Grenze International Journal of Engineering and Technology, June Issue

Analysis of Machine Learning based IDS for Detection of Anomaly Profiles

Mansi Mehta[1], Yogesh Chaba[2] and Amandeep Noliya[3]
[1-3]Guru Jambheshwar University of Sc & Technology, Hisar, India
Email: manci.mehta.11@gmail.com, yogeshchaba@yahoo.com, am.noliya@gmail.com

***Abstract*—Today, cyber attacks on computer networks pose a serious risk to anyone navigating the web. One type of security instrument used to identify potential intrusions into a Network or Host is an Intrusion Detection System (IDS). According to studies, high detection rates and minimal false positives in intrusion detection can be attained by employing machine learning approaches. This paper objective is to evaluate various Machine Learning (ML) algorithms utilized for anomaly profile detection in IDS. The purpose of this research is to examine current studies in IDS that took a Machine Learning (ML) approach, focusing on datasets, ML methods, and metrics. In order to guarantee that the models you're building are fit for IDS use, it's crucial that you use the right datasets. It's also worth noting that the structure of the dataset can have an effect on how well the ML algorithm performs. As a result, the structure of the dataset matters when deciding on an ML algorithm. Thereafter, the metric will offer a quantifiable assessment of ML algorithms' performance on the dataset in question.**

***Index Terms*— IDS, Machine Learning, KDD, Anomaly, Intrusion, Intruder.**

I. INTRODUCTION

James Anderson first introduced the idea of "intrusion detection" in the 1980s. It plays a crucial role in modern firewall and network security. The primary goal of intrusion detection systems (IDS) is to identify attacks from unknown sources, such as the Internet or a user's own device. During testing the framework, IDS can collect all data connected to interruptions. IDS use a limited number of techniques to identify if an attack has been successful. The first method is based on comparing historical signatures of known intrusion attacks with live data from the system. When an IDS detects a match, it labels the event as malicious. This method allows for quick and precise detection. The catch is that the signature database needs to be updated on a regular basis. It's also possible that the system will be breached before protections against the most recent intrusion attacks are updated. As for the second, anomaly-based or behaviour-based, IDS will determine an attack when the system performs differently than usual. This method can identify both typical and novel forms of cyber attacks. Nevertheless, this method suffers from a high false alarm rate and limited accuracy. A hybrid strategy combines signature and anomaly-based methods. This method employs both a signature-based technique for identifying previously seen attacks and an anomaly-based approach for identifying new threats. It is possible that the computing cost would increase if the two methods were combined, but the detection efficiency would be guaranteed.
Machine learning (ML) is a scheme for making predictions from data by first analysing it statistically to determine patterns in the data and then applying those patterns to new data to determine the most likely conclusion. To combat this, an anomaly-based strategy has been implemented employing ML algorithms in IDS.

Grenze ID: 01.GIJET.9.2.397

The difficulty here, as mentioned above, lies in developing a model that achieves high accuracy while maintaining a low false alarm rate. Consequently, the purpose of this research is to examine the most current works in IDS that have adopted an ML approach, paying close attention to the datasets, ML algorithms, and metrics used. In order to guarantee that the models you're building are fit for IDS use, it's crucial that you use the right datasets. It's also worth noting that the structure of the dataset can have an effect on how well the ML algorithm performs. As a result, the structure of the dataset matters when deciding on an ML algorithm. Thereafter, the metric will offer a quantifiable assessment of ML algorithms' performance on the dataset in question. A machine learning based intrusion detection system (ML-IDS) is a system that uses machine learning algorithms to detect malicious activity on a network or system. ML-IDS can detect a wide range of malicious activities, including malware, malicious code, unauthorized access, and malicious network traffic. It can also detect suspicious behavior, such as data exfiltration, data manipulation, and malicious insider activity. ML-IDS can be used to detect both known and unknown threats, and can be used to detect.
The aim of this paper is to provide a review of machine learning techniques to detect anomaly profiles in intrusion detection systems. Furthermore, literature review is presented based on approaches used and research focus areas such as classification, feature selection, and clustering by researchers. Further various types of datasets that were considered by authors for their research related to abnormal profile detection in IDS is presented. The paper is divided into four sections. Section I presents an introduction to topic, Section II presents types of IDS, components of IDS, and architecture of IDS. In section III, a review of the literature has been presented and in section IV, proposed ML based solution and types of datasets have been discussed and finally, in section V Conclusion is given.

