLENGES AND APPLICATIONS OF MACHINE LEARNING-BASED INTRUSION DETECTION SYSTEMS (IDS) FOR ADVANCED PERSISTENT THREATS (APTs)

Problems and Limitations	Description	Applications
High False Positive Rates	Traditional IDS methods, particularly anomaly-based detection, often generate a high number of false positives. This can lead to alert fatigue among security analysts, reducing the effectiveness of the detection system.	Affects the accuracy and reliability of APT detection, leading to potential oversight of genuine threats and overwhelming security teams with false alerts.
Insufficient Training Data	Machine learning models require large and diverse datasets to be effectively trained. APTs are relatively rare and highly targeted, making it difficult to obtain sufficient training data.	Limits the model's ability to accurately detect and respond to new and evolving APT tactics, techniques, and procedures (TTPs).
Evolving Nature of APTs	APTs continually evolve, requiring models to adapt quickly to new TTPs. Traditional IDS methods struggle to keep up with the sophisticated and adaptive nature of APTs.	Necessitates continuous updates and adaptations of machine learning models to remain effective against the latest threats.
Detection Accuracy vs. False Positives	Balancing detection accuracy with false positive rates is challenging. High detection accuracy often comes at the cost of increased false positives, and vice versa.	Critical for ensuring the IDS is both reliable and practical in real-world scenarios, maintaining a balance that minimizes false positives without compromising on detection accuracy.
Integration of Algorithms	Developing a cohesive IDS framework that effectively integrates multiple machine learning algorithms can be complex.	Essential for leveraging the strengths of different algorithms to provide robust and adaptive threat detection capabilities.
Practical Validation	Many studies lack extensive empirical validation using real-world data, which is crucial for assessing the IDS's practicality and reliability.	Ensures that the developed IDS is effective and applicable in diverse network environments, providing robust protection against APTs.
Adaptation to Real-World Scenarios	Assessing the performance of IDS frameworks in real-world scenarios is often limited. Realistic testing conditions are necessary to validate system effectiveness.	Helps in understanding the practical challenges and ensures the IDS can perform effectively in dynamic and complex network environments.

3. METHODOLOGY

A comprehensive study was carefully conducted to address the major challenges in APT detection and mitigation. The approach focused on developing a robust, machine learning-based IDS framework that can fully explore the phenomenal properties of APTs. The first step is “data collection and preprocessing”. To ensure that machine learning models can be trained on different network scenarios, real-world network traffic data were collected from various sources and the data collected included both negative traffic and malicious traffic mimicking APTs. Extensive preprocessing of the data was performed to ensure the accuracy and efficiency of the model training. Noise and redundant information were removed, and the data were normalized in preparation for feature extraction. The study used tools such as “Arcsight Moloch (Arkime)” to analyze and reduce complex data, while “CICFlowmeter” was used to extract 83 critical features from network traffic And for these features is needed to distinguish between normal and malignant APT-related activities.

After preprocessing the data, the next step was “feature selection”. Using “Analysis of Variance (ANOVA)”, the study narrowed down the extracted 83 factors to 12 significant factors that contributed significantly to the identification of APT activities These factor selection processes are important to ensure that the model is properly trained while maintaining high detection accuracy. Reducing the number of items helped simplify the machine learning process without compromising the model's ability to distinguish between normal and APT-related intermediate behaviors.

The core of the course is “model selection and training”. The machine learning model selected for the study is “eXtreme Gradient Boosting (XGBoost)”, a popular algorithm known for its accuracy and efficiency in classification tasks Optimization of XGBoost with specific hyperparameters such as a learning rate of 0.1,000. maximum depth 10, and 100 counters. The data were divided into training and testing sessions in an 80/20 ratio, ensuring that the model had enough information to learn from and accept its performance. The XGBoost model was trained to classify various types of network traffic, including normal traffic, inspection activity, basic contracts, segment movements, and data encryption, all of which are common actions seen in APT attacks.

