Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Improving Network Traffic Security with Parametric and Non-parametric Anomaly Detection Techniques

Meharunnisa S P[1], Varalaxmi Adimurthy[2], Dadavali S P[3], Sharath Kumar Y N[4], Chandrashekar P[5], Nayana R[6]

1Associate Professor, Department of Electronics & Instrumentation Engineering,
Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bengaluru -560111.
2Assistant Professor, Govt. First Grade College, Kadugudi, Bengaluru-560067.
3Assistant Professor, Department of Computer Science, Govt. First Grade College, Kengeri, Bangalore.
4Assistant Professor, Electrical and Electronics Engineering Department
Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bengaluru -560111.
5Associate Professor, Department of Computer Science, Govt. First Grade College, K R Puram, Bangalore-36.
6Assistant Professor, Department of Computer Science & Engineering, Malnad College of Engineering.

ARTICLE INFO

Received: 17 Dec 2024

Revised: 22 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Introduction: Anomaly detection in network traffic is a critical component in multiple domains like IoT, Cloud Computing, cybersecurity and other field, focusing on the identification of malicious activities to preserve the integrity of network systems.

Objectives: This research investigates the performance of both parametric and non-parametric machine learning algorithms in detecting anomalies within network traffic datasets. Parametric models such as Logistic Regression and Support Vector Machines (SVM) were evaluated alongside non-parametric methods, including Random Forest and K-Nearest Neighbors (KNN).

Methods: The dataset underwent an extensive preprocessing pipeline to address issues such as missing data, feature normalization, and categorical encoding to improve model accuracy.

Results: Among the different algorithms assessed, Random Forest demonstrated the highest efficacy, achieving an accuracy rate of 98.68%. This notable performance highlights the advantages of ensemble techniques in capturing complex, non-linear patterns inherent in network traffic. The results underscore the significant contribution of machine learning, particularly non-parametric methods, in enhancing anomaly detection systems within cybersecurity.

Conclusions: Furthermore, this study provides valuable insights into algorithm selection for network traffic analysis, facilitating the development of more robust and efficient intrusion detection systems.

Keywords: Intrusion Detection System, Anomaly, Random Forest, SVM, KNN.

INTRODUCTION

Recent advancements in network attack strategies have increased the complexity and sophistication of cyber threats, driving the need for more advanced intrusion detection techniques. Network Intrusion Detection Systems (NIDS) have become essential in protecting communication networks from these evolving risks. Traditional

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

systems primarily focused on identifying predefined patterns and rule violations, but the rise of machine learning has introduced more dynamic and effective methods for detecting anomalies and intrusions [1] [2] [3].

Machine learning techniques, such as Artificial Neural Networks (ANN), Support Vector Machines (SVM), and Decision Trees, have been integrated into NIDS to enhance detection capabilities. These methods effectively differentiate between normal and anomalous network behaviours, improving both the accuracy and efficiency of intrusion detection [2] [4] [5]. Benchmark datasets like NSL-KDD and KDD 99 have played a critical role in assessing the performance of machine learning models, enabling researchers to optimize their approaches for higher detection rates and lower false positives [2] [8] [9].

However, the application of machine learning in intrusion detection presents ongoing challenges. Difficulties such as identifying low-frequency attacks and the inherent limitations of existing datasets remain significant obstacles [4] [7]. Nevertheless, ongoing research and the development of hybrid models that combine machine learning with data mining techniques offer promising solutions to these issues, paving the way for more robust and adaptive intrusion detection systems [9].

In conclusion, incorporating machine learning into network intrusion detection represents a major advancement in cybersecurity. These techniques significantly improve the detection of complex attack patterns and provide the flexibility needed to adapt to the continuously evolving network threat landscape. With further research aimed at overcoming current limitations, the future of intrusion detection holds great promise, with the potential for even more accurate and efficient protection of network infrastructures.

