Machine Learning Approaches for Intrusion Detection System in Network Security

Vikash[1], Suruchi[2]
[1]Student, Department of CSE, BRCM CET, Bahal, Bhiwani, Haryana, India
[2]Professor, Department of CSE, BRCM CET, Bahal, Bhiwani, Haryana, India
Corresponding Author: vikashpilania60@gmail.com

Abstract— **IDS: An Intrusion Detection System refers to software used to monitor the entire network or the traffic to detect any type of malicious or abnormal activities. IDS plays an essential role in safeguarding computer networks against harmful activity. Traditional rule-based IDS such as firewalls are based on the method of data filtering, which is not capable of detecting all types of attacks & often encounters difficulties in adapting to the rapidly growing nature of the cyber threats. As a result, there's been increasing interest in utilizing ML techniques to improve the functioning of the IDS. This ML-based detection system is used to detect the following 4 kinds of attacks in the network namely Pro, U2R (User to Root), R2L (Remote to Local), and Denial of Services. This study presents a novel ML strategy for IDS that makes use of a wide range of ML algorithms, like decision trees, k-Nearest Neighbors (KNN), SVMs, & naïve Bayes, etc. The proposed system extracts feature from the network traffic data and employs supervised ML techniques to classify instances as normal or malicious. Moreover, the system incorporates anomaly detection mechanisms to identify previously unseen attack patterns. We used the 'NSL-KDD Dataset' in that paper.**
The outcomes of the experiments show how well the suggested method works in precisely identifying different kinds of intrusions while reducing false positives and adhering to performance metrics like F1 score, Precision, Recall, and Accuracy to evaluate each model's performance. Overall, this research helps make IDS better at keeping networks safe from cyber threats by using ML.

***Index Terms*— Intrusion Detection System, Machine Learning, Datasets, feature selection.**

1. Introduction

IDS plays a crucial part in defending computer networks from malevolent activity and illegal access. Conventional rule-based IDSs frequently encounter difficulties in adapting to the rapidly evolving various types of cyber threat landscape. As a result, there is growing interest in using ML approaches to improve the efficacy of IDS. [1]

Manuscript revised May 09, 2024; accepted May 10, 2024. Date of publication May 12, 2024.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.59

ML algorithms provide the ability to automatically learn and adjust to novel attack patterns, rendering them highly suitable for intrusion detection tasks. A variety of ML methodologies, including supervised, unsupervised, and semi-supervised learning, have shown promising outcomes when applied to IDSs.[2]

Supervised learning algorithms leverage labeled data to differentiate between the normal and malicious instances, Decision Trees, SVM, & Random Forest are widely used Supervised ML methodologies.[3] while unsupervised techniques excel at detecting anomalies without relying on the labeled data.

Most popular algorithms K-means are used in the unsupervised machine learning methodology.[4] By using a smaller pool of labeled data and a larger pool of unlabeled data, semi-supervised learning incorporates the components of both supervised & unsupervised learning.[5] Despite the efficacy of ML approaches for intrusion detection, several challenges persist. These include the availability of labeled training data and the adaptability of models to emerging attack vectors.

In conclusion, machine learning presents promising opportunities for augmenting the capabilities of Intrusion Detection Systems by facilitating automated threat detection and response. However, careful attention must be paid to feature engineering, algorithm selection, & model evaluation to assure the reliability & efficacy of ML-based IDSs.

A. Need For Intrusion Detection System:

In today's world, the internet plays a significant role in our daily lives, especially for businesses. Many people use the internet every day for buying and selling things online. But, using the internet also comes with risks. It's like a two-sided coin for businesses: it helps them reach more customers, but it also exposes them to dangers. Businesses have to deal with both friendly internet users and bad ones. Despite companies' efforts to safeguard their data, vulnerabilities still exist that hackers can exploit. Therefore, companies must implement robust security measures to protect their information from internet threats, originating both externally and internally. some of the common types of attacks that are introduced using the Intrusion Detection System are as follows:

Denial of Services: These attacks aim to overwhelm a network service with an excessive number of requests, leading to the disruption of its availability.

User to Root: Unprivileged users try to gain unauthorized access to a system by exploiting vulnerabilities, thereby elevating their privileges.

Remote to Local: Attackers obtain illegal access to a local system through this kind of attack from a remote location, exploiting vulnerabilities in network services or protocols. Examples include password-guessing attacks and unauthorized access to services like FTP and Telnet.

Probing: Attackers do detective work to find out about a network or system they want to target, looking for weak spots. They might check which ports are open or map out the network to find where they can sneak in.

