Explainable Hybrid Machine Learning for Autonomous Optimization of Network QOS in Cyber Security

Anan Ismail Ahmed[1†],

University of Science and Technology, Sudan, Faculty of Engineering

Abstract

Cyber Security is a smart defense strategy that uses advanced artificial intelligence as a shield. Artificial Intelligence (AI) and Machine Learning (ML) enhance cyber security by enabling faster and more accurate threat detection, automated responses and adaptive defense system that learn from data. Network security on the other hand, involves protecting, monitoring and controlling the network infrastructure and the data transmitted across it. In this study predictive analysis was performed to classify network threats based on key performance metrics such as band width, latency response time and jitter. The network data set consisted of 1000 instances and 5 attributes to evaluate the classification performance; several data mining algorithms namely Naive Bayes, IBK, SMO, Logistic, and Random Tree were implemented using the WEKA data mining tool. The experimental results indicate that the Random Tree classified achieved the best performance compared to the other algorithms. The accuracy obtained by the five algorithms was as follows (Random Tree 99.8%) IBK (95.9%) Naive Bayes (94.8%) Logistic Regression (87.9%) and SMO (87.7%). These findings demonstrate that the Random Tree model provides superior predictive capability for network threat detection. The confusion matrix analysis indicates that the proposed model has a strong capability to correctly identify attack traffic. With minimal misclassification. The model also demonstrates reliable performance in distinguishing between warning and normal network states. These results confirm it effectiveness in detecting real time performance degradation and identifying potential network threats. The evaluation process includes measuring model accuracy to determine the effectiveness of the classification results. The findings indicate that machine learning based approaches significantly improve network monitoring performance and enhance cyber security decision making processes. These results demonstrate the importance of predictive models in identifying network anomalies and supporting proactive threat mitigation strategies.

Keywords:

Network performance Analysis; Network Traffic Predication; Performance Optimization; Throughput Optimization; Real-Time Monitoring; Feature Selection; Predictive Modeling; Network Delay Analysis; Intelligent Network Management; Weka Tool

1. Introduction

Artificial Intelligence adds significant value to Cyber Security due to its ability to rapidly process and monitor large volumes of data. This capability enhances threat visibility by identifying unusual patterns or suspicious activities that humans might miss. AI systems also enable faster response times by automating detection and mitigation processes, thereby reducing the window of opportunity for attackers. In additional AI supports predictive analysis helping security teams anticipate potential threats before they occur and proactively strengthen their defenses.

An exploit is a piece of code or technique that takes advantage of vulnerability in a system. Once vulnerability is discovered, the information can be used by the finder or share with other to develop an exploit. The exploit is then used to attack vulnerable systems, enabling malicious actions such as gaining unauthorized access, stealing data or disrupting of operations.

Exploit code is specially crafted software designed to leverage a known vulnerability in a system and allow an attacker to execute unauthorized actions. In modern Cyber Security Machine Learning models can be trained on large and diverse data sets to detect attacks and identify anomalies that may indicate previously unseen threats. Advanced techniques such as deep learning, further enhance this capability by learning complex patterns; Additionally, Natural Language Processing (NLP) enable security systems to analyze logs, reports and threat intelligence written in human language together these AI technologies significantly improve the accuracy and speed of threat detection.

With the rapid growth of communication technologies and the increasing reliance on digital services, maintaining a secure and reliable Network infrastructure has become a critical requirement. Network traffic monitoring plays a vital role in ensuring service quality, detecting anomalies and preventing potential cyber threats. Continuous

Manuscript received April 5, 2026
Manuscript revised April 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.4.3

observation of traffic patterns enables network administrators to identify abnormal behavior that may indicate malicious activities such as attacks, intrusions or system misuse [1] key network performance indicators such as bandwidth, latency, Response time and jitter provide essential insights in to network conditions and overall system performance. Significant deviations in these metrics often reflect congestion configuration issues, or security incidents for instance, abnormal increases in latency and jitter may signal denial-of service attacks, while unusual bandwidth consumption can indicate unauthorized data transfer or malware activity [2] traditional traffic analysis techniques, including port-based and payload –based methods, have limitations in modern networks due to dynamic port usage and widespread encryption consequently machine learning approaches ,have emerged as effective solutions for analyzing complex traffic patterns, and identifying hidden threats. By learning from historical data, these techniques can accurately distinguish between normal and abnormal network behavior, thereby enhancing cyber security capabilities [3] tool such as wire shark enable the capture of real-time network traffic, while data mining platforms like WEKA provide a wide arrange of machine learning algorithms for classification and predictive analysis. These tools facilitate the development of intelligent monitoring systems capable of detecting performance degradation and potential security threats [4] therefore analyzing network performance metrics as indicators of abnormal behavior represents a promising approach for proactive Cyber security management. Such analysis supports early heart detection, improves network reliability and assists decision-maker in maintaining secure and efficient communication systems.