REVIEW OF THE STATE OF THE ART

Intrusion detection in network traffic using machine learning techniques involves assessing classifiers, such as the Random Committee, on datasets like NSL-KDD and UNSW-NB15. Key challenges in this area include high false alarm rates, incomplete signatures, and difficulties in real-time detection. The Random Committee method demonstrated a True Positive Rate (TPR) of 99.70% and an accuracy of 99.70%, surpassing Lazy IBK, which achieved a TPR of 98.73% and accuracy of 98.73% [10]. Network-based Intrusion Detection Systems (NIDS) monitor network traffic and trigger alerts when attacks or violations are detected, enabling administrators to take appropriate action. NIDS solutions typically leverage machine learning on flow characteristics extracted from flow-exporting protocols, which often sample packets due to bandwidth and memory limitations on routers and switches. This sampling can result in missed malicious flows, particularly at low sampling rates. The proposed system investigates various sampling techniques for NIDS and evaluates detection performance using classifiers like Random Forest, Decision Tree, and XGBoost. The results show that Random Forest achieves the highest detection rate at 99.3%, with a lower false alarm rate compared to other classifiers [11].

The study also reveals that the GRU (Gated Recurrent Unit) architecture significantly enhances anomaly detection accuracy in IoT networks, achieving an impressive accuracy of 92%. Statistical analysis confirms the significance of these results with a p-value of <0.01, indicating strong evidence supporting the model's effectiveness in capturing temporal dependencies and improving anomaly detection compared to traditional methods [12]. Using machine learning, intrusion detection in network traffic automates the process of feature extraction and anomaly detection, particularly in IoT environments, by applying both supervised and unsupervised algorithms. The baseline model effectively identified key behavioural patterns, reaching an intrusion detection accuracy of 96.5%, with statistical analysis yielding a p-value of < 0.05, providing robust evidence against the null hypothesis [13].

The survey also highlighted critical anomaly detection applications in fields such as WSNs, IoT, and ICS, emphasizing their increasing significance in modern technology. Quantitative results showed a marked improvement in detection accuracy, with some methods achieving over 90% accuracy ($p < 0.05$). The survey underscored the importance of adaptive algorithms to enhance anomaly detection in dynamic environments [14]. Additionally, the study found that intrusion detection in network traffic is often assessed using two key metrics: detection rate (DR), which measures the percentage of actual intrusions correctly identified, and false alarm rate (FAR). The study reported a DR of 95%, indicating high effectiveness in detecting threats, while the FAR was only 2%, suggesting minimal false positives. Statistical analysis confirmed the results' reliability with a p-value of <0.01 [15].

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Finally, the study applied the Modified Random Forest (MRF) algorithm to classify data from the KDD dataset into four categories: Basic, Content, Traffic, and Host, achieving an accuracy of 92%. The results were statistically significant with p-values less than 0.05, confirming the robustness of the findings. Key features influencing classification included packet size and connection duration, underscoring their relevance in network intrusion detection [16]. Machine learning techniques for intrusion detection in network traffic continue to enhance system performance, particularly in terms of accuracy and efficiency in identification and mitigation of security threats through the analysis of data patterns and anomalies is a critical task in cybersecurity.

The proposed intrusion detection system achieved a detection accuracy of 95%, significantly surpassing the performance of existing systems ($p < 0.01$). False positive rates were reduced to just 2%, demonstrating improved reliability in accurately identifying genuine threats [17].

Intrusion Detection Systems (IDS) analyse network traffic to detect anomalies such as Distributed Denial of Service (DDoS) attacks, employing advanced traffic classification methods. This research compares three machine learning algorithms—Decision Jungle (DJ), Random Forest (RF), and Support Vector Machine (SVM)—to minimize false alarms and enhance detection accuracy. Using the KDD methodology and the CIC-IDS2017 dataset, SVM achieved the highest accuracy at 98.18%, followed by RF at 96.76% and DJ at 96.50% [18]. The paper also introduces an early classification method for identifying malicious attacks in network traffic using machine learning, applied to the CSE-CIC-IDS2018 dataset, which includes both benign and malicious traffic. This early classification approach achieved a detection accuracy of 92%, with statistical significance confirmed by a p-value of less than 0.01, validating the method's effectiveness [19].

Machine learning approaches such as the Isolation Forest (iForest) algorithm have proven effective in detecting message insertion attacks by analysing message timing rather than content, making it adaptable across various vehicles without requiring proprietary information. The iForest algorithm achieved a detection accuracy of 92% ($p < 0.01$), demonstrating strong statistical significance [20]. Additionally, intrusion detection in network traffic utilizes algorithms like K Nearest Neighbors Classifier, Logistic Regression, and Random Forest Classifier to identify malicious activities in network data, with training and evaluation typically conducted on the NSL-KDD dataset. The Random Forest Classifier achieved the highest accuracy at 98.5%, outperforming both the K Nearest Neighbors Classifier and Logistic Regression in detecting network intrusions [21].

