Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Vol:
Issue:
Pages:

Packet Analysis for Malicious Activity Detection Using Machine Learning

Aryan Dinesh Deshmukh[1*]

[1]Computer Engineering, Vishwakarma University, Pune, 411048, Maharashtra, India
*Corresponding Author: 202000584@vupune.ac.in

Article history: Received: xxxxxxxx, Revised:xxxxxxxx, Accepted: xxxxxxx, Published Online:xxxxxxxx

Abstract: This study investigates the detection of malicious and malformed network packets using supervised machine learning techniques. The research utilizes a subset of the UNSW-NB15 dataset to analyze network packet metadata. Key techniques such as k-nearest neighbors (kNN) and decision trees were implemented to differentiate between normal and malicious activities. The models achieved a classification accuracy exceeding 90%, highlighting their potential in enhancing cybersecurity defenses. This work underscores the necessity of continuous innovation in intrusion detection systems (IDS) to counteract evolving cyber threats.

Keywords: Malicious packet detection, machine learning, k-nearest neighbors, decision trees, cybersecurity, network security

1. Introduction:

In a time of constant technological progress, network system security has become a top priority for people, businesses, and governmental bodies. Data availability, confidentiality, and integrity are seriously threatened by the increasing complexity and frequency of cyberattacks. Novel and complex attacks are frequently difficult for conventional Network Intrusion Detection Systems (NIDS) to detect since they rely on established criteria and signatures. These constraints call for the creation of more intelligent and adaptable security solutions that can quickly detect and neutralize new threats. A viable substitute for improving intrusion detection capabilities is machine learning. Machine learning models can detect patterns suggestive of malicious activity by examining large volumes of network data. Using the UNSW-NB15 dataset, this study investigates the use of supervised machine learning techniques to differentiate between benign and malicious network packets. Important methods like decision trees and k-nearest neighbors (kNN) are used to create models that correctly categorize network activity. The project intends to expand the understanding and implementation of machine learning in network security using rigorous evaluation measures, such as accuracy, precision, recall, and F1-score. This will ultimately contribute to the development of more resilient and adaptable NIDS.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Vol:
Issue:
Pages:

2. Material and Methods:

The rise of cyber dangers in the modern digital age presents serious challenges to network security. In order to detect attacks, traditional Network Intrusion Detection Systems (NIDS) mostly rely on predefined rules and signatures. But given the dynamic nature of contemporary cyberattacks, more clever and adaptable strategies are required. The goal of this research is to improve NIDS by analyzing network packet metadata using supervised machine learning techniques. The initiative seeks to increase NIDS detection accuracy and responsiveness by finding patterns that distinguish between benign and malevolent activity.

The main source of data for this study is the UNSW-NB15 dataset, which was created by the Australian Centre for Cyber Security. It includes features that describe different aspects of network packets, including packet flow, protocol type, and service information. It is a comprehensive collection of network traffic statistics. For the purpose of assessing machine learning models in relation to network security, this dataset is ideal. To guarantee the accuracy and dependability of the dataset, data preparation is an essential stage. Duplicate record removal and missing value handling were part of the first data cleaning process. Major missing data records were discarded, and imputation techniques were used to fill in smaller gaps. Numerical data were imputed with the mean or median, where applicable, while categorical variables were imputed using the mode method.

Log transformations were used to alleviate the skewness in the distribution of several numerical features. By helping to normalize the data, this step improves its suitability for machine learning methods that depend on the assumption that input feature distributions are Gaussian. Outliers have a big impact on how well machine learning models work. To find and eliminate outliers from the dataset, statistical techniques such the Interquartile Range (IQR) and Z-score analysis were used. By doing this, it is made sure that the models are trained on representative data, which enhances their capacity for generalization. In order to improve model performance by lowering dimensionality and removing unnecessary features, feature selection is essential. The study employed mutual information analysis to evaluate the degree of dependence between the target variable and the features. Features with low mutual information scores were discarded, retaining those that contribute significantly to the classification task.

The k-Nearest Neighbors (kNN) algorithm, a non-parametric method used for classification, classifies a data point based on the majority class among its k-nearest neighbors in the feature space. The distance metric, typically is Euclidean distance, determines the neighbors. The value of k was optimized using cross-validation, balancing bias and variance to achieve optimal performance. Decision trees are intuitive and interpretable models that recursively split the feature space into regions with homogeneous class labels. The splits are determined based on criteria such as information gain. Pruning techniques were applied to prevent overfitting,

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Vol:
Issue:
Pages:

ensuring that the model generalizes well to unseen data.