The study focused on “systemic changes” to create a more sensitive and reliable detection system. This phase involves the integration of multiple machine learning frameworks in the integrated IDS framework. The combination of algorithms allowed to exploit the strengths of each of the systems, providing a comprehensive and flexible approach to APT detection The resulting IDS was designed to be dynamic, i. Strategies would also turn against continuously improving oversight.

An important part of the method is “empirical validation”. The system was tested using real-world network data to evaluate the applicability of the IDS system in the real world. This testing was necessary to validate the usefulness, reliability and efficiency of the system. The IDS was deployed on a variety of networks simulating real-world scenarios, allowing the researchers to evaluate its performance in detecting APTs on different networks This real-world validation helped ensure that the IDS was not effective at simulation not only inside but in actual cybersecurity operations It is also useful for deployment.

Table II shows the important parameters and parameters used in machine learning based intrusion detection system (IDS) for advanced persistent threat (APT) detection for performance and analysis with performance metrics such as data preprocessing, feature extraction , model specification, and detection accuracy and false positive rates s are included, which of the system Provides a comprehensive view of design and evaluation criteria.

TABLE II. KEY PARAMETERS AND METRICS FOR MACHINE LEARNING-BASED INTRUSION DETECTION SYSTEMS IN APT DETECTION

Parameter	**Details**
Data Collection	Real-world network traffic data, including both benign and malicious traffic. Data was preprocessed using Arcsight Moloch (Arkime).
Feature Extraction Tool	CICFlowmeter used to extract 83 features from network traffic.
Feature Selection Method	Analysis of Variance (ANOVA) performed to reduce 83 features to 12 critical features.
Machine Learning Model	eXtreme Gradient Boosting (XGBoost).
Hyperparameters	- Learning Rate: 0.1 - Maximum Depth: 10 - Number of Estimators: 100 - Training/Testing Split: 80%/20% - Batch Size: 10 samples
Traffic Categories	- Normal Traffic - Reconnaissance - Initial Compromise - Lateral Movement - Data Exfiltration
Framework Integration	Integration of multiple machine learning algorithms for robust and adaptive threat detection.
Validation Method	Empirical validation using real-world network data to test system practicality and reliability.
Performance Metrics	Detection accuracy, false positive rate, and computational efficiency.
Key Challenge Addressed	Balancing detection accuracy with false positive rates.

BEGIN

 # Step 1: Data Collection and Preprocessing
Collect real-world network traffic data (benign + malicious).
FOR each data sample:
Normalize and clean data to remove noise.
Store preprocessed data.

 # Step 2: Feature Extraction
Apply CICFlowmeter tool to extract 83 features from network traffic.

Store extracted features.

 # Step 3: Feature Selection
Apply ANOVA for feature selection.
Reduce 83 features to 12 significant features.
Store selected features.

 # Step 4: Model Selection and Training
Initialize the XGBoost model with parameters:
learning_rate = 0.1
max_depth = 10
n_estimators = 100
training/testing_split = 80/20
batch_size = 10 samples

Split data into training and testing sets.
Train the XGBoost model using the training set.
Validate the model using the testing set.

 # Step 5: Framework Integration
Combine multiple machine learning algorithms (including XGBoost) in a unified IDS framework.
Ensure the framework allows continuous updates for adapting to evolving APTs.

 # Step 6: Empirical Validation
Deploy the IDS framework in real-world network environments.
FOR each real-world scenario:
Test the system's detection accuracy and false positive rate.
Record results and evaluate system performance.

 # Step 7: Performance Assessment
Measure key performance metrics:
- Detection accuracy (%)
- False positive rate (%)
- Computational efficiency (time in seconds/minutes)

Optimize the system for balanced accuracy and low false positives.
IF performance is satisfactory:
Finalize the IDS framework.
ELSE:
Adjust parameters and retrain the model.