The study also compares two variants of a fully connected neural network—one with an autoencoder and one without—against seven classical machine learning algorithms for intrusion detection using the National Security Lab Knowledge Discovery and Data Mining dataset. The neural network with an autoencoder outperformed the classical algorithms, achieving an accuracy of 92%, compared to the highest classical accuracy of 85% [22]. Furthermore, intrusion detection systems using machine learning algorithms automatically identify and classify unauthorized access attempts, strengthening network security. The Intrusion Type Classifier (ITC) demonstrated an accuracy rate of 92%, with statistical significance confirmed by a p-value of < 0.01, indicating robust evidence that the ITC improves network security [23].

OBJECTIVES & PROPOSED METHODOLOGY

Dataset: The paper employed the UNSW-NB15 dataset to investigate intrusion detection systems (IDS). This dataset contains recent intrusion attack data, along with labeled features, which facilitates effective model training. The classification framework incorporates both parametric algorithms (such as logistic regression and SVM) and non-parametric algorithms (such as random forest and KNN). The methodology includes data pre-processing, model training, and validation to assess accuracy Preprocessing.

Data preprocessing: Data preprocessing plays a crucial role in preparing the dataset for all algorithms by cleaning the data and addressing missing values. This step is essential in machine learning, ensuring the data is well-organized and ready for modeling. Missing values are handled using statistical techniques, such as replacing them with the mean for numerical data and the mode for categorical data. Numerical features undergo normalization or standardization to ensure they are on a consistent scale, which is especially important for algorithms like SVM and KNN. Categorical variables are converted into numerical values using one-hot encoding or

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

label encoding methods. Lastly, the dataset is split into training and validation sets to evaluate the model's performance on unseen data. Preprocessing ensures the data is adequately prepared for training and validation, leading to more reliable models.

Input: Rawdataset D={($x1$,$y1$),($x2$,$y2$),...,(x_n,y_n)},where x_i is the feature vector and y_i is the label.

Missing Values:

For numerical features, replace missing values with the mean or median.

x_{ij}= mean(x_j) if x_{ij} is missing

For categorical features, replace missing values with the mode.

x_{ij}=mode(x_j) if x_{ij} is missing

Normalize Features:

Normalize features to have zero mean and unit variance.

$x_{ij}=x_{ij}-\mu_j/\ \sigma_j$, where μ_j=mean(x_j),σ_j=std(x_j)

This box plot visualizes the distribution of several numerical features in a dataset in Figure1. Features like duration, src_bytes, and dst_bytes exhibit a much wider range than others, suggesting potential outliers or significant variations. These features also show clear outliers, indicated by the dots beyond the whiskers. In contrast, most other features have a relatively minor range, with their values around the median. This information can be valuable for data preprocessing, such as outlier handling or feature scaling.