The dataset was split into training and test set using an 80-20 split. The training set was used to build the models, while the test set evaluated their performance. Cross-validation was implemented using five folds to ensure robust model evaluation and to mitigate the risk of overfitting. Model performance was assessed using standard classification metrics: Accuracy, the ratio of correctly classified instances to the total instances; Precision, the ratio of true positive instances to the sum of true positive and false positive instances; Recall, the ratio of true positive instances to the sum of true positive and false negative instances; and F1-Score, the harmonic mean of precision and recall, providing a balance between the two metrics. The confusion matrix was used to gain deeper insights into the models' performance. It provides a detailed breakdown of true positive, false positive, true negative, and false negative predictions, allowing for the assessment of the models' ability to distinguish between normal and malicious packets accurately.

3. Results and Discussion:

Model Performance-

Decision tree models and k-nearest neighbors (kNN) models performed well at dividing network activity into groups that classified it as malicious or benign. The decision tree model has the highest accuracy of 92% on the test set after the models were thoroughly assessed using cross-validation to assure robustness. This high degree of accuracy highlights the models' capacity to identify complex patterns in the metadata of the network packets. Furthermore, the decision tree model demonstrated superior performance not only in overall accuracy but also in precision and recall, with values of 91% and 90%, respectively, according to the computation of precision, recall, and F1-score metrics. The confusion matrix study verified the decision tree model's dependability in further demonstrating the model's effectiveness by displaying a balanced distribution of true positives, true negatives, false positives, and false negatives in real-world scenarios.

Comparative Analysis-

Compared to the decision tree model, kNN performed wonderfully with an accuracy of 89%, but it was somewhat less successful in recall, suggesting a higher chance of missing harmful packets. The decision tree's interpretability offered further benefits, presenting cybersecurity experts with simple-to-understand and actionable choice pathways. This openness is essential for practical deployment in network security environments, as it helps refine and improve intrusion detection tactics by providing insight into a model's decision-making process. Moreover, the decision tree model demonstrated consistent performance across distinct dataset subsets, indicating that it has the potential to be generalized to other network contexts. These results highlight how crucial it is to use machine learning models that are suitable for the cybersecurity task at hand based on its particular requirements such as balancing accuracy, interpretability & robustness.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Vol:
Issue:
Pages:

4. Conclusion:

This study highlights how machine learning approaches may significantly improve cybersecurity defenses, especially when it comes to identifying fraudulent and malformed network packets. Using the UNSW-NB15 dataset, this study implemented and assessed decision tree and k-nearest neighbors (kNN) models, demonstrating great accuracy in differentiating between neutral and malevolent network activity. The decision tree model proved to be the most effective tool for this work because of its superior accuracy of 92% and interpretability. The results highlight the need for intrusion detection systems (IDS) to continuously innovate and adapt in order to stay up with changing cyberthreats. The effectiveness of these models indicates that machine learning can improve traditional rule-based NIDS considerably, offering a more responsive and flexible method of detecting and thwarting cyberattacks.

Subsequent investigations needs to be focused on enhancing these models even more, investigating novel machine learning methodologies, and verifying their suitability in actual settings. Further understanding of these models' applicability and effectiveness will come from testing them in real-world network scenarios and integrating them with current cybersecurity frameworks. Additionally, adding more modern and diverse data to the dataset will aid in the creation of more resilient and adaptable models that can fend off a wider variety of cyberthreats. In the end, this research provides a solid basis for the development of sophisticated, machine learning-driven intrusion detection systems (IDS) that can provide proactive and dynamic protection mechanisms in a world that is becoming increasingly digital.

References:

1. Australian Centre for Cyber Security. (2015). UNSW-NB15 dataset. Available at: https://research.unsw.edu.au/projects/unsw-nb15-dataset
2. GitHub Repository. (n.d.). Malformed random packet pcaps for some QA testing. Available at: https://github.com/pevma/mrp
3. Robbins, J. G. (n.d.). ML-Malicious-Packet-Detection. Available at: https://github.com/j-g-robbins/ML-Malicious-Packet-Detection
4. Huawei. (n.d.). Defense Against Malformed Packet Attacks - Configuration Guide - Security. Available at: https://www.huawei.com
5. Stack Overflow. (n.d.). "Malformed Packet: TNS" retrieving data from Oracle database. Available at: https://stackoverflow.com
6. Open Source for You. (n.d.). Cyber Attacks Explained: Packet Crafting. Available at: https://opensourceforu.com
7. Hewlett Packard Enterprise. (n.d.). Single-packet attacks. Available at: https://www.hpe.com