END

4. RESULT

Table III summarizes the main results of the study, focusing on the performance and features of machine learning based intrusion detection system (IDS) for detecting persistent threats (APTs) This still decreases from 83 to 12 features using ANOVA are revealed, optimizing the model without loss of accuracy. The system achieved a high “94.5% detection accuracy”, which demonstrated its effectiveness in detecting APT-related applications, and maintained a “3.2% low false positive rate”, important parameters such as “XGBoost model's hyperparameters”, training /test separation, calculation efficiency and others on the table are included as well, giving the system a balance between accuracy and real-world utility.

TABLE III. PERFORMANCE RESULTS AND KEY PARAMETERS OF MACHINE LEARNING-BASED INTRUSION DETECTION SYSTEMS IDS FOR APT DETECTION

Parameter	Measure	Description
Number of Features (Before Reduction)	Count	83 features extracted from network traffic using CICFlowmeter.
Number of Features (After Reduction)	Count	12 features selected after applying ANOVA for significant feature selection.
Detection Accuracy	94.5%	The percentage of correctly identified APT activities out of the total tested scenarios.

False Positive Rate	3.2%	The percentage of benign activities incorrectly flagged as threats.
Training/Testing Split	80%/20%	The proportion of data used for training (80%) and testing (20%) during the model training process.
Model Used	XGBoost	eXtreme Gradient Boosting model used for classification of network traffic.
Learning Rate	0.1 (dimensionless)	Controls the step size during model training, affecting how quickly the model adapts to the training data.
Maximum Depth of Model	10 levels	Maximum depth of the trees in the XGBoost model, controlling the complexity of the model.
Number of Estimators	100 estimators	The number of trees used in the XGBoost model to make predictions.
Batch Size	10 samples per batch	The number of data samples processed in one iteration during model training.
Computational Efficiency	~2 minutes per batch	The time taken to process and classify network traffic, including the training and testing process.
Real-World Validation Performance	High reliability across diverse environments	Empirical testing showed that the IDS performed well in various real-world network scenarios, maintaining both high accuracy and low false positive rates.

5. DISCUSSION

The development and implementation of machine learning based intrusion detection (IDS) systems for persistent threats (APTs) provides many important features and addresses key challenges in cybersecurity.

The IDS developed in this study, based primarily on the “eXtreme Gradient Boosting (XGBoost)” model, demonstrated impressive performance with “94.5% detection accuracy” and “3.2% false positive rate.” These results indicate that the model is more effective in identifying APT-related activities hold. In real-world cybersecurity scenarios, this balance between accuracy and false positives is important because a high number of false positives can overwhelm security teams, causing cognitive fatigue , and the possibility of ignoring real threats arises. The study's reduction method, using “ANOVA,” successfully combined the 83 factors into the 12 most important factors, without compromising the research process, thus providing order improved mathematical performance of the trainee. The XGBoost model, with a “learning rate of 0.1” and a “maximum depth of 10”, showed the best performance, balancing model complexity and training time using 100 calculations also contributed to model performance den, and allowed it to learn from a wide range of network behaviors including normal and malicious traffic.

The main challenge in identifying APTs is their stealth and changing nature. Traditional IDS systems often struggle to detect APTs because they rely on signature-based techniques or static anomaly detection techniques, which are insufficient to detect new threats that do not match the existing signature Machine learning approach used in this study IDS capable of learning both bad behaviors do address this limitation, making it adaptable to other evolving APT processes, techniques and processes (TTPs). Using real-world data for truth retrieval, the system demonstrated high reliability across networks. This empirical validation is important because APTs can manifest differently depending on network architecture, traffic patterns, and the specific tools and techniques used by attackers.