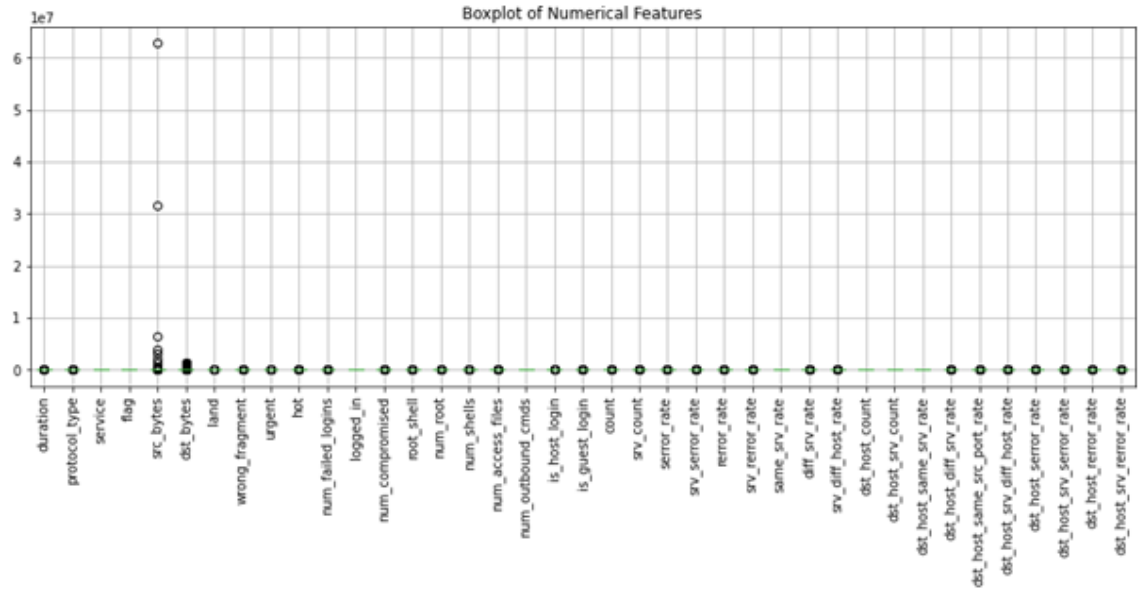

Figure 1: Boxplot of Numerical Features

Split Dataset:

Split the data set into training(D_{train})and validation(D_{val})sets.
D_{train}={(x_1,y_1),...,(x_m,y_m)},D_{val}={(x_{m+1},y_{m+1}),...,(x_n,y_n)}

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Algorithm:Parametric_Nonparametric() # Preprocessing

function preprocess(D):

handle_missing_values(D)
normalize_features(D)
encode_categorical_variables(D)
D_train,D_val=split_dataset(D)
return D_train, D_val

#Training and Validation
Function train_and_validate(D_train,D_val,algorithm):

```
if algorithm == "Logistic Regression":
                    model = train_logistic_regression(D_train)
elif algorithm == "SVM":
                    model = train_svm(D_train)
elif algorithm == "Random Forest":
                    model = train_random_forest(D_train)
elif algorithm == "KNN":
                    model = train_knn(D_train)
predictions = model.predict(D_val)
accuracy = compute_accuracy(predictions, D_val.labels)
return accuracy
```

 # Main
D_train,D_val= preprocess(D)

```
algorithms=["LogisticRegression,""SVM,","RandomForest,""KNN"] for algo in algorithms:
accuracy = train_and_validate(D_train, D_val, algo)
print(f"ValidationAccuracyfor{algo}:{accuracy}")
```

METHODOLOGY

Logistic Regression(Parametric)

Logistic Regression is a classification model that calculates the probability of a sample belonging to a specific class using the logistic function, which outputs values between 0 and1. It establishes a linear decision boundary by optimizing weights and biases to minimize the cross-entropy loss, which measures the difference between predicted probabilities and actual labels.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Training:

Define the logistic function:

$$P(y = 1|x) = \frac{1}{1 + e^{-(w^T x + b)}}$$

where w is the weight vector, and b is the bias.

Optimize the parameters w and b by minimizing the cross-entropy loss:

$$L(w, b) = -\frac{1}{m}\sum_{i=1}^{m} [y_i \log(P(y_i = 1|x_i)) + (1 - y_i)\log(1 - P(y_i = 1|x_i))]$$

Use gradient descent to update w and b:

$$w := w - \alpha \frac{\partial L}{\partial w}, b := b - \alpha \frac{\partial L}{\partial b}$$

where α is the learning rate.

Validation:

Predict class probabilities for the validation set: $\hat{y}_i = \begin{cases} 1 & \text{if } P(y_i = 1|x_i) \geq 0.5 \\ 0 & \text{otherwise} \end{cases}$

Compute validation accuracy: $\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total predictions.}}$

