Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

Network Traffic Classification Using Machine Learning Algorithms Based on Quality of Service Parameters

Hermansyah[1,*], Al–Khaidar[1], Lisa Mulia Al Ikhlas[2], Husni[1]

[1]Informatics Study Program, Faculty of Computer Science, Universitas Almuslim, Aceh, Indonesia
[2]Informatics Study Program, Faculty of Computer and Multimedia, Universitas Islam Kebangsaan Indonesia, Aceh, Indonesia
Email: waxherman@gmail.com, alkhaidar@umuslim.ac.id, lisamulia14@gmail.com, husniabda7@gmail.com
Correspondence Author Email: waxherman@gmail.com
Submitted: 07/08/2026; Accepted: 31/08/2026; Published: 31/08/2026

Abstract–The growth of multimedia services requires network operators to identify traffic types quickly so that Quality of Service (QoS) policies can be applied precisely, while port-based classification and payload inspection are becoming unreliable because of encryption and dynamic port usage. This study analyzes 20,000 labeled flow records from four application classes, namely File Transfer, Video Streaming, VoIP, and Web Browsing, under three network load levels. Seven machine learning algorithms, namely Naive Bayes, Logistic Regression, K-Nearest Neighbor, Decision Tree, RBF-kernel Support Vector Machine (SVM), Random Forest, and XGBoost, were tested on two feature scenarios. Scenario A uses four QoS parameters (throughput, delay, jitter, and packet loss), while scenario B adds ten flow statistics. Port and protocol attributes were removed to prevent label leakage. Evaluation used a stratified 80:20 split, accuracy, precision, recall, F1-score, Cohen's Kappa, and 5-fold cross validation. All four QoS parameters differ significantly across classes (Kruskal-Wallis test, $p < 0.001$). SVM-RBF achieved the highest performance in both scenarios, with 74.3% accuracy (F1 74.9%; Kappa 0.656) in scenario A and 98.0% accuracy (F1 98.0%; Kappa 0.974) in scenario B, while Random Forest and XGBoost followed within 0.2 points in scenario B. Throughput (33.0%) and jitter (30.5%) were the most informative QoS parameters, and VoIP was the easiest class to recognize. QoS parameters alone are sufficient to separate interactive traffic such as VoIP but not to distinguish Video Streaming from Web Browsing and File Transfer. Combining QoS parameters with flow statistics raises accuracy by about 24 percentage points and provides a basis for adaptive traffic classification in QoS management.

Keywords: Machine Learning; Quality of Service; Random Forest; Support Vector Machine; Traffic Classification

1. INTRODUCTION

Accurate network traffic classification is a key prerequisite for enforcing Quality of Service (QoS) policies, because each application requires different treatment of bandwidth, delay, jitter, and packet loss [1], [2]. An operator that cannot quickly recognize traffic types will treat a VoIP call in the same way as a large file download, even though VoIP is highly sensitive to delay and jitter, whereas file transfer mainly demands throughput [3]. Such prioritization errors directly degrade the service quality perceived by users, particularly in campus and institutional networks that carry heavy traffic loads and require continuous connectivity [4]–[7].

Conventional classification approaches based on port numbers and Deep Packet Inspection (DPI) are losing their reliability. Modern applications use dynamic ports, tunneling, and end-to-end encryption, so packet payloads can no longer be read [1], [8]. Measurements on operational networks show that the share of encrypted web traffic keeps growing and that even the handshake fields relied upon by many classifiers are gradually being concealed [9]. This condition drives a shift toward classification based on flow statistics and QoS parameters, which remain observable even when packet content is encrypted [3], [10]. Machine learning has become the strongest candidate for this task because it can learn non-linear patterns from traffic characteristics without manually written rules [2], [11], and comprehensive surveys position it as the mainstream approach for encrypted traffic analysis [12], [13].

Various recent studies have demonstrated this potential. Transformer-based models such as ET-BERT achieve high performance on encrypted traffic [14], and the masked-autoencoder-based YaTC model further improves accuracy by learning multi-level flow representations [15]. Systematic reviews show the dominance of deep learning and pre-training approaches over the last five years [8], [16]. Image-like representations such as FlowPic [17] and multimodal multitask architectures such as DISTILLER [18] have also been proposed, although a study on a commercial-grade dataset with hundreds of applications revealed that the accuracy of deep models drops considerably when they face many classes and zero-day applications [19]. In Software-Defined Networking (SDN) environments, Random Forest, K-Nearest Neighbor (KNN), and Decision Tree algorithms have been reported to reach 85% to 99% accuracy [2], and more recent SDN studies confirm that classical models combined with feature selection remain competitive for stream traffic classification [20], [21]. Studies on 5G networks use traffic classification for network slicing and for predicting the Quality of Experience (QoE) of video services [22]–[24], while other studies combine traffic classification and traffic prediction in wireless networks [25] or compare online learning techniques for traffic stream analysis [26]. In Indonesia, SVM applied to campus internet traffic data achieved only about 64% accuracy [27], whereas Random Forest and SVM have proven effective for VPN traffic classification, early detection of cyber-attacks, and bandwidth usage pattern analysis [28]–[31].