This study focuses on monitoring network traffic using band width latency, response time, and Jitter as primary indicators to evaluate network conditions and detect abnormal behaviors. According to International Telecommunication Union (ITU) maintaining stable latency and minimal Jitter is critical for real time services including voice and video communications. Similarly, studies published by the IEEE high light the integration of machine learning techniques with network performance metrics to improve predictive threat detection and automated decision-making processes. Therefore, monitoring network traffic using band width latency, response time and Jitter provides a comprehensive framework for assessing network health and identifying potential security risks.

This research focuses on analyzing these performance indicators to support proactive network management and strengthen cyber security infrastructure through data driven methodologies.

1.1 Problem Statement:

Modern networks face increasing challenges in maintaining optimal QOS (latency, bandwidth, Jitter, and response time) under evolving cyber threats, while existing solutions lack both adaptability and interpretability therefore, there is a need for an explainable hybrid machine learning approach that can autonomously optimize QOS and enhance cyber security through transparent and intelligent decision - making.

1.2 Research Questions:

1. How can explainable hybrid machine learning architectures effectively model and analyze large-scale, dynamic network traffic to detect sophisticated and evolving cyber threats?
2. To what extend can these architectures generalize to identify zero - day attack while sustaining optimal QOS metrics (latency, bandwidth, and Jitter) under real world conditions?
3. How do explain ability techniques influence the interpretability transparency, and operational trust of AI driven cyber security systems?
4. What is measurable impact of autonomous optimization mechanisms on enhancing network QOs and resilience in adversarial environments?

1.3 Objective:

A. To design an explainable hybrid machine learning framework for intelligent network QOS optimization in cyber security contexts.
B. To evaluate the model's capability in detecting both known and unknown (zero – day) cyber threats.
C. To assess the trade-off between model performance and explain ability.

D. To improve QOS parameters (latency, bandwidth and Jitter) through autonomous optimization techniques.

2. Literature Review

Machine Learning (ML) and Deep Learning (DL) have become indispensable in cyber security, offering robust tools for identifying and mitigating cyber threats traditional ML, approaches, such as decision trees, support vector machines (SVMS), and K-nearest neighbors, rely on feature engineering to detect patterns and anomalies in network traffic, system logs, and other data sources [13] these methods have been successfully deployed for intrusion detection system (IDSs) and malware classification. However, their reliance on manually engineered features and inability to scale to high dimensional data often limit their performance in real-world applications.

Deep learning, on the other hand, provides an automated framework for feature extraction, enable models to learn complex representations from raw data. DL architectures, such as convolutional neural networks (CNNS) and recurrent neural networks (RNNs), have demonstrated superior performance in detecting threats like phishing attempts and advanced persistent threats (APTs) [14]. Moreover, hybrid models combining the strengths of different DL techniques have emerged, addressing diverse challenges in cyber security. These advancements are critical for processing the massive and continuously growing datasets typical in cyber security environments.

Ahmed et al [15] (2018) highlighted the importance of performance – based traffic features in anomaly detection frameworks.
Lippmann et al [16] (2000) introduced the DARPA intrusion detection evolution framework, which laid to foundation for traffic based detection.

Moustafa and Slay (2015) developed the UNSW-NB15 data set in cooperating modern network traffic features or intrusion analysis

Kim et al [17] (2016) demonstrated the effectiveness of deep learning modes in detecting abnormal network traffic patterns.

NIST describes intrusion detection systems as critical components of cyber security infrastructure.

IEEE research publications emphasize anomaly detection using performance based metrics. ACM digital library studies demonstrate the effectives of supervised learning in network security.

AI-yaSeen, Othman and AI-yassen [18] (2017) implemented a hybrid support vector machine (SVM) approach for intrusion detection, achieving higher accuracy than traditional signature based models.

Vinay a Kumar et al [19] (2019) applied recurrent neural networks (RNNS) and Long Short-Term Memory (LSTM) models to detect anomalies in traffic flows demonstrating that deep learning can effectively capture temporal dependencies in complex data sets.

In malware analysis, Raff et al [20] (2018) used neural networks architectures trained on raw binary data to distinguish between being and malicious files without manual feature extraction, showing significant improvements over classic features based methods.