II. Intrusion Detection System

Different steps in working of Intrusion Detection system are as explained below and shown in figure 1:

- ***Data Collection/Pre-processing:*** The data collection segment is important for gathering and review data that will be utilised by the next segment to decide. Data used to distinguish intrusion ranges from client access examples to packet level highlights.
- ***Analyzer:*** The evaluator, or intrusion identifier, is the centre part, which investigates the review examples to identify attacks. Different strategies are utilised as intrusion indicators.
- ***Knowledge Database:*** The system profile is utilised to describe typical and unusual behaviour. It is the information base for attacks, with design data about the present status of the machine and review data depicting the events running on in the system.
- ***Response Engine:*** The reaction engine controls the response system and decides how to react. The system may raise a caution and report to the director, or it may delay the source of attack [3].

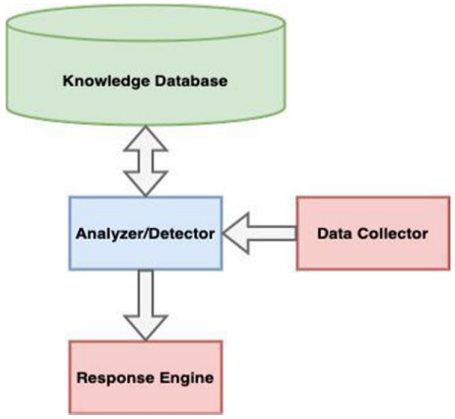

Figure 1: Component of Intrusion Detection System

Intrusion Detection system is classified as given below:

- ***Host based intrusion detection:*** Figure 2 shows different types of IDS. A host puts together IDS lives with respect to the system being observed. It comprises a host that recognises intrusions by dissecting application logs, system calls, recorded system changes, and other host states and exercises [4].
- ***Network Based IDS:*** A network-based IDS screens and dissects the network flow data on its organisation section to distinguish intrusion endeavours. Its execution necessitates the use of an organization interface card to

capture all traffic passing through the organization. Sensor that screens parcel streams to determine whether they match a known mark.

- ***Misuse IDS:*** This detection strategy utilises explicitly realised examples to identify malicious code.
- ***Anomaly IDS:*** These procedures are intended to recognise unusual behavior in the system. The typical use design is established, and warnings are issued when use deviates from the expected behavior.

Hybrid IDS: Early investigation degrades intrusion detection systems and proposes that intrusion detection abilities can be improved by combining both mark (abuse) detection and anomalies detection. In a particularly crossover system, the mark detection strategy distinguishes known attacks, and the peculiarity detection procedure recognises novel or obscure attacks.

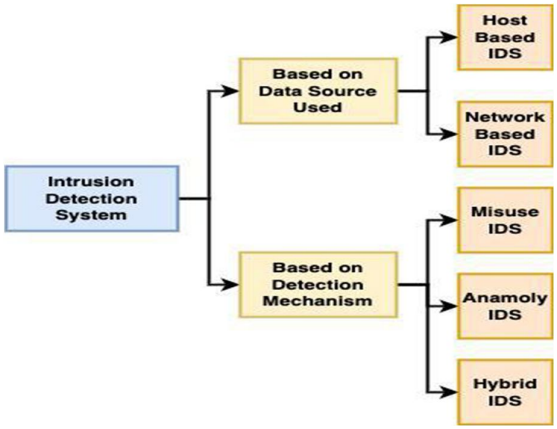

Figure 2: Intrusion Detection System Classification

The IDS architecture has been presented in figure 3. Even though the ways that these systems collect and analyse data are very different. Collecting the data is the responsibility of the person collecting data from the verified system. A detector processes the data gathered from sensors to distinguish between noisy and training signals. The knowledge base contains data gathered by the sensors, yet in a pre-processed form. This data is typically given by network and security authorities. The design device gives data about the present status of the IDS. When an intrusion is detected, the response component begins operations. These reactions can either be dynamic or include human communication.