The success of machine learning on tabular data is also evident beyond the network domain. Large benchmark studies show that tree-based ensembles such as Random Forest and XGBoost still match or outperform deep learning on typical medium-sized tabular datasets [32], [33], and Random Forest combined with k-fold cross

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

validation has been applied successfully to administrative classification problems [34]. Comparative studies of SVM, Decision Tree, and Logistic Regression further confirm that the performance of each method depends strongly on the characteristics of the data [35], [36]. These findings indicate that algorithm selection cannot be generalized and must be tested empirically in every data domain, including network traffic described by QoS parameters.

The research gap arises from three issues. First, most studies use raw flow features or packet bytes, so the separate contribution of QoS parameters to traffic identification is rarely measured. Second, many studies include port numbers as features, even though ports can leak the class label and produce spurious accuracy; this type of data leakage has been identified as a major cause of irreproducible results in machine-learning-based science [37]. Third, QoS studies in Indonesia generally stop at descriptive measurements based on the TIPHON standard [4]–[6] without linking them to automatic traffic classification.

Therefore, this study aims (1) to analyze differences in throughput, delay, jitter, and packet loss across four traffic classes and three network load levels; (2) to compare seven machine learning algorithms in two feature scenarios, namely QoS parameters only and QoS parameters complemented by flow statistics; and (3) to identify the most influential features as a basis for designing an adaptive QoS management system. The main contributions of this study are an evaluation protocol that is free from label leakage and a quantitative measure of the extent to which QoS parameters can explain application identity. The results are expected to help network administrators decide which measurements should be collected by a monitoring system so that traffic prioritization can be performed automatically without inspecting packet payloads.

2. RESEARCH METHODOLOGY

2.1 Research Stages

This study uses a quantitative experimental approach consisting of six stages, namely dataset collection, preprocessing, data splitting, model training, evaluation, and feature analysis. Figure 1 summarizes the research flow together with the two feature scenarios tested. The dataset stage prepares labeled flow records; the preprocessing stage removes attributes that could leak the label and standardizes numeric features; the data splitting stage separates training and testing data in a stratified manner; the training stage fits seven classifiers in each scenario; the evaluation stage measures classification quality and stability; and the analysis stage interprets feature importance and compares QoS values with the TIPHON categories.



Figure 1. Research flow of network traffic classification based on QoS parameters

2.2 Dataset

The dataset consists of 20,000 network flow records with 21 attributes covering the period from January to December 2026. Each record is labeled with one of four application classes, namely File Transfer (4,339 flows), Video Streaming (5,556), VoIP (4,489), and Web Browsing (5,616). Network load conditions are evenly divided into Low (6,687), Medium (6,672), and High (6,641). The dataset contains no missing values and no duplicate records. Table 1 presents the attribute groups and their roles in this study.

Table 1. Dataset attribute groups and their roles

Group	Attributes	Unit	Role
Label	Traffic_Class	–	Target (4 classes)
QoS parameters	Throughput, Delay, Jitter, Packet Loss	Mbps, ms, ms, %	Features of scenarios A and B
Flow statistics	Flow Duration, Total Packets, Forward Packets, Backward Packets, Total Bytes, Mean Packet Size, Packet Rate, Byte Rate, Active Mean, Idle Mean	s, packets, bytes, pps, KBps, ms	Additional features of scenario B
Context	Network_Load	Low/Medium/High	Descriptive analysis
Excluded	Record_ID, Timestamp, Source_Port, Destination_Port, Protocol	–	Not used (identifier or label leaker)

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*. Page 171
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

The four QoS parameters were selected because they are the indicators most commonly monitored by network operators and are used by the TIPHON standard to grade service quality [6]. The ten flow statistics describe the volume, direction, size, rate, and timing of each flow, which are known to be informative for traffic identification even when payloads are encrypted [10], [17].