According to [5] high quality training data sets is required because reducing the large number of false alerts and increasing accuracy during the process of detecting unknown attack patterns remains unresolved problem. Unfortunately, the data set available have deficiencies, correlated data set and applicable to only DOS attack. [6], [7] and [8] evaluated machine learning –based intrusion detection systems using only a single attack type (e.g. DOS), to measure performance accuracy. However, these models against other and more recent attack types remains uncertain, and their performance tends to decline when exposed to diverse attack scenarios. Therefore, it is necessary to evaluate intrusion detection systems using multiple categories of attacks to abstain a more comprehensive and reliable assessment. The behavior of these models under varying attack conditions is not fully understood, particularly regarding their generalization capability across different environments to address this limitation, this study employs the recent CSE-CIC-IDS2018 dataset, which provides a comprehensive and realistic SDN environment .By synthesizing and analyzing existing research, this work situates itself

with in broader context of intrusion detection ,emphasizing the need for innovative solutions to counter evolving cyber threats .Accordingly, this study establishes a foundation for exploring the integration of SDN and IDS using machine learning techniques to enhance network security.

In [9] the CIGIDS 2017 IDS data set was introduced. This data set consists of seven real-time attacks with 80 network traffic features. The random Forest Regress or features reducing algorithm was used to determine the best feature set for detecting each attack. Then seven ML classifiers were employed to evaluate the performance with these features. The results obtained show that Rand Forest has the highest accuracy and shortest execution time. Moreover, a comparison was made between the GIGDS 2017 data set and publicly available data set based on criteria for an ideal data set in [10]. It was concluded that none of the data set exceeded the criteria except GIGIDS 2017.

In [11], the Random Tree, J48, Naïve Bayes, FM Decision table, Bayes Network, and MLP algorithms were evaluated using the KDDIDS data set. This data set consists of 19% benign instances 79% DOS attacks and 2% other attack. SQL server 2008 was used to extract 148753 instances to train the model and 60000 instances for testing. The results obtained show that the Rand Forest classifier achieved the highest accuracy and the Smallest Root Square Error (RMSE) and False Positive Rate (FPR), RMSE is a measure of difference between the predicted and actual outcomes, and while FPR is the ratio of benign instances incorrectly classified as attacks the total number of benign instances.

In [12], fifteen ML classification algorithm, namely Bayes Net, Naïve Bayes, Naive Bayes updateable naive Bayes Multinational text, logistic, simple logistic, voted perceptron, decision table, JRIP one R, zero Rm J48, Random tree and Random Forest were implemented. The NSL-KDD data set was considered using the data processing tool WEKA with 10-fold cross-validation. The results obtained show that Random Tree has the lowest execution time and the highest accuracy. Research on machine learning classifiers shows that decision trees, Bayesian models, and support vector machines can effectively distinguish between normal and malicious traffic patterns. A study on network traffic analysis using WEKA demonstrate that decision tree algorithms such as C4.5 achieve high classification accuracy when applied to extracted traffic features.

3. Methodology:

In methodology using threat intelligence to the collection, processing and analysis of data to understand a threat actor's motives, targets and attack methods transforms raw data into actionable insights to make informed, data driven decisions.

3.1 Data Description

The data set used in this study consists of network performance metrics. The metrics include Bandwidth, latency, response time and Jitter which represent fundamental indicators for evaluating network performance and detecting abnormal behavior. The data were collected in the form of numerical records where each record represents specific network state at a particular point in time. In addition, the data set include class attribute (Actual class) performance degradation or an early alert condition.

Table 1: Data set description

Item	Describe	Attribute Type
Band width	The maximum data transfer rate of the network during specific period	Numeric
Latency	The time taken for a packet to travel from source to destination	Numeric
Response Time	The total time between sending a request and receiving a reply	Numeric
Jitter	The variation in packet delay over time	Numeric
Traffic Label	Classification of network categorical state (Normal/attack)	Nominal
Time Stamp	Time when the measurement was recorded	Temporal

3-2 Selected Tool

The framework implemented in this study is based on WEKA platform. WEKA is comprehensive data mining environment developed at the University of Waikato in New Zeeland, utilizing the JAVA programming language. It provides a robust set of machine learning capabilities designed for analyzing real- world datasets. The platform includes wide range of algorithms that support various data mining tasks such a data pre-processing, classification, regression, clustering, and association rule mining. Additionally, WEKA offers integrated visualization tools to facilitate data interpretation. Its open-source nature allows researchers to develop and customize new machine learning models efficiently under a general public license (21)

3-3 Pre-processing

Data pre-processing (22) represents a fundamental stage in the data mining pipeline, as it directly influences the quality and reliability of subsequent analysis. This phase involves transforming raw data- often stored in CSV format-in to a structured and analyzable from key operations (23), include handling missing value, eliminating inconsistencies, and converting data in to appropriate formats such as numerical and nominal attributes. Effective pre- processing enhances data integrity and significantly improves the performance of machine learning models (24).