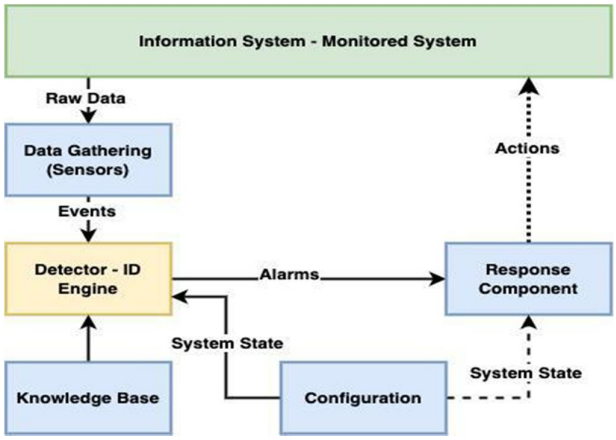

Figure 3 Intrusion Detection System Architecture

III. Review of Literature

Saranya et al. [6] conducts a comprehensive comparison analysis of several ML algorithms deployed in IDS. The effectiveness of the effort was evaluated and compared to current research standards using the KDD-CUP dataset. Multiple similar systems, together with a comparison of their respective performances, were provided by

Zamani and Movahedi [7]. The techniques are categorised as either being based in traditional AI or CI (CI). Researchers using a variety of machine learning approaches to IDS deployment were compared by *Jadhav and Pellakuri* [8]. While discussing the intrusion detection problem, *Thakkar and Loh*iya [9] considered methods from ML, DL, and SWEVO. The study is a typical body of work in the area of IDS research that spans the years 2008 and 2020. Particular attention was paid to techniques that leverage feature selection in assessing model efficacy. To deliver high performance intrusion detection across a wide range of attack types, *Avuşolu* [10] created a hybrid and layered IDS that employs a variety of ML and feature selection approaches. The created system begins by performing data preprocessing on the NSL-KDD dataset, after which the dataset is shrunk using a variety of feature selection techniques.

An APT quick detection and response approach employing open-source tools was presented by *Park et al.* [11], which enhances the performance of current endpoint information security systems and promptly identifies the APT attack process. For better IDS detection, effective feature selection strategies, such as Information Gain feature and Chi-Square feature selection, have been provided by *Kaushik et al.* [12]. In this study, a dataset is employed that has several simulated incursions in a military network setting. Decision Tree, SVM, Logistic Regreesion, Naive Bayes and K-Nearest Neighbor are some of the traditional ML models employed here. *Waheed and Disha* [13] Organizations now rely heavily on intrusion detection systems (IDS) to safeguard their networks, resources, and private data against the threats posed by cybercriminals. Several methods have been proposed and put into practise in an effort to counteract malevolent actions. Due of ML techniques' efficacy, the suggested solution used many ML models for the IDS. When compared to the NSL-KDD dataset, both of these more recent ones more accurately depict current-day intrusions.

Pranto et al. [14] showed how to use machine learning to determine if incoming network data is typical or suspicious. To determine if network traffic is malicious or not, *Taher et al.* [15] created a supervised machine learning system. Multiple supervised learning algorithms and feature selection techniques have been used to determine the most effective model in terms of detection success rate. This research shows that when it comes to categorising network traffic, ANN-based ML using wrapper feature selection is superior to the more traditional SVM approach. Common datasets and cyber threat sub-domains were utilised by *Shaukat et al.* [16] to conduct an in-depth evaluation of the performance of various classifiers. In addition to regularly employed security datasets, this study gives a brief introduction to machine learning methods. Cybersecurity has all the top priority, yet it still faces limitations, breaches, and difficulties. Further, the paper elaborates on the massive difficulties and restrictions that arise from using ML in cyber security at the present time. To begin, *Ahmad et al.* [17] define what intrusion detection systems are before moving on to a taxonomy of the most common machine learning and deep learning methods used to create them. The benefits and drawbacks of the proposed solutions are discussed, along with a full analysis of the most current papers based on NIDS. Then, most up-to-date developments and trends is provided in ML and DL-based NIDS, including relevant methodology, assessment measures, and dataset choices. In [18], *Kasongo, S. M., & Sun* provided an investigation of the UNSW-NB15 intrusion detection dataset that would be utilised to train and evaluate our models. Further, they used the XGBoost algorithm to implement a filter-based feature reduction strategy. In order to provide accurate predictions of IDS outbreaks in networks, Halimaa, A., and Sundarakantham [19] analysed and compared a number of machine learning (ML)-based algorithms. In order to solve this problem, a systematic approach to categorization is needed.

