Grenze International Journal of Engineering and Technology, June Issue

Intrusion Detection System with Machine Learning Algorithms

Shaik Shoaib[1], Enamala Koushik[2] and K. Pradeep Mohan Kumar[3]
[1-3]SRM Institute of Science and Technologies, Department of Computing Technologies, Kattankulathur, 603203, Tamil Nadu, India
Email:ss2457@srmist.edu.in, {ek1020, pradeepk}@srmist.edu.in

***Abstract*— This research paper provides an explanation for IDS (Intrusion Detection System). The recent technological advancements have raised security and privacy concerns. As cyber networks and their applications expand, network security becomes increasingly important .Machine learning-based intrusion detection systems (IDS) are effective, particularly the Supervised Model, which increases detection rates. Complex models can make it difficult for people to understand their decisions. Currently, most research on model interpretation is focused on fields such as computer vision, natural language processing, and biology. In practice, cybersecurity experts struggle to optimize decisions based on model judgments. To address these concerns, a framework is suggested.**

***Index Terms*— Introduction, Literature Survey, Methodology, System architecture and Design , DataSet, Evaluation, Proposed System, Results and Discussion, Future Scope, Conclusion, References.**

I. INTRODUCTION

Cloud computing, 5G communication, and the Internet of Things (IoT) have driven rapid development. The number of physical devices connected to the Internet is expected to reach a trillion by 2022. However, recent technological advancements have raised security and privacy concerns. Cyberattacks are more likely to target Internet equipment due to its widespread distribution and open nature. Many Internet devices collect and process private information, making them a potential target for malicious attacks. Intrusion detection systems (IDSs) play a crucial role in ensuring network security. An IDS detects misuse, unauthorized use, and abuse within the host's network

Various approaches have been used to develop and evaluate IDSs in recent years. Some systems detect intrusions using shallow methods. Various classification algorithms, including Decision Tree, SVM,K-Nearest Neighbours, Bayes Classifier , have been used for intrusion detection tasks. Other systems use feature selection or ensemble classifiers to create intrusion detection models. Deep learning methods, including DNNs, CNNs, RNNs, and VAEs, are increasingly used in IDSs. These methods are highly accurate and have a low false positive rate when detecting attacks.

However, issues remain in the field of intrusion detection, particularly regarding system transparency .Cybersecurity experts typically make decisions based on. IDS. recommendations require understandable model predictions. Although the before mentioned models achieve impressive accuracies, their increasing complexity is a major drawback when humans are involved. This is due to the fact that DNNs are still used as black boxes and

Grenze ID: 01.GIJET.10.2.240

cannot provide reasons for decisions.
To detect such attacks, IDS will first train with all possible attack signatures originating from malicious user requests, and then generate a training model. When IDS receives a new request, it applies it to the train model to predict whether the request belongs to the normal or attack classes. To train and predict such models, various data mining classification or prediction algorithms will be used. In this paper, the author evaluates the performance of SVMs and ANN