2.3 Preprocessing and Label Leakage Prevention

An initial inspection showed that each destination port number appears only in a particular class; for example, ports 5004, 5060, and 5061 appear only in VoIP, while ports 20, 21, and 22 appear only in File Transfer. The UDP protocol also dominates VoIP (94.4%). Including these attributes would make the model memorize ports instead of learning traffic behavior, a typical form of label leakage [37]; therefore, Destination_Port, Source_Port, and Protocol were removed. Numeric features were standardized using the z-score for scale-sensitive algorithms, namely Naive Bayes, Logistic Regression, KNN, and SVM [38], as shown in Equation (1), where x is the original value, μ is the mean, and σ is the standard deviation of the feature.

$$z = \frac{x-\mu}{\sigma} \quad (1)$$

Differences in the distribution of QoS parameters across classes were tested with the non-parametric Kruskal-Wallis test because the data are not normally distributed. QoS quality was compared with the TIPHON standard categories commonly used in network studies in Indonesia [6].

2.4 Scenarios and Algorithms

Two feature scenarios were designed to measure the contribution of QoS parameters. Scenario A uses only the four QoS parameters, while scenario B uses the four QoS parameters plus ten flow statistics, giving a total of 14 features. Seven algorithms were compared using the configurations listed in Table 2. The selection of algorithms follows the practice widely adopted in traffic classification studies [2], [11], [28] and in previous tabular classification studies [32], [34], covering probabilistic, linear, instance-based, tree-based, kernel-based, bagging, and boosting families.

Table 2. Configuration of machine learning algorithms

Algorithm	Main configuration	Standardization
Naive Bayes (NB)	Gaussian	Yes
Logistic Regression (LR)	Multinomial, max_iter = 2000	Yes
K-Nearest Neighbor (KNN)	k = 7, Euclidean distance	Yes
Decision Tree (DT)	max_depth = 12	No
Support Vector Machine (SVM)	RBF kernel, C = 10, gamma = scale	Yes
Random Forest (RF)	300 trees	No
XGBoost	400 estimators, max_depth = 6, learning rate = 0.1	No

2.5 Evaluation

The data were split in a stratified manner into 80% training data (16,000 flows) and 20% testing data (4,000 flows) with random_state = 42. Performance was measured using accuracy, macro-averaged precision, recall, and F1-score as defined in Equations (2) to (5), as well as Cohen's Kappa in Equation (6). Model stability was tested through 5-fold stratified cross validation on the entire dataset [38]. Feature importance was computed from the mean decrease in Gini impurity of the Random Forest model. All experiments were run with Python 3.13, scikit-learn [39], and XGBoost [40].

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (3)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (4)$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)$$

$$\kappa = \frac{p_o - p_e}{1 - p_e} \quad (6)$$

In these equations, TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively. The notation p_o denotes the observed proportion of agreement between predictions and actual labels, while p_e denotes the proportion of agreement expected by chance. Kappa was included because it corrects accuracy for chance agreement, which makes comparisons between the four-class scenarios more robust.

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

3. RESULTS AND DISCUSSION

3.1 Traffic Characteristics and QoS Parameters

The class composition of the dataset is relatively balanced, with a ratio of 1.29 between the largest and smallest classes. Web Browsing and Video Streaming account for 28.1% and 27.8% of the data, while VoIP and File Transfer account for 22.4% and 21.7%, respectively. The three network load levels are distributed almost evenly in every class, as shown in Figure 2, so differences between classes are not caused by load imbalance.

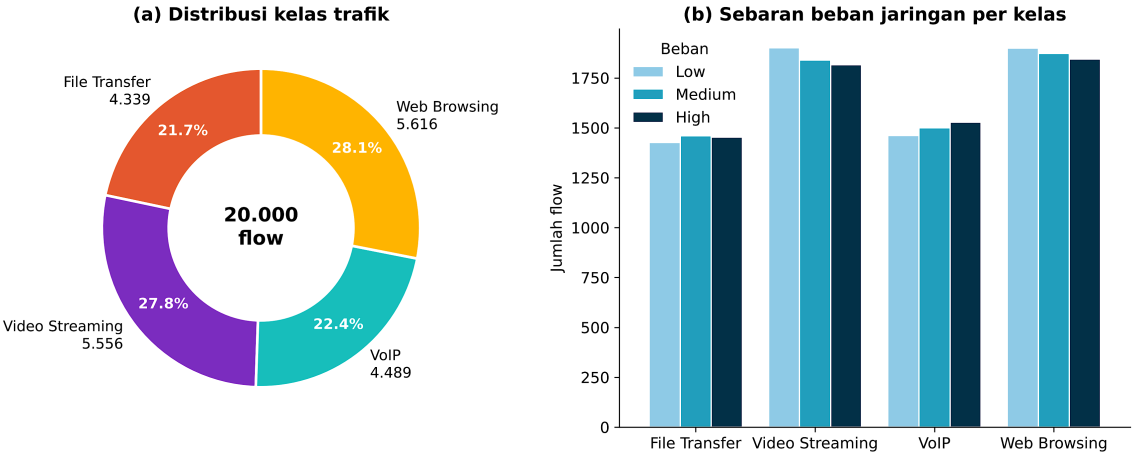


Figure 2. (a) Distribution of traffic classes (b) distribution of network load in each class