The extraction and selection process played an important role in the performance of the system. The original 83 factors were reduced to 12 significant factors using “ANOVA”, optimizing the model without sacrificing detection ability. This reduction not only improved the computational efficiency, but also reduced the system complexity required for real-time implementation. Technical cost can be a limiting factor in large networks, and the ability to accurately detect threats while minimizing resource consumption is a key advantage of this IDS. Furthermore, the “batch size of 10 samples” used in model training ensured that the system can handle data efficiently, making it suitable for real-time or near-real-time detection “Computation efficiency”, measured at “2 minutes per batch”., meaning the system is high- It can keep up with network traffic in volume, which is important for threat detection and timely response in dynamic network environments.

Despite its robust performance, the system has some inherent challenges. One of the key trade-offs in IDS-based machine learning is between “detection accuracy” and “false positive rate”. Although the system achieved a low false positive rate of 3.2%, even a small percentage of false positives can translate into a number of alerts in large networks, especially when processing millions of packets more processed each day This score other security tools, such as security reporting events. Emphasize the importance of continuous tuning and the ability to integrate with management (SIEM) systems to help filter out high-quality counterfeits. Another challenge lies in the “changing nature of APT”. While machine learning can adapt to new threats, it requires constant retraining and updating to be effective. APTs are highly adaptable, using new techniques that can bypass even the most sophisticated devices. The feature sets and model parameters will need to be updated regularly, as well as the acquisition of new data to ensure long-term performance. These activities can be resource-intensive and require complex strategies for continuous data collection, sample retraining, and reorganization.

The results of the study have important implications for the successful application of machine learning-based IDS for APT detection in real situations. The system’s ability to perform well in a variety of communication environments means it can be used in a variety of industries including government, finance, healthcare, and infrastructure but the effectiveness of an IDS will depend on data quality and its variety so greatly separate. Organizations with limited access to complete datasets may struggle to replicate program success, especially with highly specialized APTs targeting a specialized area or using non-generic methods the use of the. Furthermore, although computing efficiency is promising, organizations will need to ensure that their services can support IDS operational requirements, especially in large networks where large amounts of

data are important By integrating these IDSs, organizations can drive trade between detection better handle accuracy, false positives, and computational resources requirements.

This study lays the foundation for future research on machine learning based IDS for APT detection. One possible direction is to explore “cohort learning techniques” that combine multiple models to reduce false positives and further increase detection accuracy, with “unsupervised learning” and “anomaly detection” techniques together to address situations where labeled data is limited or unavailable, without relying on default attack models - Improves the ability of the system to detect attacks Another approach for future work is “. real-time optimization,” where the model dynamically updates itself based on new threat intelligence, reducing the need for manual retraining.

Funding:

The authors declare that no specific financial aid or sponsorship was received from governmental, private, or commercial entities to support this study. The research was solely financed by the authors' own contributions.

Conflicts of Interest:

The authors declare that there are no conflicts of interest in this study.

Acknowledgment:

The authors express their heartfelt appreciation to their institutions for the essential support and motivation provided throughout the research period.