B. Types Of Intrusion Detection System

In the study, we address the following kinds of IDS:

1) Network Intrusion Detection System:

NIDS are strategically positioned across a network to keep an eye on all linked devices' traffic. They examine every subnet communication and compare it to a database of known attack patterns. Upon detecting suspicious activity or identifying an attack, NIDS promptly alerts the administrator.

2) Host Intrusion Detection System:

On specific hosts or devices inside a network, HIDS runs independently. They specifically oversee incoming and outgoing packets of the respective device, promptly notifying the administrator upon detecting any potentially malicious or suspicious activities. HIDS also periodically captures snapshots of the system files, contrasting them with previous versions. When changes are found in the system files, a notification is sent to the administrator right away.

3) Hybrid Intrusion Detection System:

It combines two or more ID techniques. The hybrid IDS outperforms conventional intrusion detection systems in comparison.

C. Methods Of the Intrusion Detection System

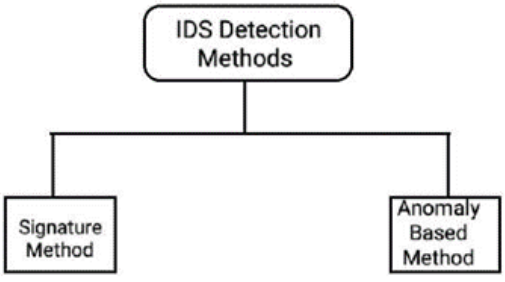

Fig.1. Methods of IDS

1) Signature-Based IDS:

By identifying particular patterns, such as byte counts, the frequency of 1s or 0s in network traffic, and known sequences of harmful instructions used by malware, signature-based IDS are able to identify attacks. We refer to these identifiable patterns as signatures. While signature-based IDS are excellent at identifying attacks that have pre-existing signatures, they struggle to identify novel malware attacks because they lack a known pattern or signature.

2) Anomaly Based IDS:

Because new malware is generated more quickly, it is utilized to detect unknown malware attacks on the network. An activity model is created with ML by anomaly-based IDS. Every new piece of data is checked against this model, and if any missing, it is reported as suspicious. Unlike signature-based IDS, this machine learning algorithm offers superior generalization as models can be tailored to specific applications.

2. Methodology

In this section, we shall talk about the research methodologies. The dataset used here is the NSL-KDD dataset after that it will be analyzed and trained using the following ML algorithms, SVMs, Random Forest, Naïve Bayes, etc.

The methodology used by ML for IDS typically involves several key steps:

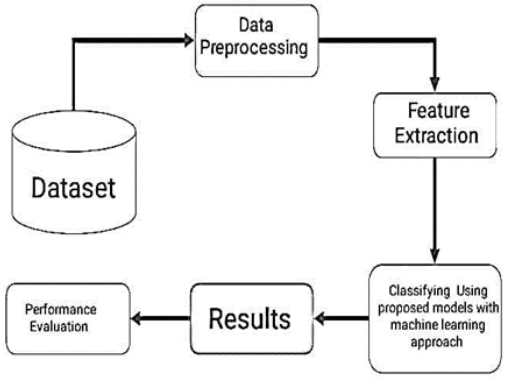

Fig.2. Data Reduction Process

- *Data Collection*: Gathering network traffic data, system logs, or other relevant information to use as input for the intrusion detection system.
- *Data Preprocessing*: In this step, the data is cleaned and prepared for analysis. This involves tasks such as removing noise or standardizing the data.
- *Feature Selection/Extraction*: Identifying and selecting relevant features. Feature extraction techniques may involve transforming raw data into more meaningful information suitable for machine learning algorithms.
- *Model Selection & Training*: Select a suitable ML model according to the data's properties. This stage uses supervised, unsupervised, or semi-supervised ML techniques to train the chosen models by dividing the preprocessed data into training & validation sets.
- *Model Evaluation*: Use evaluation metrics, including precision, accuracy, recall, F1-score, & ROC (receiver operating characteristic) curves, to assess how well the

trained models work. Analyze how well the model detects intrusions while reducing false alarms and how well it generalizes to data that has not yet been seen.

A. Dataset Used

We utilized the NSL-KDD dataset in this paper.[6] The most popular benchmark for assessing the effectiveness of the IDS is the NSL-KDD dataset. It is an improved dataset from the KDD Cup 1999. It has 41 features. This dataset is the collection of both normal and attack traffic data which enable the researcher to easily distinguish between the normal and malicious network activities. The NSL-KDD dataset addresses issues including imbalance, redundancy, and some unnecessary features, in contrast to the KDD Cup 1999 dataset.