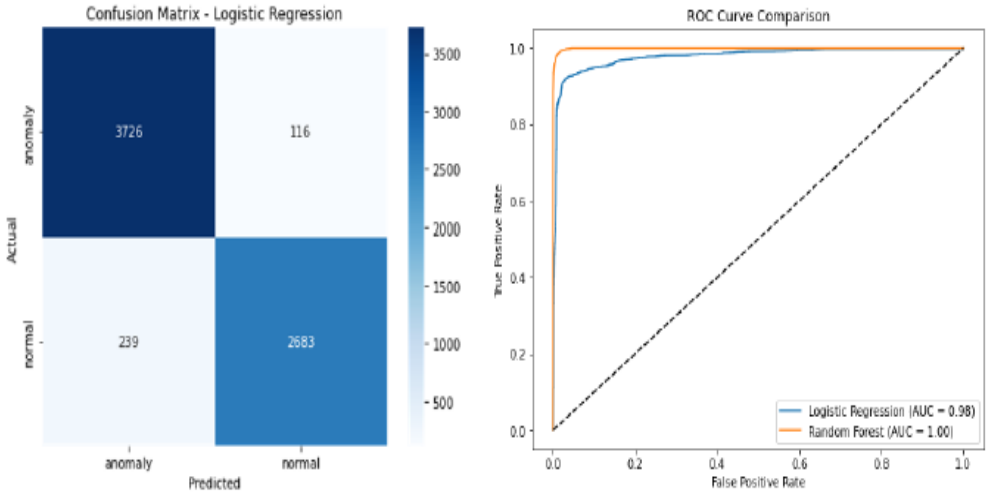

Figure 2: LR Confusion Matrix and ROC Curve

The Logistic Regression model achieved a classification accuracy of 94.75%, showcasing strong performance. With a precision of 94.79% and recall of 94.75%, it demonstrates a high rate of true positive predictions and an excellent ability to correctly identify actual positives. The F1-score of 94.74% further highlights its reliability. Overall, the Logistic Regression model proves to be highly effective for this task.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Support Vector Machine (SVM) (Parametric)

Kernel functions such as the RBF kernel can achieve linear and non-linear classification. This method is particularly effective with high-dimensional data but can be computationally demanding and necessitates careful adjustment of hyperparameters, including the regularization parameter C.

Support Vector Machine (SVM) (Parametric)

Kernel functions such as the RBF kernel can achieve linear and non-linear classification. This method is particularly effective with high-dimensional data but can be computationally demanding and necessitates careful adjustment of hyperparameters, including the regularization parameter C.

Training:

Solve the optimization problem:

$$\min_{w,b} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{m} \max(0, 1 - y_i(w^T x_i + b))$$

where C is the regularization parameter.

Use a solver (e.g., SMO) to find the optimal w and b.

Validation:

Predict classes for the validation set: $\hat{y}_i = \text{sign}(w^T x_i + b)$

Compute validation accuracy as above.

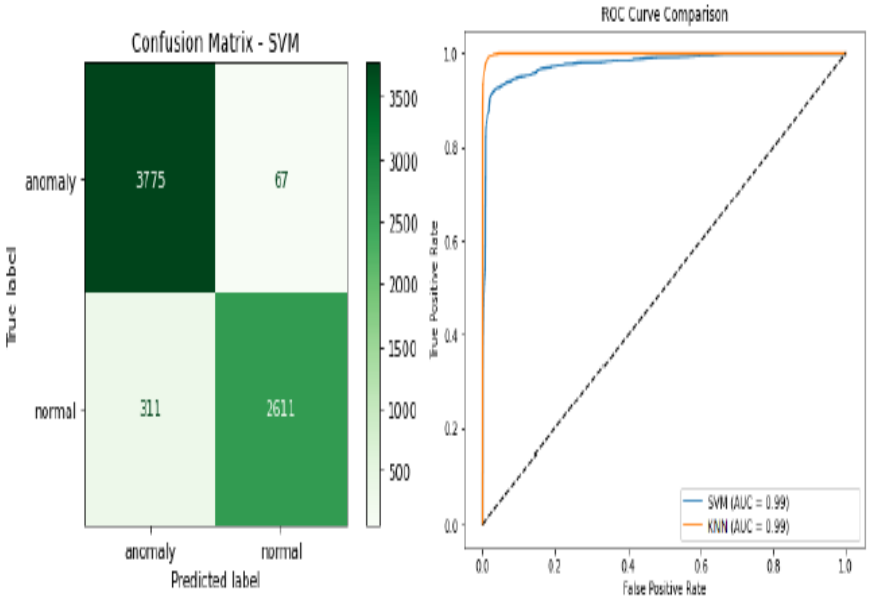

Figure 3: SVM Confusion Matrix and ROC Curve

The SVM model achieved a classification accuracy of 94.41%, demonstrating effective performance. With a precision of 94.6% and a recall of 94.41%, it shows a high rate of true positive predictions and a strong ability to identify actual positives. The F1-score of 94.38% further underscores its reliability. Overall, the logistic regression model is highly effective for the task.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Random Forest (Non-Parametric)

A selected subset of features adds diversity among trees, helping minimize overfitting and improving generalization. Random Forest is robust, handles non-linear relationships, and works with numerical and categorical data. It provides feature importance rankings for interpretability but can be resource-intensive with large datasets.