Table 3 and Figure 3 show a distinctive QoS profile for each class. File Transfer has the highest average throughput (0.855 Mbps) as well as the highest delay (47.8 ms), reflecting the nature of bulk traffic that fills queues. VoIP shows the tightest profile, namely low throughput (0.177 Mbps), the lowest delay (23.8 ms), and the lowest jitter (3.2 ms), in line with the requirements of real-time voice communication [3]. Web Browsing and Video Streaming have the highest jitter (8.7 ms and 8.0 ms), while Video Streaming records the highest average packet loss (0.487%).

Table 3. Mean (± standard deviation) of QoS parameters per traffic class and TIPHON category

Class	Throughput (Mbps)	Delay (ms)	Jitter (ms)	Packet Loss (%)
File Transfer	0.855 ± 0.525	47.78 ± 17.48	6.51 ± 2.46	0.310 ± 0.337
Video Streaming	0.464 ± 0.289	37.50 ± 16.16	7.97 ± 2.94	0.487 ± 0.531
VoIP	0.177 ± 0.115	23.78 ± 14.64	3.20 ± 1.20	0.250 ± 0.268
Web Browsing	0.232 ± 0.147	43.39 ± 16.72	8.68 ± 3.27	0.382 ± 0.406
TIPHON category	–	Very good (< 150 ms)	Good (0–75 ms)	Very good (0–2%)

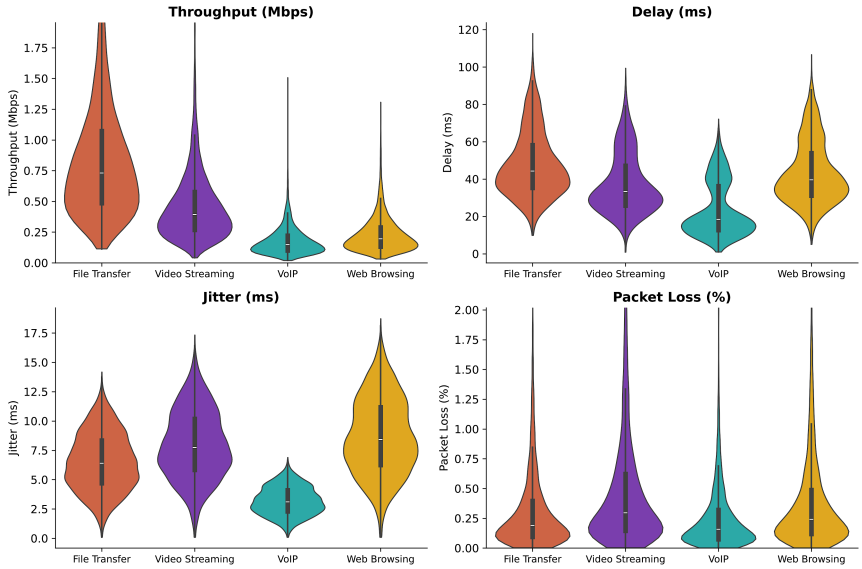


Figure 3. Distribution of throughput, delay, jitter, and packet loss in each traffic class (violin plots with embedded box plots)

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

The Kruskal-Wallis test confirms that all four QoS parameters differ significantly across classes ($p < 0.001$). The largest H statistic belongs to throughput (H = 10,538.6), followed by jitter (H = 8,514.3), delay (H = 4,583.3), and packet loss (H = 958.3). This ranking gives an early indication that throughput and jitter are the strongest class discriminators, whereas packet loss is the weakest because its distribution overlaps across all classes.

Network load affects all QoS parameters consistently, as shown in Figure 4. Average delay increases from 25.7 ms under Low load to 56.7 ms under High load, jitter increases from 4.7 ms to 9.3 ms, and packet loss rises 4.6 times from 0.147% to 0.684%. The combination of File Transfer and High load produces the highest delay (66.2 ms), while Web Browsing under High load records the highest jitter (12.1 ms). All of these values are still within the very good to good categories according to TIPHON [6], but the increasing pattern shows that the same traffic class can appear different under different load conditions. This phenomenon is one source of difficulty for classification that relies only on QoS parameters.