3-4 Predictive Models

Machine Learning techniques encompassing both supervised and unsupervised approaches, play avital role in the development of predictive systems. These models leverage historical data to extract meaningful patterns and correlations associated with cybersecurity threat. By learning from past behaviors predictive models can forecast potential risks and support proactive decision –making. furthermore, comparative evaluations against traditional approaches are typically conducted to assess improvement in detection accuracy and overall system performance (25).

3-5 Comparative Analysis

A comparative evaluation is conducted to analyze the performance differences between traditional cyber security techniques and machine learning based approaches. This analysis focuses on key performance indicators including response time, detection accuracy, and resource utilization. The results highlight the effectiveness of AI-driven models in enhancing cybersecurity operations by improve detection capabilities and optimizing system efficiency. such comparisons provide deeper insights in to the advantages of integrating intelligent systems with in network security frameworks (26).

3-6 Statistical Evaluations

Statistical methods are employed to evaluate the performance and reliability of anomaly detection models, as well as the effectiveness of network optimization strategies (27). Key metrics such as false positive rates, latency improvement, and band width efficiency are analyzed to assess model accuracy and system performance. furthermore, graphical representations, including charts and plots, are utilized to clearly illustrate patterns, trends and overall outcomes, enabling a more comprehensive understanding of the results.

4. Experiments and Results

In this article, we will examine a comparative report on a data extraction technique used to forecast network detection threats using actual class from the bandwidth, responsible time, latency and Jitter of network traffic and then choose the most efficient classifier on the basis of these metrics.

4-1 Evaluation Metrics:

1. Accuracy:
   accuracy is defined as the proportion of correctly classified instances with in a given dataset. It evaluates the overall effectiveness of the model by measuring the agreement between predicted and actual outcomes.

2. Recall:
   Recall measures the models ability to correctly identify all relevant instances. Its calculated as the ratio of correct predicted positive instances to the total actual positive instances in the dataset.

3. F-Measure(F1 Score):
   The F-measure, also known as the F-score, represents the harmonic mean of precision and recall. It provides a balanced evaluation of the models performance,

particularly when dealing with imbalanced datasets. The F-score ranges between 0 and 1, where higher values indicate better performance.

4. Error Rate:

The error rate represents acritical evaluation metric in machine learning and classification tasks, reflecting the models overall misclassification frequency. It provides direct measure of model reliability, where minimizing the error rate is essential for achieving robust and accurate predictive performance.

4-2 Data Set:

Cyber security full data is the name of the data set. This CSV file includes the following five elements (Band width, Latency, Response time, Jitter, Actual class) The following Figures demonstrate the performance of classification algorithms implemented using the WEKA tools, reflecting the network providers' state at a specific time based on a dataset of 1000 instances.