II. Literature Survey

Title: "Cloud computing research: A review of themes, frameworks, methods, and future directions". This paper provides a meta-analysis of cloud computing research in information. Over a 7-year period, a literature review was conducted to assess research frameworks, methodology, geographical distribution, analysis level,
and trends. The existing cloud computing literature focuses on technological aspects, neglecting business, conceptualization, and application domains. Over the past seven years, there has been a steady increase in cloud computing studies. However, many of these studies lack theoretical frameworks and models. Most cloud computing studies used experimentation and simulation, rather than qualitative, quantitative, or mixed methods. This study adds to cloud computing research by providing Gain comprehensive insights into research themes, methodology, framework, geography, and future directions.
Title: " A survey of data mining and machine learning methods for cyber security, including intrusion detection". This survey paper describes a focused literature survey on machine learning (ML). We use data mining (DM)methods for cyber analytics to detect intrusions. Each ML/DM method is described briefly in a tutorial format. Papers on emerging methods were identified, read, and summarized based on their citation count or relevance. ML/DM relies heavily on data, so we've included descriptions of popular cyber data sets. This article discusses the complexity of ML/DM algorithms, challenges in using them for cyber security, and offers recommendations on when to use each method.
Title: " Hybrid ML models are increasingly used in anomaly-based IDS for improved performance and efficiency." Chi-square feature selection, with multi-class SVM model was introduced in. Statistical significance was calculated using Chi-square for each feature, and low-ranking features were removed. The number of features was reduced from 41 to 31 during the feature selection process. The RBF-kernel SVM hyperparameters were tuned to achieve the optimal combination of C and gamma values. Although the model produced excellent results, the authors did not evaluate it using KDD Test+. Yao et al introduced a hybrid multilevel data mining framework with hybrid feature selection. The authors conducted multiple experiments to select the optimal ML algorithms.
Bostani and Sheikhan proposed a graph-based machine learning framework using a modified Optimum-path Forest model (OPF). In the framework, the authors used K-Means to partition the original NSL-KDD dataset into K different training Subsets are used in the training of OPFs. To speed up the OPF stage, a pruning module used the concept of centrality and prestige in social network analysis to select the most predictive samples from subsets obtained through K-Means implementation.

III. Methodology

A. Data Analysis and Preprocessing

After compiling datasets from various sources. Dataset must be pre processed before training the model. Various methods can be used for data pre-processing. The process involves reading the collected dataset, followed by data cleaning. During data cleaning, some redundant attributes are removed from career prediction models. To improve accuracy, it is necessary to remove unwanted attributes and datasets with missing values, or replace them with nan values accuracy, we need to remove missing values or replace them with nan values.

B. Machine Learning Algorithm for Prediction

Machine learning predictive algorithms has highly optimized estimation has to be likely outcome based on trained data. Predictive analytics is the use of data statistical algorithms and machine learning techniques to identify the likelihood of future outcomes based on historical data. The goal is to go beyond knowing what has happened to providing a best assessment of what will happen in the future. In our system we used supervised machine learning algorithm having subcategories as classification and regression.

IV. System Architecture And Design

Network traffic includes inbound and outbound network packets, flows, and logs. System logs are generated by various network devices, servers, and applications.

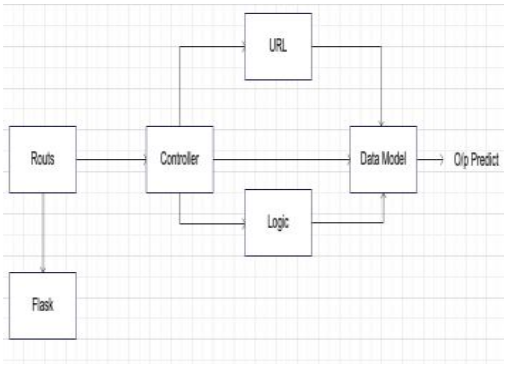

Figure 1. Architecture Diagram

A. Data Collection

Collect raw data from multiple sources Data Cleaning: Eliminate noise, missing values, and irrelevant features.

B. Feature Extraction

Obtain relevant features from raw data. This could include statistical data, frequency distributions, and so on.

C. Normalization/Scaling

Scale features to a standard range to ensure consistency. Feature Selection: Choose the features that are most relevant for training the machine learning model.

D. Machine Learning Models

Training Phase: Use labelled data to train the machine learning model. Common algorithms include decision trees, support vector machines, neural networks, and so on.

E. Testing and validation

To ensure generalizability, evaluate the model's performance using separate test data. Model Selection: Select the optimal machine learning algorithm based on performance metrics and requirements.

F. Model Selection

Select the optimal machine learning algorithm based on.

G. Intrusion Detection Engine

Real-time monitoring involves continuously monitoring incoming network traffic and system logs. Feature Extraction Obtain features from incoming data streams. Prediction Using the trained machine learning model, determine whether a given instance is normal or malicious.