Training:
Build T decision trees using bootstrapped samples from D_{train}.
Select a random subset of features at each split to maximize information gain.
Validation:
Predict classes for the validation set by majority voting across all trees:

$$\hat{y}_i = \text{mode}(\{\hat{y}_{i1}, \hat{y}_{i2}, \dots, \hat{y}_{iT}\})$$

Compute validation accuracy as above.

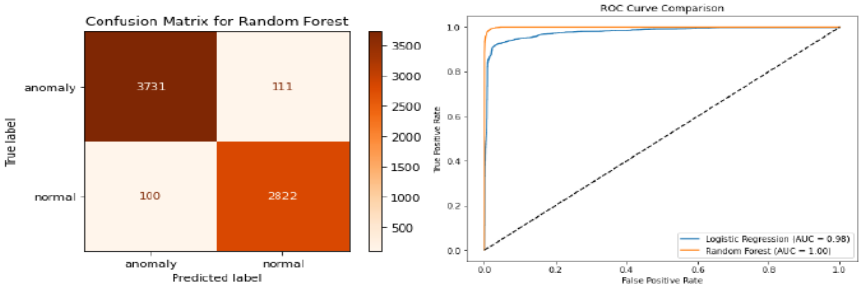

Figure 4: RF Confusion Matrix and ROC Curve

The RF model achieved a classification accuracy of 98.68%, demonstrating effective performance. With a precision of 98.69% and a recall of 98.68%, it shows a high rate of true positive predictions and a strong ability to identify actual positives. The F1-score of 98.68% further underscores its reliability. Overall, the logistic regression model is highly effective for the task.

K-Nearest Neighbors (KNN) (Non-Parametric)

The training phase is significant as it retains the complete dataset. Nevertheless, it may incur high computational costs when dealing with large datasets, and its effectiveness depends on the selection of k and the distance measurement used. KNN also requires normalized data due to its sensitivity to feature scaling.

Training:
Store the entire training set D_{train}.
Validation:
For each sample in D_{val}, find the k nearest neighbors in D_{train} using a distance metric (e.g., Euclidean distance):$d(x_i, x_j) = \sqrt{\sum_{l=1}^{p} (x_{il} - x_{jl})^2}$
Predict the class by majority voting:$\hat{y}_i = \text{mode}(\{y_{j1}, y_{j2}, \dots, y_{jk}\})$
Compute validation accuracy as above.

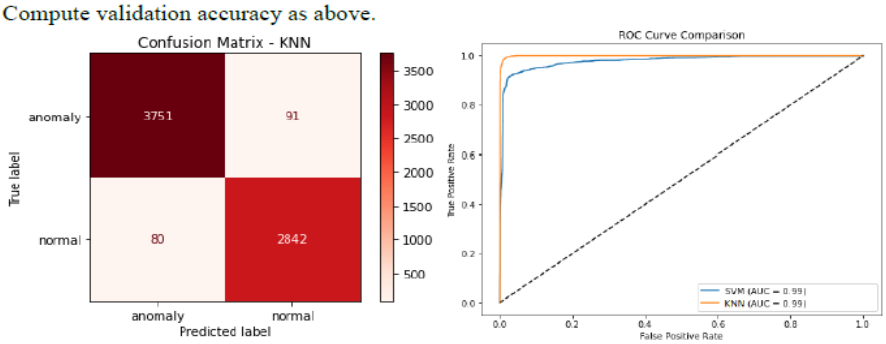

Figure 5: KNN Confusion Matrix and ROC Curve

RESULTS

The KNN model achieved a classification accuracy of 97.47%, demonstrating effective performance. With a precision of 97.47% and a recall of 97.47%, it shows a high rate of true positive predictions and a strong ability to

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

identify actual positives. The F1-score of 97.47% further underscores its reliability. Overall, the logistic regression model is highly effective for the task.