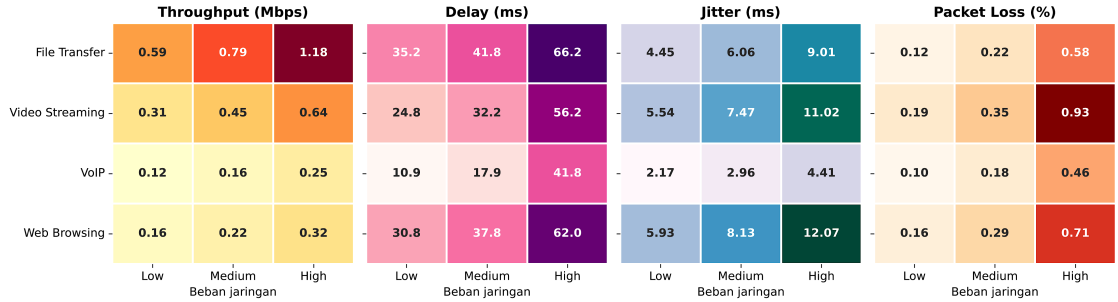


Figure 4. Average QoS parameters by traffic class and network load level

The Spearman correlation in Figure 5 shows that the QoS parameters have weak to moderate correlations with one another, so each carries relatively different information. Very strong correlations instead occur among flow volume statistics, such as Total Packets, Total Bytes, and Byte Rate. Throughput is positively correlated with mean packet size and packet rate, which explains why flow statistics are able to complement QoS parameters in scenario B.

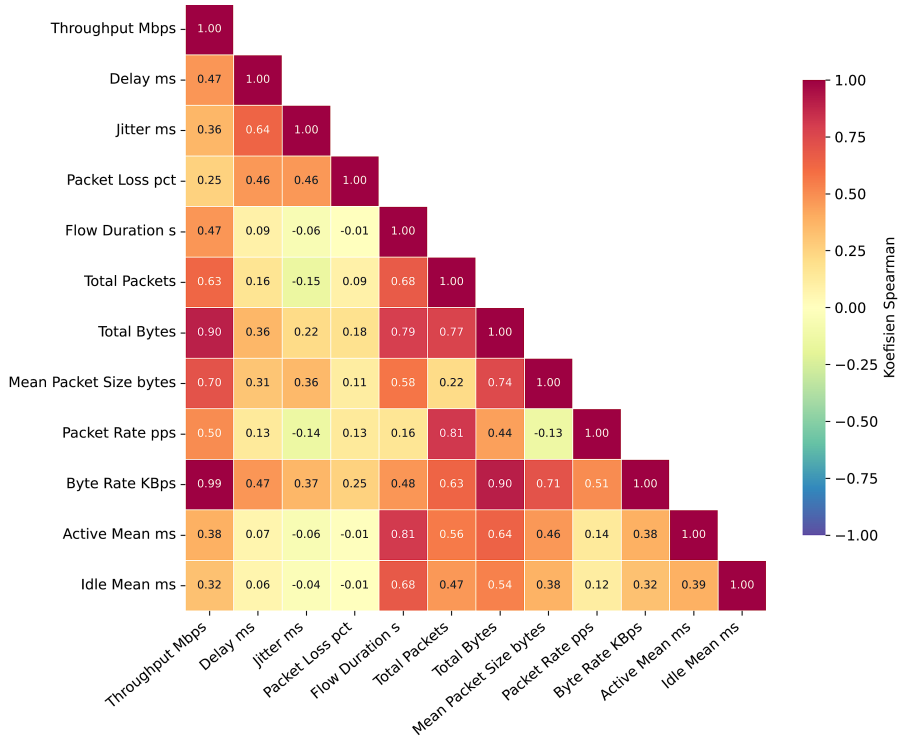


Figure 5. Spearman correlation matrix between QoS parameters and flow statistics

3.2 Comparison of Algorithm Performance

SVM-RBF is the best algorithm in both scenarios, as shown in Table 4 and Figure 6. In scenario A, SVM achieves 74.30% accuracy and a 74.90% F1-score, slightly ahead of XGBoost (73.45%) and Random Forest (73.42%). In scenario B, SVM reaches 98.02% accuracy and a Kappa of 0.974, followed by Random Forest and XGBoost, both at 97.85%. Naive Bayes ranks last in both scenarios because its assumption of feature independence is not satisfied, especially for flow statistics that are strongly correlated with each other.