The "NSL-KDD dataset consists of 39 attacks and each attack can be categorized into one of the four attacks including DoS, U2R, & R2L. [7]

Table.1.
Attack Classifications

Class	Attack Type
DOS	Apache2, Netpune, Pod, Land, Smurf, Mailbomb
PROBE	Satan, Saint, Ipsweep, Portsweep, Msan, Nmap
U2R	Buffer Overflow, Httptuneel, Rootkit, LoadModule, SQL Attack
R2L	WarezMaster Password, Imap, Spy", Xsnoop, Sendmail.

B. Performance Metrics

This paper will explore commonly utilized performance metrics for assessing the effectiveness of machine learning models, including:

1) Accuracy: This measure expresses the percentage of correctly identified samples relative to all "samples.[8]

$$A = \frac{TP + TN}{TP + FP + FN + TN}$$

2) Precision: The ratio of real positive forecasts to all positive predictions is measured by this statistic.[9]

$$P = \frac{TP}{TP + FP}$$

3) Recall: This represents the proportion of true positive predictions to total actual positive predictions. [10]

$$R = \frac{TP}{TP + FN}$$

4) F1 Score: This metric is the harmonic mean of precision" & recall.[11]

$$F = \frac{2 * P * R}{P + R}$$

5) False Positive Rate (FPR): FPR measures "the ratio of false positive predictions to the total actual negative instances in the dataset.[10]

$$FPR = \frac{FN}{TP + FN}$$

6) False Negative Rate (FNR): It quantifies the ratio of false negative predictions to the total actual positive instances in the dataset.[10]

$$FNR = TP + FP$$

In this context, TP represents True Positives, FP stands for False Positives, TN indicates True Negatives, and FN" signifies False Negatives.

3. Experimental Results

We have used the NSL-KDD datasets which consist of 42 features and contain different four varieties of attacks such as DoS, U2R, & R2L. 'NSL-KDD' datasets contain 125973 training instances and 22544 test instances and the distribution of each training and test dataset according to different attacks is given below:

Table.2.
NSL-KDD Dataset

Dataset	Class	Training Set	Test Set
NSL-KDD	Normal	67343	9711
	DOS	45926	7459
	Probe	11655	2422
	R2L	995	2754
	U2R	52	200

The experimental outcomes of the following Supervised ML algorithms are given below:

Table.3.
Results

Supervised Machine Learning				
Algorithm	Accuracy	Precision	Recall	F score
SVM	97.77%	87%	96.4%	89.3%
NB	95.33%	89.8%	95.8%	92.7%
Decision Tree	99.97%	99.38%	99.28%	99.21%
Random Forest	99.99%	99.78%	99.76%	99.68%
LR	98.4%	98.7%	97.4%	98%

4. Conclusion

From the above table, we can conclude that the Random Forest (RF) algorithm has the highest accuracy percentage which is 99.99 followed by the Decision Tree. In that paper, we applied various ML algorithms to detect various types of attacks

and we found that the RF has the highest accuracy among all the algorithms.

References

[1]. D. Z. Du and S. Y. Ko, "Intrusion Detection Systems in Machine Learning," International Journal of Computer Applications, vol. 180, no. 35, pp. 14-20, 2018.
[2]. M. N. Md. Nasir and M. N. M. Saad, "A Survey of Machine Learning Techniques for Intrusion Detection System," 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 2018, pp. 269-274.
[3]. K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, 2007.
[4]. A. L. M. dos Santos, J. B. Gomes, and R. S. de Moraes, "Machine Learning Applied to Network Intrusion Detection: A Survey," Computer Networks, vol. 151, pp. 58-76, 2019.
[5]. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), Ottawa, ON, Canada, 2009, pp. 1-6.
[6]. Almutairi, Y., Alhazmi, B., & Munshi, A. (2022)."Network Intrusion Detection Using Machine Learning Techniques". In Advances in Science and Technology Research Journal (Vol. 16, Issue 3, pp. 193–206). Wydawnictwo Naukowe Gabriel Borowski (WNGB).
[7]. Japkowicz, N., & Shah, M. (2011). "Evaluating learning algorithms: A classification perspective". Cambridge University Press.
[8]. Powers, D. M. (2011). "Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation". Journal of Machine Learning Technologies, 2(1), 37-63.
[9]. Fawcett, T. (2006). "An introduction to ROC analysis". Pattern Recognition Letters, 27(8), 861-874.
[10]. Davis, J., & Goadrich, M. (2006). "The relationship between Precision-Recall and ROC curves". Proceedings of the 23rd International Conference on Machine Learning (ICML), 233-240.