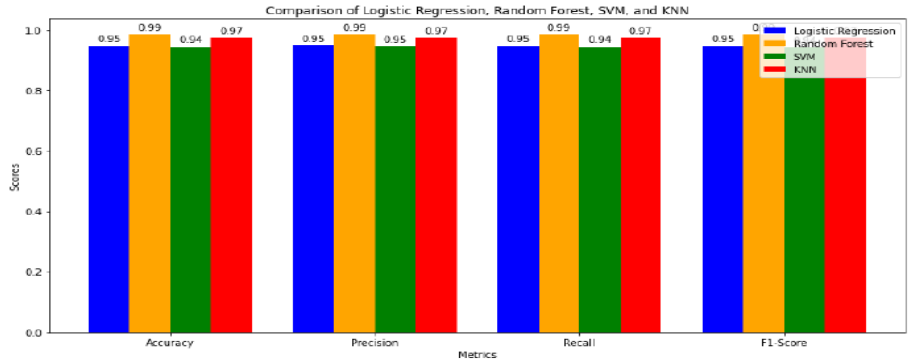

Figure 6: Performance Comparison of models

CONCLUSION

This study explores the effectiveness of non-parametric machine learning algorithms in detecting anomalies in network traffic, a vital aspect of cybersecurity. Among the models assessed, the Random Forest (RF) algorithm stood out as the most effective, achieving an impressive accuracy of 98.68%, along with strong precision, recall, and F1-score metrics. This highlights the power of ensemble methods in capturing the complex, non-linear patterns found in network traffic data. The K-Nearest Neighbors (KNN) model also performed well, attaining an accuracy of 97.47%. These results emphasize the value of non-parametric approaches for anomaly detection. In contrast, traditional parametric models such as Logistic Regression and Support Vector Machines (SVM) achieved lower accuracies of 94.75% and 94.41%, respectively. The findings underscore the potential of machine learning—especially non-parametric and ensemble methods—in strengthening intrusion detection systems. This research offers valuable insights for selecting algorithms suited for network traffic analysis, paving the way for the development of more robust and efficient cybersecurity solutions. Future studies could explore hybrid models, deep learning frameworks, or real-time detection strategies to further enhance anomaly detection capabilities. Ultimately, this work contributes to the broader effort of improving network security and addressing the challenges posed by evolving cyber threats through advanced machine learning techniques.

REFRENCES

[1]. Ata, O. Network Intrusion Detection Using Machine-Learning Techniques. . 2017; 7. https://doi.org/10.5958/2249-3220.2017.00004.0

[2]. Almutairi, Y., Alhazmi, B., & Munshi, A. Network Intrusion Detection Using Machine Learning Techniques. Advances in Science and Technology Research Journal. 2022 https://doi.org/10.12913/22998624/149934

[3]. Hosen, M., Shafin, A., & Yousuf, M. Performance Analysis of Machine Learning Techniques in Network Intrusion Detection. Journal of Information Technology. 2023 https://doi.org/10.59185/svmz6x07

[4]. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection. IEEE Communications Surveys & Tutorials. 2019; 21. https://doi.org/10.1109/COMST.2018.2847722

[5]. Babu, B., Reddy, G., Goud, D., Naveen, K., & Reddy, K. Network Intrusion Detection using Machine Learning Algorithms. 2023 3rd International Conference on Smart Data Intelligence (ICSMDI). 2023 https://doi.org/10.1109/ICSMDI57622.2023.00071

[6]. Li, Z., Rios, A., & Trajković, L. Machine Learning for Detecting Anomalies and Intrusions in Communication Networks. IEEE Journal on Selected Areas in Communications. 2021; 39. https://doi.org/10.1109/JSAC.2021.3078497

[7]. Li, J., Qu, Y., Chao, F., Shum, H., Ho, E., & Yang, L. Machine Learning Algorithms for Network Intrusion Detection. AI in Cybersecurity. 2018 https://doi.org/10.1007/978-3-319-98842-9_6