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

Table 4. Algorithm performance on testing data and 5-fold cross validation

Algorithm	Accuracy A (%)	Kappa A	CV A (%)	Accuracy B (%)	Kappa B	CV B (%)	Training time B (s)
Naive Bayes	62.98	0.505	62.66 ± 0.64	93.60	0.914	93.48 ± 0.51	0.01
Logistic Regression	72.40	0.631	72.14 ± 0.74	97.70	0.969	97.68 ± 0.28	0.07
KNN	72.08	0.627	72.50 ± 0.32	97.50	0.967	97.33 ± 0.28	0.03
Decision Tree	68.45	0.577	68.88 ± 0.61	96.37	0.951	96.54 ± 0.19	0.19
SVM (RBF)	74.30	0.656	74.78 ± 0.90	98.02	0.974	97.72 ± 0.29	0.56
Random Forest	73.42	0.644	73.46 ± 0.90	97.85	0.971	97.58 ± 0.21	4.89
XGBoost	73.45	0.645	73.68 ± 0.71	97.85	0.971	97.65 ± 0.24	1.88

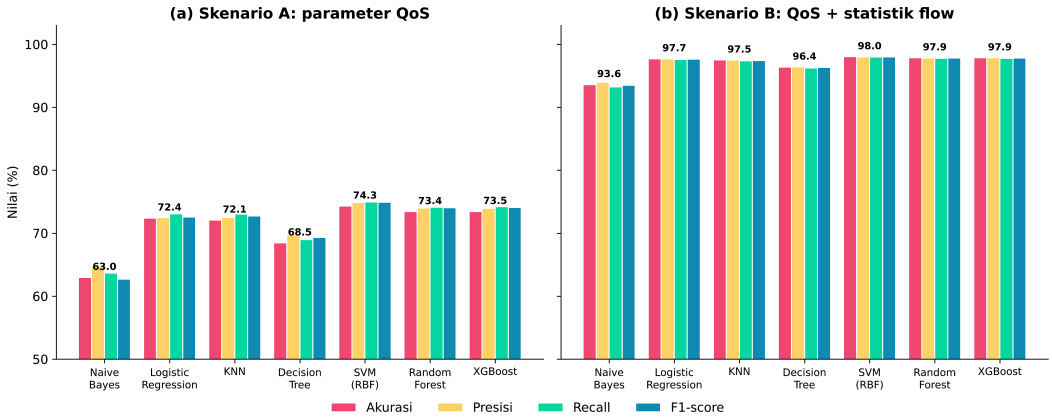


Figure 6. Accuracy, precision, recall, and F1-score of seven algorithms in (a) scenario A and (b) scenario B

The difference between test accuracy and the mean cross-validation accuracy does not exceed 0.5 points for any model, with standard deviations below 1 point. This consistency indicates that the models do not overfit and that the results do not depend on a particular data split. Adding flow statistics increases the accuracy of SVM by 23.7 percentage points and that of Naive Bayes by 30.6 points. Even a linear algorithm such as Logistic Regression achieves 97.70% in scenario B, indicating that the combined feature space is already almost linearly separable. In terms of computational cost, Naive Bayes, KNN, and Logistic Regression train in less than 0.1 s, SVM in 0.56 s, XGBoost in 1.88 s, and Random Forest in 4.89 s, so all models are light enough to be retrained periodically on a network monitoring server.

3.3 Per-Class Error Analysis

The SVM confusion matrices in Figure 7 show markedly different error patterns between the two scenarios. In scenario A, VoIP is recognized best with a recall of 88.1%, while Video Streaming is the most difficult class with a recall of 62.9%. As many as 18.9% of Video Streaming flows are misclassified as Web Browsing and 17.9% of Web Browsing flows are misclassified as Video Streaming. File Transfer is also wrongly predicted as Video Streaming in 20.0% of cases. Both pairs of classes have overlapping ranges of delay, jitter, and packet loss (Figure 3), so QoS parameters alone are not sufficient to separate them.