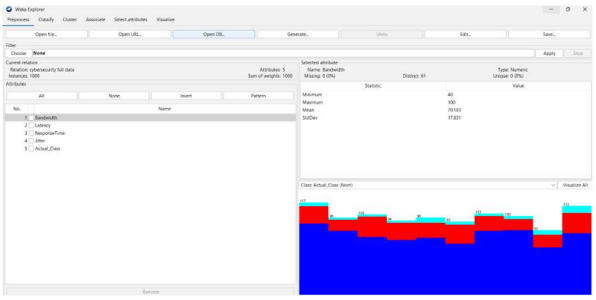

Figure 1: Data set

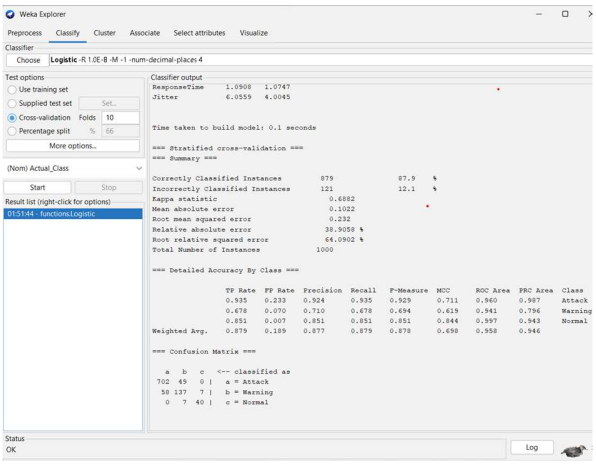

Figure 2: Result of a classification model generated by the Logistic Algorithm

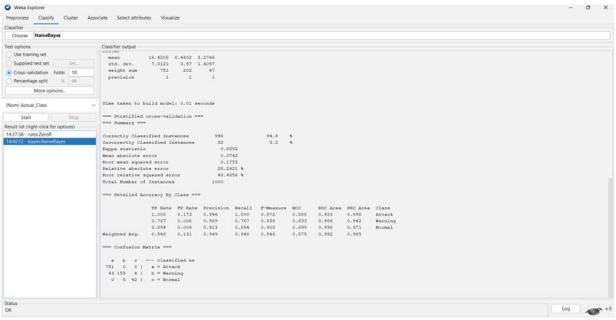

Figure 3: Result of a classification model generated by the Naïve Bayes Algorithm

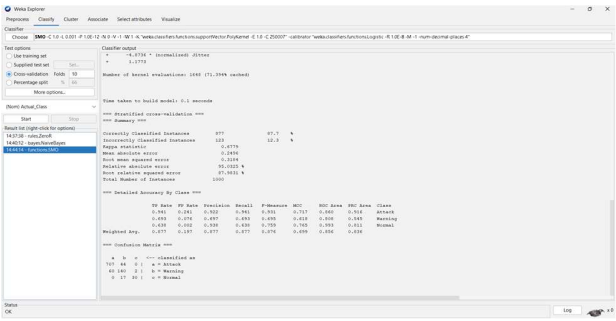

Figure 4: Result of a classification model generated by the SMO Algorithm

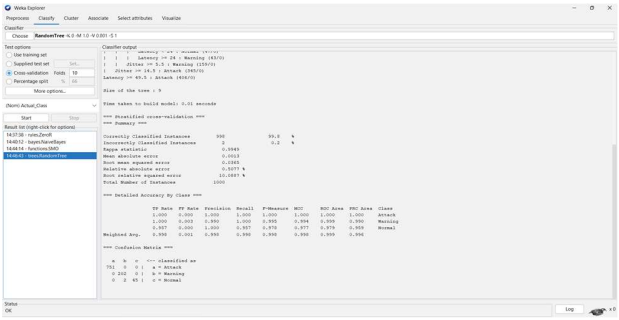

Figure 5: Result of a classification model generated by the Random Tree Algorithm

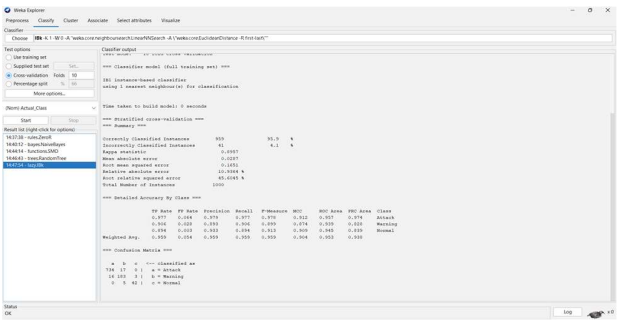

Figure 6: Result of a classification model generated by the IBK Algorithm

5. Results:

Performance Evaluation of the proposed Model: This section evaluates the performance of the proposed network detection model using accuracy, precision, recall and F measure as performance metrics. The assessment was conducted with the cyber security data set in the WEKA application, utilizing Principal Component Analysis (PCA) for feature selection. Machine Learning classifiers including Random Tree, Naïve Bayes, IBK, SMO and Logistic Regression were tested and compared in this research. Figure (7) provides a visual representation of the evaluation outcomes across these metrics.

Accuracy:

The accuracy metric determines the fraction of correctly classified packets in the data set. It measures the classifier's ability to identify Legitimate and Malicious traffic. Figure (7) illustrates the accuracy values for various algorithms. Random Tree achieves the highest accuracy at 99.8% slightly surfacing IBK which recorded 95.9%. Conversely, SMO demonstrated the lowest accuracy at 87.7%. The accuracy value for Naive Bayes and Logistic were 94.8% and 87.9% respectively reflecting their moderate performance.