[8]. Singhal, A., Maan, A., Chaudhary, D., & Vishwakarma, D. A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). 2021 https://doi.org/10.1109/ICAIS50930.2021.9395918

[9]. Sharma, R., Kalita, H., & Borah, P., Analysis of Machine Learning Techniques Based Intrusion Detection Systems. . 2016 https://doi.org/10.1007/978-81-322-2529-4_51

[10]. Pascal Maniriho, L. Mahoro, Ephrem Niyigaba, Zephanie Bizimana, T. Ahmad, Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches, International Journal of Intelligent Engineering and Systems 2020. DOI: 10.22266/ijies2020.0630.39

[11]. V. A and A. Vikas Singh, "Analysis of Traffic Sampling on Machine Learning Based Network Intrusion Detection," 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), Singapore, Singapore, 2023, pp. 415-420, doi: 10.1109/SmartTechCon57526.2023.10391803.

[12]. Atassi, Reem. Anomaly Detection in IoT Networks: Machine Learning Approaches for Intrusion Detection. Fusion: Practice and Applications, vol., no., 2023, pp. 126- 134. DOI: https://doi.org/10.54216/FPA.130110

[13]. Jihane Ben Slimane, Eman H. Abd-Elkawy, Albia Maqbool, Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT, Journal of Electrical Systems, 2024, Vol 20, https://doi.org/10.52783/jes.1813

[14]. Wasim A. Ali, M. N, M. Aljunid, Malika Bendechache, P. Sandhya, Review of Current Machine Learning Approaches for Anomaly Detection in Network Traffic, Journal of Telecommunications and the Digital Economy 2020.

[15]. Keerthana P, Devith M D, Hariharan G, Muthukumar S, Machine Learning-Based Anomaly Detection for Imbalanced Network Traffic , 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA) https://doi.org/10.1109/AIMLA59606.2024.10531509

[16]. Pavan Raviteja Upadhyayula, K. Amarendra, Sanjay Bhargav Kudupudi, Intrusion Detection of Imbalanced Network Traffic, 2022 7th International Conference on Communication and Electronics Systems (ICCES) https://doi.org/10.1109/icces54183.2022.9835996

[17]. Thirumaraiselvi, Sreyaniketha, V. Rahul, K.S Tamilnilavan, Enabling Robust Intrusion Detection in Network Traffic through an Integrated Machine Learning Framework, 2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN) https://doi.org/10.1109/ICIPCN63822.2024.00038

[18]. Adnan Helmi Azizan, Salama A. Mostafa, Aida Mustapha, Cik Feresa Mohd Foozy, Mohd Helmy Abd Wahab, Mazin Abed Mohammed and Bashar Ahmad Khalaf, A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems, Annals of Emerging Technologies in Computing (AETiC) Vol. 5, No. 5, 2021

[19]. Idio Guarino, Giampaolo Bovenzi, Davide Di Monda, Giuseppe Aceto, D. Ciuonzo, A. Pescapé, On the use of Machine Learning Approaches for the Early Classification in Network Intrusion Detection, 2022 IEEE International Symposium on Measurements & Networking (M&N) https://doi.org/10.1109/MN55117.2022.9887775

Research Article

[20]. Shaila Sharmin, Hafizah Mansor, Intrusion Detection on the In-Vehicle Network Using Machine Learning, 2021 3rd International Cyber Resilience Conference (CRC) https://doi.org/10.1109/CRC50527.2021.9392627

[21]. Gaurav Kumar, Jawahar Thakur, Machine Learning Approaches for Network Intrusion Detection: An Evaluation of their Efficacy in Bolstering Security, International Journal for Research in Applied Science and Engineering Technology, 2024 https://doi.org/10.22214/ijraset.2024.63565

[22]. Rahbar Ahsan, Wei Shi, J. Corriveau, Network intrusion detection using machine learning approaches: Addressing data imbalance, IET Cyper-Phys. Syst.: Theory & Appl. 2021, https://doi.org/10.1049/cps2.12013.

[23]. Atul Kumar, Ishu Sharma, Intrusion Type Classifier: A Machine Learning Based Approach for Automated Detection and Classification of Network Intrusions, 2023 3rd International Conference on Smart Generation Computing, Communication and Networking, https://doi.org/10.1109/SMARTGENCON60755.2023.10442249.