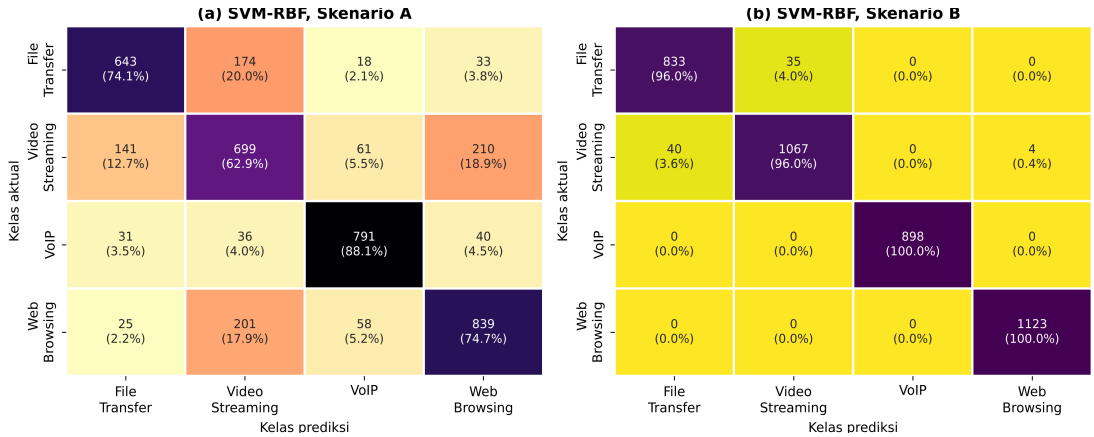


Figure 7. Confusion matrices of SVM-RBF in (a) scenario A and (b) scenario B; numbers in parentheses are percentages of the actual class

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*. Page 175
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

In scenario B, VoIP and Web Browsing are recognized perfectly (100% recall). The remaining errors occur only between File Transfer and Video Streaming, namely 35 and 40 flows, or about 4% of each class. Both classes carry large packets (an average of 1,141 bytes and 1,047 bytes) with long flow durations. Figure 8 summarizes the per-class F1-score for all models and shows that this difficulty pattern is consistent across all algorithms rather than being a weakness of a single model.

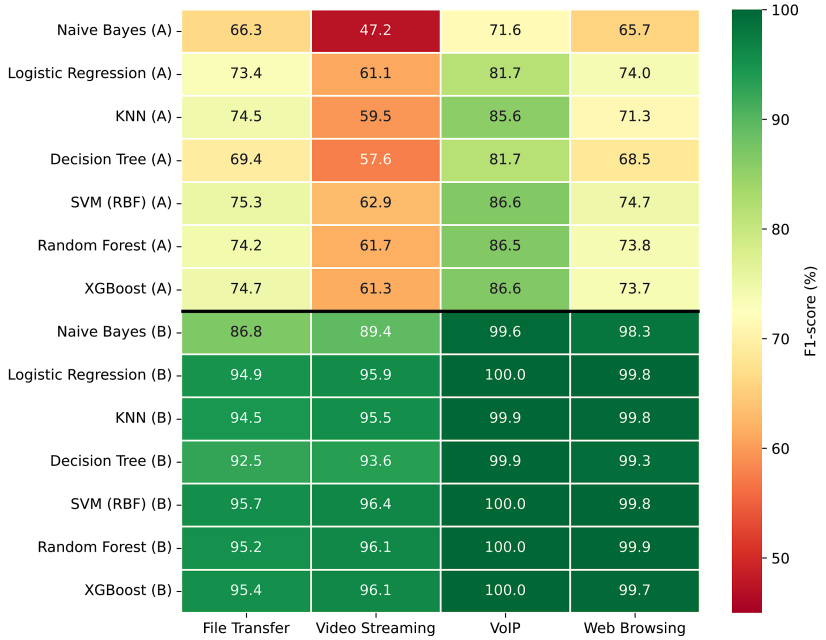


Figure 8. Per-class F1-score for each algorithm in scenario A (above the line) and scenario B (below the line)

3.4 Feature Importance

Random Forest in scenario A ranks throughput as the most influential QoS parameter (33.0%), followed by jitter (30.5%), delay (22.1%), and packet loss (14.4%), as shown in Figure 9(a). This ranking is consistent with the Kruskal-Wallis results in subsection 3.1. In scenario B, the top five features come from flow statistics, namely Flow Duration (19.5%), Mean Packet Size (18.8%), Total Bytes (15.7%), Total Packets (11.2%), and Forward Packets (9.2%). Jitter remains the most important QoS parameter (4.5%) and ranks above several flow statistics.