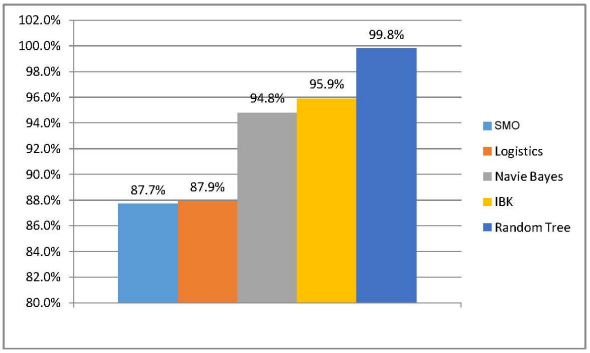

Figure 7: Accuracy

Precision:

Precision evaluates the reliability of the model when identifying positive instances. Precision measures the proportion of correctly predicted positive instances among all instances predicted as positive by the model. As shown in Figure (8), Random Tree achieved precision values of 99.8% followed by IBK with 95.9% Naive Bayes and SMO achieved precision values of 94.3% and 87.7% respectively, while Logistic displayed the lowest precision at 86.7%

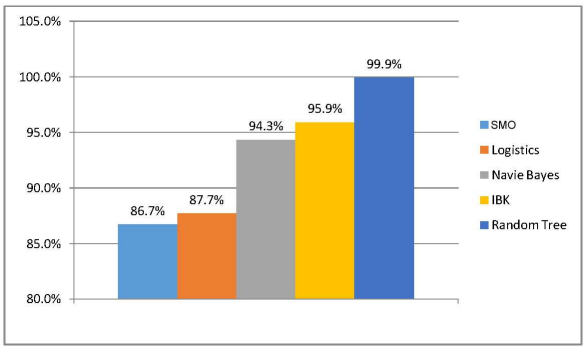

Figure 8: Precision

Recall:

Recall measure the ability of classification model to correctly identify all relevant positive instances in the data set. Figure (9) highlights that Random Tree performed the best recall value, achieving a recall of 99.9% IBK followed closely with recall of 95.9%, Naive Bayes demonstrated recall values of 92.2% while Logistic and SMO exhibited the lowest recall value (87.7%) among a valuated algorithm.

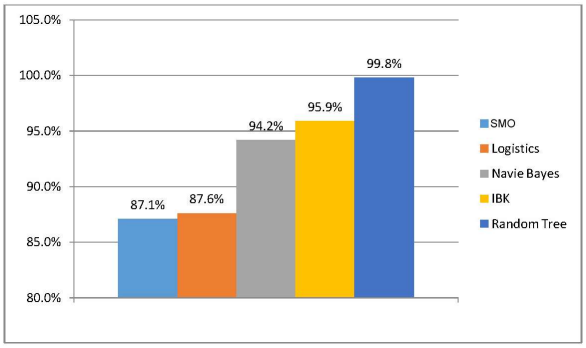

Figure 9: Recall

F-measure:

The F-measure represents the harmonic mean of precision and recall and is used to evaluate the balance between these two metrics in classification models. Figure (10) shows that the Random Tree algorithm achieved the highest F-measure value of 99.8%. Followed by IBK with 95.9% while Naïve

Bayes scored 94.2%, Logistic regression and SMO recorded the lowest F-measure both at 87.7%

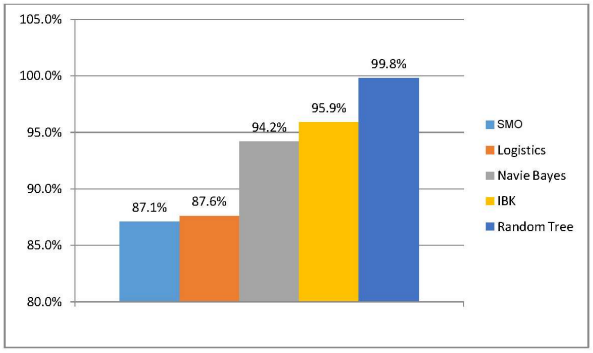

Figure 10: F-measure

From the performance results, show that Random Tree classifier outperformed the other models, achieving the highest scores across all evaluation metrics including Accuracy, Precision, Recall and F-measure. This indicates its strong capability and suitability for network intrusion detection tasks while the remaining algorithms exhibited comparatively lower and varying levels of effectiveness.

Performance of classifiers

This study analyzed the effectiveness of several machine learning classification algorithms, including IBK, Random Tree, Logistic Regression, SMO and Naïve Bayes for monitoring network performance using Quality of Service (QOS) parameters such as response time, latency, band width and Jitter. The experimental results showed that machine learning techniques can effectively classify network conditions and analyze network behavior based on these QOS metrics. Among the evaluated algorithms, Random Tree achieved the best classification performance with the highest accuracy, while IBK also demonstrated strong capability in identifying patterns in the data set. Logistic Regression and SMO produced stable and reliable results, whereas Naïve Bayes provided efficient performance with low computational complexity.