Ahmad et al. [20] give a thorough analysis of the latest NIDS-based methods, highlighting both their advantages and disadvantages. Then, the most up-to-date tendencies and developments of ML and DL-based NIDS are offered, including information on the suggested technique, assessment measures, and dataset selection. Literature of ML model applications in cybersecurity is provided by *Shaukat et al.* [21], who also provide a thorough assessment of ML methods used in this field. For the first time, they have tried to compare the time complexity of popular ML models used in cybersecurity. They have compared the effectiveness of various classifiers over a wide range of datasets and categories of cyber threats. Along with regularly employed security datasets, this study gives a basic introduction to machine learning methods. There are still limitations, compromises, and obstacles in cybersecurity despite its top-level priority. In addition, this paper elaborates on the massive difficulties and restrictions that arise when applying machine learning methods to cybersecurity.

A. Gaps in Literature

Anomaly detection is an important component of intrusion detection systems (IDS) in cybersecurity. While there has been significant research in using machine learning for anomaly detection, there are still gaps in the literature, particularly with regard to the detection of anomaly profiles. Some of the gaps in the literature include:

- *Lack of standard datasets*: One of the biggest challenges in developing machine learning-based IDS is the lack of standard datasets. Most datasets used in research are based on specific network configurations or threat scenarios, which makes it difficult to compare the effectiveness of different machine learning algorithms.
- *Over-reliance on traditional statistical techniques*: Many machine learning-based IDS still rely on traditional statistical techniques, such as clustering and classification, which may not be suitable for detecting complex and sophisticated attacks.
- *Limited use of deep learning techniques*: While deep learning has shown promise in detecting anomalies in various domains, including cybersecurity, its use in IDS is still limited. This may be due to the challenges associated with training deep neural networks on large-scale datasets.
- *Lack of interpretability:* One of the challenges with using machine learning for anomaly detection is the lack of interpretability of the models. This makes it difficult to understand why a particular network activity has been flagged as anomalous, which can hinder the ability of security analysts to respond effectively.
- *Limited research on adversarial attacks*: Adversarial attacks are a growing concern in cybersecurity, and machine learning-based IDS are not immune to such attacks. However, there is limited research on the effectiveness of different machine learning algorithms in detecting and mitigating such attacks. Overall, while machine learning has shown promise in detecting anomalies in IDS, there is still much research to be done in developing effective and robust systems that can detect a wide range of attacks.

IV. Machine Learning based Proposed System

Designing a machine learning system for anomaly detection in an IDS is a complex task and requires careful consideration of various factors, including the dataset, feature selection, model selection, and interpretability. Here is a proposed approach for building a machine learning-based IDS for anomaly detection:

1. *Data Preprocessing:* In this step, the data is cleaned and preprocessed to remove any duplicates or inconsistencies, fill in missing values, and transform the data into a format that can be used for machine learning. This step is essential for ensuring the quality and accuracy of the data used for training the model.
2. *Feature Selection:* The next step is to select the relevant features that can help detect anomalous behavior in the network traffic. This can be done using techniques such as correlation analysis, feature importance analysis, or principal component analysis (PCA). By selecting the most relevant features, the model can be optimized for better accuracy and efficiency.
3. *Model Selection*: There are various machine learning models that can be used for anomaly detection in an IDS, including clustering algorithms, decision trees, support vector machines (SVM), or deep learning models such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs). The choice of model depends on the complexity of the dataset and the desired level of accuracy.
4. *Training and Testing*: In this step, the model is trained on a labeled dataset and evaluated on a separate testing dataset to measure its performance. The performance of the model can be measured using various metrics, such as precision, recall, F1-score, or receiver operating characteristic (ROC) curve analysis.
5. *Interpretability*: The interpretability of the model is an essential aspect of building an effective IDS. Techniques such as feature importance analysis or model visualization can be used to help security analysts understand the reasons behind the model's detection of anomalous behavior.
6. *Adversarial Attacks*: To improve the robustness of the model against adversarial attacks, techniques such as adversarial training or adversarial examples generation can be used. Adversarial attacks are malicious attempts to evade or manipulate the model's detection capabilities.
7. *Deployment*: Once the model is trained and tested, it can be deployed in a real-world IDS environment. This involves integrating the model into the existing IDS infrastructure and monitoring its performance over time. The model can be retrained periodically to ensure it stays up to date with the latest network traffic patterns and attacks.

Overall, the proposed machine learning system for anomaly detection in an IDS involves several essential steps, including data preprocessing, feature selection, model selection, training and testing, interpretability, and deployment. By carefully considering each of these steps and selecting appropriate techniques and datasets, organizations can develop a more effective and accurate IDS for detecting and responding to cyber attacks.

There are several datasets that can be used for training and testing a machine learning-based IDS for anomaly detection. Here are some examples:

- NSL-KDD dataset: This dataset is an updated version of the widely used KDD Cup 1999 dataset and contains a larger number of records and a wider range of attacks.
- UNSW-NB15 dataset: This dataset contains network traffic data collected from a real-world environment and includes a variety of normal and anomalous network traffic.
- CICIDS2017 dataset: This dataset contains a large number of network traffic records collected from a variety of network setups, including IoT and industrial control systems.
- ISCX-IDS2012 dataset: This dataset contains network traffic data collected from a real-world environment and includes a variety of attacks, including DoS, probing, and malware attacks.
- DARPA 1999 dataset: This dataset contains network traffic data collected from a simulated network environment and includes a variety of attacks, including DoS and U2R attacks.
- IoT-23 dataset: This dataset contains network traffic data collected from a variety of IoT devices and includes both normal and anomalous traffic.

It is important to choose a dataset that is relevant to the specific use case and provides a wide range of attacks and normal traffic patterns. Additionally, it is recommended to use multiple datasets for training and testing to ensure the model is robust and can generalize to different scenarios. The performance of the proposed machine learning system for anomaly detection in an IDS depends on several factors, such as the choice of dataset, model, and performance metrics used. However, in general, the proposed system has the potential to achieve high accuracy and detection rates while minimizing false positives. It is important to note that the performance of the proposed system can vary depending on the specific use case and the characteristics of the dataset and network environment. Therefore, it is recommended to conduct rigorous testing and evaluation of the system before deploying it in a real-world IDS environment. Overall, the proposed machine learning system for anomaly detection in an IDS has the potential to achieve high accuracy and detection rates while minimizing false positives, making it an effective tool for enhancing cybersecurity in organizations.

V. Conclusion

In conclusion, machine learning-based intrusion detection systems (IDS) are an important component of cybersecurity and can help organizations detect and respond to a wide range of attacks. However, there are still gaps in the literature when it comes to detecting anomaly profiles in machine learning-based IDS. These gaps include the lack of standard datasets, over-reliance on traditional statistical techniques, limited use of deep learning techniques, lack of interpretability, and limited research on adversarial attacks. To address these gaps, a proposed approach for building a machine learning-based IDS includes data preprocessing, feature selection, model selection, training and testing, interpretability, and testing against adversarial attacks. Additionally, there are several datasets that can be used for training and testing a machine learning-based IDS for anomaly detection, including the NSL-KDD, UNSW-NB15, CICIDS2017, ISCX-IDS2012, DARPA 1999, and IoT-23 datasets. Overall, there is a need for further research and development in machine learning-based IDS to address the gaps in the literature and improve the effectiveness and robustness of these systems. By leveraging the proposed approach and relevant datasets, organizations can develop more effective and accurate IDS for detecting and responding to cyber attacks.