V. DATA SET

The dataset is essential for training machine learning to detect anomalous threats. This study found that many researchers continue to use outdated methods. The NSL-KDD datasets, a variant of KDD00, have been criticized for being outdated and irrelevant to modern network infrastructure. This dataset, produced in 1999, is nearly 20 years old. New technologies like cloud computing, social media, and the Internet of Things are transforming network infrastructure. These changes are driving the evolution of threat attacks. As a result, some research findings are perceived as exaggerated, despite their high accuracy.

1. Upload NSL-KDD Data Set
2. Preprocess the Data Set

VI. EVALUATION

A. Support Vector Machine (SVM)

SVM is a popular supervised learning algorithm used for classification and regression. However, it is primarily used for classification problems in machine learning. The SVM algorithm aims to create a decision boundary that divides an n dimensional space into classes, making it easier to assign new data points to the appropriate category. The best decision boundary is known as a hyperplane.

B. Linear regression

Linear regression is a supervised machine learning model commonly used for forecasting. In supervised machine learning models, we use the training data is used to build the model, followed by testing its accuracy with the loss function. Linear regression is a well-known time series forecasting technique used for predictive modelling. The name implies a linear relationship between independent variables and the dependent variable (of interest).We're all familiar with the equation for the linear regression model, which is shown below.

$$y=mx+c$$

Where y is the dependent variable.
M represents the line's slope, X is the independent variable, and C is a constant

C. Decision Tree

Decision Tree is a tree-like structure made up of nodes representing decisions or choices based on data features (attributes). It recursively partitions the data into subsets based on the feature values, resulting in a tree structure with each internal node representing a "decision" based on a feature, each branch representing the outcome of that decision, and each leaf node representing the final prediction.

D. Random Forest

Random Forest is a powerful ensemble learning method that is commonly used for classification and regression tasks in machine learning. During training, it generates a large number of decision trees and outputs the class that represents the mode of the classes (classification) or the mean prediction (regression) of the individual trees. Here's an overview of the Random Forest classifier algorithm.

VII. Proposed System

A framework is proposed to provide an explanation for IDSs. This framework improves the interpretation of Intrusion Detection Systems (IDSs) by combining local and global explanations using SHapley Additive Explanations (SHAP). The regional justifications provide justifications for the model's decision-making processes regarding the given input. The global explanations outline the relationships between the feature values and various types of attacks, as well as provide the significant features extracted from IDSs. A comparison is made between the interpretations of two distinct classifiers, a one-versus-all classifier and a multiclass classifier. The NSL-KDD dataset is employed to evaluate the framework's viability. The framework introduced in this paper facilitates enhanced transparency of Intrusion Detection Systems (IDSs) and provides cybersecurity personnel with a more comprehensive comprehension of the assessments made by IDSs. Moreover, the divergent interpretations among various types of classifiers can assist security professionals in refining the architectures of intrusion detection systems (IDSs).

VIII. Results And Discussion

The project aimed to create a machine learning-based approach for intrusion detection systems. The implemented model achieved the highest validation accuracy of 97.188 %. The model's performance was evaluated using several metrics.

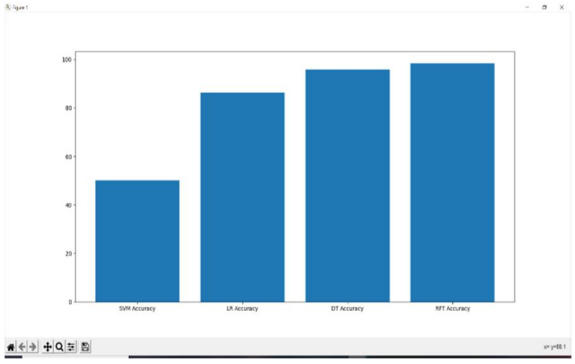

Figure 2. Accuracy Graph

IX. Future Scope

A. Enhanced Detection Accuracy

Further research into machine learning algorithms, such as deep learning and ensemble methods, can lead to higher detection accuracy for both known and unknown threats. Adversarial training is one technique that can help make models more resistant to evasion attacks.