Over all, the findings confirm that integrating machine learning algorithms with QOS parameters can significantly enhance intelligent network monitoring, improve performance evaluation, and support better decision-making for network optimization and management in modern communication systems.

In addition to the Random Tree, other classifiers were evaluated, with their results presented in Table (2) and Figure (11). These visualizations highlight the comparative performance of various machine learning algorithms. The findings suggest that employing Random Tree can enhance intrusion detection efficiency in network detection multi-controller models, providing both high accuracy and faster detection rates for intelligent network traffic management systems.

Table 2: Comparison of different machine learning classification algorithms

Algorithm	Accuracy	Precision	Recall	F-measure
SMO	87.7 %	86.7 %	87.1 %	87.1 %
Logistic	87.9 %	87.7 %	87.6 %	87.6 %
Naïve Bayes	94.8 %	94.3 %	94.2 %	94.2 %
IBK	95.9 %	95.9 %	95.9 %	95.9 %
Random Tree	99.8 %	99.9 %	99.8 %	99.8 %

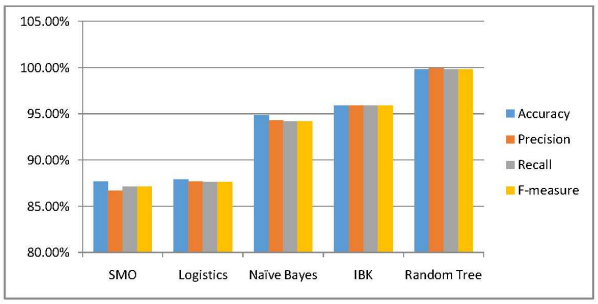

Figure 11: comparison of various machine learning classification algorithms

6. Conclusion:

In conclusion, the experimental results obtained using WEKA environment demonstrates that the IBK classifier achieved identical values for Accuracy, Precision, Recall and F-measure. This convergence among evaluation metrics indicates a highly consistent and balanced classification performance, reflecting the model's ability to maintain minimal and well distributed classification errors.

Such stability highlights the effectiveness of the IBK algorithm in capturing the intrinsic structure of the data set and producing reliable predictive outcomes.

In the context of intelligent network monitoring, the classifier showed a strong capability to analyze network performance indicators, including response time, latency, band width and Jitter. These results confirm the robustness of the model in identifying network performance patterns and supporting accurate classification of network conditions. Therefore, the IBK classifier represents a reliable approach for enhancing data – driven network monitoring and performance evaluation system. Future work may focus on integrating additional machine learning techniques and larger datasets to further improve prediction accuracy and extend the applicability of intelligent models for advanced network performance analysis and adaptive network management.

Acknowledgment

The author declares this research was conducted independently and did not receive any external funding or support.

References

[1] Nguyen T.T.T & Armitage, G (2008 A survey of techniques for internet traffic classification using machine learning IEEE communications surveys &Tutorials,10(4),56-76

[2] Call ado, A, Kamienski, C, Szabo, G, Keiner, J, fern Andes, S, & Sadok, D (2009) A survey on internet traffic identification IEEE Communications surveys &Tutorials,11(3),37-52

[3] Moore, A. W&papagi annaki, K (2005). Toward the accurate Identification of network applications passive and active Measurement conference (PAM).

[4] Witten I.H, Frank, E & Hall, M.A(2011) data mining: practical Machine learning tools and techniques. Morgan Kaufman.

[5] Said, A, Hmed, M& Mohammed E (2020) challenges in Building SDN dataset for machine learning A comprehensive survey. Journal of information security and Application ,50, 102-513 HTTp://DOI.Org/10.1016/I.Jisa 2020 102513

[6] Kumar, P, Kumar, R, &Singh A (2020) statistical Approaches for Dodos Detection in SDN International Journal of computer Networks and communication,12(2),1-16. HTTPS://DOI.Org/10.5121/''IJcnc.2020.12201

[7] Lakshmanan R. ETAI (2018) Militating DOS Attacks in SDN International Journal of cybersecurity, (29) (1),33-50.