References

[1] T. V. M. Reddy, B. Eswararao, and R. Reddy, "Advanced Persistent Threat (APT) detection using machine learning algorithms," *Procedia Comput. Sci.*, vol. 184, pp. 854-861, 2021.
[2] Y. L. Sun, B. Tan, and P. Thulasiraman, "Machine learning-based techniques for cybersecurity threats in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1454-1465, 2021.
[3] S. R. Sturgess and T. R. Bhalla, "Recent advances in APT detection techniques in cybersecurity," *Cybersecurity J.*, vol. 15, no. 2, pp. 105-118, 2022.
[4] "Xenoestrogens: mechanisms of action and detection methods," *Anal. Bioanal. Chem.*, vol. 378, pp. 582-587, 2004.
[5] N. Idris, M. Anwar, and M. Kamal, "APT countermeasures: A systematic review and future directions," *Comput. Sci. Rev.*, vol. 38, p. 100285, 2020.
[6] S. Li, F. Li, S. Tang, and W. Xiong, "A review of computer-aided heart sound detection techniques," *BioMed Res. Int.*, vol. 2020, Art. no. 5846191, Jan. 2020, doi: 10.1155/2020/5846191.
[7] W. Książek, M. Abdar, U. R. Acharya, and P. Pławiak, "A novel machine learning approach for early detection of hepatocellular carcinoma patients," *Cogn. Syst. Res.*, vol. 54, pp. 116-127, May 2019, doi: 10.1016/j.cogsys.2018.12.001.
[8] J. Smith and D. Wang, "The role of machine learning in APT detection," *J. Cybersecurity Res.*, vol. 13, no. 1, pp. 88-97, 2021.
[9] S. Al-Anisi, F. Khalid, and H. N. Tran, "Deep learning-based approaches to detect APTs," *IEEE Access*, vol. 8, pp. 178456-178465, 2020.
[10] M. Ahmed and S. A. Yousuf, "Cyber threat intelligence frameworks for APTs in cloud environments," *J. Cloud Secur.*, vol. 5, pp. 33-42, 2021.
[11] P. R. Sajwan and K. Mahesh, "A conceptual framework for APT detection in mobile devices," *Mobile Inf. Syst.*, vol. 2022, Art. ID 2073172, 2022.
[12] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, "Insider threat detection based on user behavior modeling and anomaly detection algorithms," *Appl. Sci.*, vol. 9, no. 19, p. 4018, Sep. 2019, doi: 10.3390/app9194018.
[13] R. A. Lam and A. S. Noor, "APT detection in software defined networks (SDNs) using deep learning," *J. Netw. Comput. Appl.*, vol. 188, p. 103448, 2021.
[14] D. Li and W. Zhang, "Survey of malware detection using deep learning approaches," *IEEE Access*, vol. 9, pp. 123456-123472, 2021.
[15] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Comput. Surv.*, vol. 54, no. 1, Art. no. 21, pp. 1-37, Mar. 2021, doi: 10.1145/3431233.
[16] J. V. Hernández and P. Silva, "Cyber warfare and APTs: Techniques, tools, and trends," *J. Strategic Cybersecurity*, vol. 15, no. 3, pp. 248-257, 2022.
[17] V. Atluri and J. Horne, "A machine learning based threat intelligence framework for industrial control system network traffic indicators of compromise," in *Proc. SoutheastCon 2021*, Atlanta, GA, USA, Mar. 2021, doi: 10.1109/SoutheastCon45413.2021.9401809.
[18] H. Tamaki and B. Le, "Community-based APT analysis in critical infrastructure networks," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, p. 100542, 2022.
[19] R. Thompson, M. Martinez, and E. Johnson, "Analyzing and classifying malicious code: Techniques for APT protection," *Appl. Sci.*, vol. 12, no. 6, p. 3027, 2022.
[20] J. David and M. Khan, "Deep packet inspection: Leveraging machine learning for efficient network security analysis," unpublished.
[21] D. B. da Silva, D. Schmidt, C. A. da Costa, R. da R. Righi, and B. Eskofier, "DeepSigns: A predictive model based on deep learning for the early detection of patient health deterioration," *Expert Syst. Appl.*, vol. 165, p. 113905, Mar. 2021, doi: 10.1016/j.eswa.2020.113905.
[22] S. Wong and C. K. Lim, "Detection of active eavesdropping in IoT networks using physical layer security," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3673-3681, 2022.
[23] D. Salazar, "Leveraging machine-learning to enhance network security," M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2018. [Online]. Available: https://hdl.handle.net/10945/59578.

[24] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 9, no. 3, p. e1306, Feb. 2019, doi: 10.1002/widm.1306.
[25] K. Park and T. Singh, "Anomaly detection techniques for APTs in cybersecurity," *Cybersecurity Data Prot. J.*, vol. 14, no. 1, pp. 78-89, 2021.