B. Real-time Detection and Response

Efforts can be focused on developing IDS that can detect and respond to threats in real time, reducing the time between intrusion and mitigation. Integration with automated response mechanisms can result in rapid threat containment and mitigation.

C. Scalability and Efficiency

Scalable machine learning techniques and distributed computing frameworks can be investigated to deal with the growing volume and complexity of network traffic. This includes looking into lightweight models that are appropriate for resource-constrained environments like edge devices and IoT networks.

D. Integration with Security Ecosystem

IDS can be integrated with other security technologies and tools, such as firewalls, intrusion prevention systems (IPS), and Security Information and Event Management (SIEM) systems, to provide comprehensive threat detection and response capabilities.

X. Conclusion

This paper proposes a new framework for explaining both local and global phenomena. This method has solid theoretical foundation and can be applied to any model. This framework allows for interpretation of IDS predictions. The global explanation outlines key features, feature relationships, and attack types. The proposed framework's feasibility is verified using the NSL-KDD dataset.

Our framework's interpretation results align with the characteristics of specific attacks, providing intuitive results. This paper compares the one-vs-all and multiclass classifiers and discusses their explanations. This can benefit network security personnel. Select the appropriate structure when designing an intrusion detection system.

References

[1] Aljabri, M.; Altamimi, H.S.; Albelali, S.A.; Maimunah, A.H.;Alhuraib, H.T.; Alotaibi, N.K.; Alahmadi, A.A.; Alhaidari, F.; Mohammad, R.M.A.; Salah, K. Detecting URLs using machine learning techniques: Review and research directions. IEEE Access 2022

[2] Liu, J.; Dong, Y.; Zha, L.; Tian, E.; Xie, X. Event-based security tracking control for networked control systems against stochastic cyber-attacks. Inf. Sci. 2022

[3] Zha, L.; Liao, R.; Liu, J.; Xie, X.; Tian, E.; Cao, J. Dynamic event-triggered output feedback control networked systems subject to multiple cyber attacks. IEEE Trans. Cybern. 2021

[4] Zheng, Q.; Zhao, P.; Wang, H.; Elhanashi, A.; Saponara, S. Fine-grained modulation classification using multi-scale radio transformer with dual-channel representation. IEEE 2022

[5] Elhanashi, A.; Gasmi, K.; Begni, A.; Dini, P.; Zheng, Q.; Saponara, S. Machine Learning Techniques for Anomaly-Based Detection System on CSE-CIC-IDS2018 Dataset. In Applications in Electronics Pervading Industry, Environment and Society: APPLEPIES 2022; Springer: Berlin/Heidelberg, Germany, 2023

[6] Liu, L.; Wang, P.; Lin, J.; Liu, L. Intrusion detection of imbalanced network traffic based on machine and and deep learning. IEEE Access 2020

[7] Solani, S.; Jadav, N.K. A Novel Approach to Reduce False Negative Alarm Rate in Network-Based Intrusion Detection System Using Linear Discriminant Analysis. In Inventive Communication and Computational Technologies; Springer: Berlin/Heidelberg, Germany, 2021

[8] Dini, P.; Begni, A.; Ciavarella, S.; De Paoli, E.; Fiorelli, G.; Silvestro, C.; Saponara, S. Design and Testing Novel One-Class Classifier Based on Polynomial Interpolation With Application to Networking Security. IEEE Access 2022

[9] Moualla, S.; Khorzom, K.; Jafar, A. Improving the performance of machine learning-based network intrusion detection systems on the UNSW-NB15 dataset. Comput. Intell. Neurosci. 2021

[10] Lopez-Martin, M.; Sanchez-Esguevillas, A.; Arribas, J.I.; Carro, B. Contrastive Learning Over Random Fourier Features for IoT Network Intrusion Detection. IEEE Internet Things J. 2023