[8] Ram Kumar, S, K Umar, S, &Thomas, G. (2020). An Entropy Based Approach for Detecting Dodos Attacks in SDN Environments-computers &security, 92,101-118 HTTP://DOI.Org/10.1016/J Cose 2020-101826

[9] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani. Toward generating anew intrusion detection dataset and trusion traffic characterization. International conference on information science and security vol I, pp.108-116, funchal, Madeira Portugal, Jan.2018

[10] Amirhossein Gharib, Iman sharafaldin, Arash HabibiLashkari, and Ali a Ghorbani. An evaluation framework for intrusion detection dataset. IEEE international conference on information science and security.PP.1-6, pattaya, Thail and, Dec.2016

[11] Almseidin Mohammad, Maen Alzubi, Szilveszter Kovacs, and Mouhammad Alka _sassbeh. Evaluation of machine learning algorithms for intrusion detection system IEEE international symposium on intelligent systems and informatics.PP.277-282, Subotica, Serbia, sep.2017

[12] Prachi Chaudhary. Usage of machine learning for intrusion detection in a network international Journal of computer network and applications. Vol .3, no.6, PP.139-147, Now.Dec.2016

[13] Sommer, R, & Paxson, V (2010) outside the closed world on using machine learning for network intrusion detection IEEE symposium on security and privacy.

[14] [14] Buczak, A.L., &Guven, E (2016) A. survey of datamining and machine learning methods for cybersecurity intrusion detection IEEE communication surveys &Tutorials 18(2) ,1153-1176

[15] Ahmad, 1, Basheri, M, 19bal, M. J, &Rahim, A. (2018) performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection IEEE Access ,6,33789-33795

[16] Lippmann, R.P.et al (2000) Evaluating intrusion detection systems. The 1998 DARPA of line intrusion detection Evaluation DARPA information survivability conference and Exposition Mustafa, N, &slay, J. (2015) UNSW –NB15: A comprehensive dataset for network intrusion detection systems. Military communication and information systems conference(MIKIS)

[17] Kim, G, Lee, S &Kim, S (2016) A novel hybrid intrusion detection methods integrating anomaly detection with misuse detection. Expert systems with applications ,41(4) ,1690-1700. Andrews. Tanenbaum &David J Wetherall computer networks ,5thed, Pearson, 2011.international telecommunication (ITU), "Quality of service (QOS) standards" ITU-T Recommendations IEEE Research publications on network traffic analysis and anomaly detection.

[18] AI-Yassen, W. L, Othman, Z, A&AI-Yassen, W. L (2017). An intelligent intrusion detection system based on support vector machine and information selection by filter approach the scientific world journal.

[19] Vinayakumar, R, so man, K. P, & poornachandran, P (2019) applying deep learning models for network traffic classification. computers &Electrical Engineering

[20] Raff, E, Barker, J. sylvesteer, J, Brandom, R, L, catan zaro, B, & Nicholas, C (2018) Malware detection by eating a whole exe. workshops at the thirty second AAAI conference on Artificial intelligence

[21] A. Elsharif Karrar," The use of case-based Reasoning in acknowledge –based (learning) software development

organization," international journal of Innovative Research in science, Engineering and Technology (An Iso, Vol.3297, no.5,2007, doi:10.15680 /IJIRSET.2016.0505331.

[22] I. Chakraborty and A.K. Chakraborty," super-ensemble classifier for improving predications in imbalanced dataset," commun state case stud data Anal Appl, PP.1-19, Nov2020, doi :10.1080 /23737484.2020.1740065

[23] "A Review on Data Mining Techniques for Treatment of cancer in Ayurveda Therapy." [On Line] .Available:WWW.IJcset.net

[24] A.E. Karrar, "The Effect of using Data Pre –Processing by Imputation in Handling Missing Values" Indonesian journal of Electrical Engineering and Informatics (IJEEI), Vol .10, no, 2, Apr.2022, doi :10. 525491ijeei.v 10i 2.3730

[25] S. Faroo9 Mohi-U-din, M. Tari9 and A. Tari9, Deep dive in to health: Harnessing AI and deep learning for brain and heart care" International Journal of Advanced Engineering Technologies and Innovations, Vol. I, no.4, PP.248-267, 2024.Available from: HTTPS://ijaei.com/index.php/journal / article /view /272

[26] M. Tari9, Y. Hayat, A. Hussain, A. Tari9, and S. Rasooi," principles and perspectives in medical diagnostic systems employing artificial intelligence (AI) algorithms," international Research Journal of Economics and Management studies, vol. 3, no. 1, 2024. Available form: HTTPS://WWW.journal.mediapublikasi.id/index.php/bullet/ article/view/4094

[27] S.K. Lodhi, A. Y. Gill and H.K. Hussain," Green innovations: Artificial intelligence and sustainable materials in production, "BULLET: journal Multidiscipline ILmu Vol.3, no .4, pp.492-507, 2024.Available from: HTTPs://Journal.mediapublikasi.id/index.php/bullet/article view 4474