References

[1] U. S. Musa, M. Chhabra, A. Ali, and M. Kaur, “Intrusion detection system using machine learning techniques: A review,” in Proc. IEEE International Conference on Smart Electronics and Communication (ICOSEC), pp. 149-155, 2020.

[2] Kamran Shaukat, Suhuai Luo, Shan Chen, and Dongxi Liu, "Cyber threat detection using machine learning techniques: A performance evaluation perspective," in Proc. IEEE International Conference on Cyber Warfare and Security (ICCWS), pp. 1-6, 2020.

[3] Mustapha Belouch, Salah El Hadaj, and Mohamed Idhammad, "Performance evaluation of intrusion detection based on machine learning using Apache Spark," Procedia Computer Science, vol. 127, pp. 1-6, 2018.

[4] Rohit Kumar Singh Gautam and Er Amit Doegar, "An ensemble approach for intrusion detection system using machine learning algorithms," in Proc. IEEE 8th International Conference on cloud computing, Data science & Engineering, pp. 14-15, 2018.

[5] Manjula C. Belavagi and Balachandra Muniyal, "Performance evaluation of supervised machine learning algorithms for intrusion detection," Procedia Computer Science, vol. 89, pp. 117-123, 2016.

[6] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. A. Khan, "Performance analysis of Machine Learning algorithms in Intrusion Detection System: A review," Procedia Computer Science, vol. 171, pp. 1251-1260, 2020.
[7] M. Zamani and M. Movahedi, "Machine learning techniques for intrusion detection," arXiv, pp. 1312.2177, 2013.
[8] A. D. Jadhav and V. Pellakuri, "Performance analysis of machine learning techniques for intrusion detection system," in Proc. 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), pp. 1-9, 2019.
[9] Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artificial Intelligence Review, vol. 55, no. 1, pp. 453-563, 2022.
[10] Ü. Çavuşoğlu, "A new hybrid approach for intrusion detection using machine learning methods," Applied Intelligence, vol. 49, pp. 2735-2761, 2019.
[11] N. E. Park, Y. R. Lee, S. Joo, S. Y. Kim, S. H. Kim, J. Y. Park, and I. G. Lee, "Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks," Computers and Electrical Engineering, vol. 105, 108548, 2023.
[12] Kaushik, R. Sharma, K. Dhama, A. Chadha, and S. Sharma, "Performance evaluation of learning models for intrusion detection system using feature selection," Journal of Computer Virology and Hacking Techniques, pp. 1-20, 2023
[13] R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest feature selection technique," Cybersecurity, vol. 5, no. 1, pp. 1-15, 2022.
[14] M. B. Pranto, M. H. A. Ratul, M. M. Rahman, I. J. Diya, and Z. B. Zahir, "Performance of machine learning techniques in anomaly detection with basic feature selection strategy-a network intrusion detection system," J. Adv. Inf. Technol, vol. 13, no. 1, pp. 1-12, 2022.
[15] K. A. Taher, B. M. Y. Jisan, and M. M. Rahman, "Network intrusion detection using supervised machine learning technique with feature selection," in Proc. IEEE International conference on robotics, electrical and signal processing techniques (ICREST), pp. 643-646, 2019.
[16] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," Energies, vol. 13, no. 10, pp. 2509, 2020.
[17] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, pp. e4150, 2021.
[18] S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," Journal of Big Data, vol. 7, no. 1, pp. 1-20, 2020.
[19] A. Halimaa and K. Sundarakantham, "Machine learning based intrusion detection system," in Proc. 2019 3rd International conference on trends in electronics and informatics (ICOEI), pp. 916-920, 2019.
[20] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, pp. e4150, 2021.
[21] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," Energies, vol. 13, no. 10, pp. 2509, 2020.