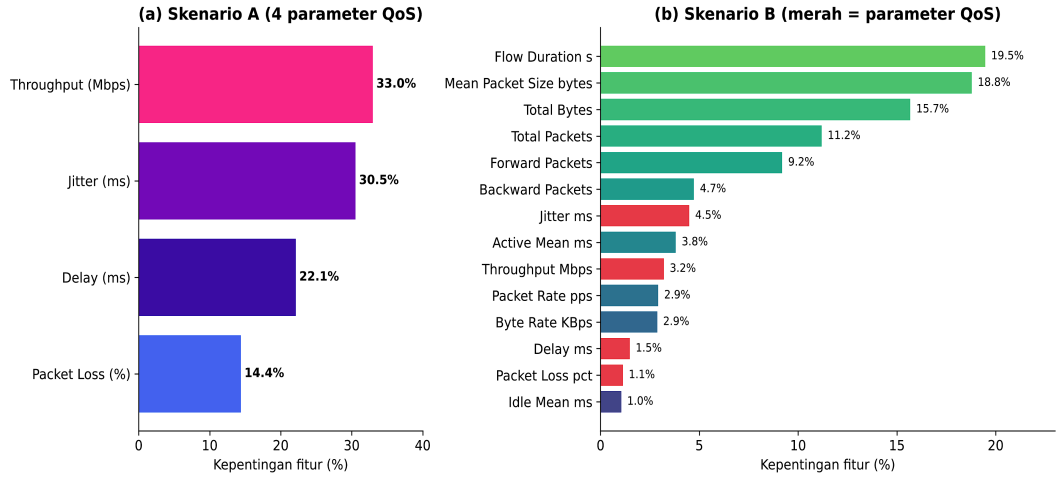


Figure 9. Random Forest feature importance in (a) scenario A and (b) scenario B; red bars indicate QoS parameters

3.5 Discussion

The results show that QoS parameters carry real but limited information about application identity. The accuracy of 74.3% in scenario A is far above random guessing for four classes (25%) and above the 64% SVM accuracy reported in a previous campus traffic classification study [27]. However, this figure is still below the 85% to 99% range reported in SDN studies that use complete flow features [2], [20]. This gap is reasonable because QoS parameters describe the network conditions experienced by a flow, whereas application identity is determined more by sender behavior, such as packet size and session duration.

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*.
This work is licensed under a Creative Commons Attribution 4.0 International License.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

The accuracy of 98.0% in scenario B is comparable to traffic classification studies based on classical machine learning and deep learning [3], [10], [11], [31], even though this study deliberately excluded ports and protocols. The finding that Random Forest, XGBoost, and SVM deliver almost equal performance is also in line with reports that ensemble and kernel models excel on tabular data [28], [32]–[34]. Transformer and pre-training models such as ET-BERT and YaTC offer high accuracy on encrypted traffic [8], [14], [15], but they demand large computational resources and their accuracy may decline on many-class and zero-day traffic [19]. SVM with a training time of 0.56 s and XGBoost with 1.88 s are more realistic for deployment on campus network devices.

The practical implications are threefold. First, VoIP can be recognized from its delay and jitter profile alone, so a router can quickly assign queue priority without reading packet payloads, complementing static QoS configurations such as those on Cisco routers [4]. Second, separating Video Streaming from Web Browsing and File Transfer requires flow statistics, so a monitoring system needs to record packet size and flow duration rather than QoS parameters only. Third, the feature importance analysis provides a basis for explaining model decisions, in line with the principles of Explainable Artificial Intelligence [41]; post-hoc methods such as SHAP [42] have already been used to make lightweight traffic classifiers interpretable [43], and such explanations can be integrated with network continuity mechanisms such as automated failover [7].

This study has several limitations. The dataset comes from real traffic observations in a single network environment, so the patterns found may not apply equally to networks with different topologies, capacities, and user profiles. The traffic classes are also limited to four applications and do not yet include online gaming, video conferencing, or IoT traffic. Validation on other institutional networks, testing on public encrypted datasets, evaluation against zero-day applications [19], and application to 5G and network slicing scenarios [22]–[24] are directions for future research.

4. CONCLUSION

This study demonstrates that QoS parameters significantly distinguish network traffic classes, with throughput and jitter as the strongest discriminators and packet loss as the weakest, as confirmed by both the Kruskal-Wallis test and Random Forest feature importance. SVM-RBF delivers the best performance in both scenarios, achieving 74.30% accuracy with the four QoS parameters alone and 98.02% accuracy after the QoS parameters are complemented by flow statistics, while Random Forest and XGBoost achieve almost equal performance (97.85%) and remain stable under 5-fold cross validation with standard deviations below one percentage point. VoIP can be recognized from QoS parameters alone with a recall of 88.1%, whereas Video Streaming, Web Browsing, and File Transfer require flow statistics such as flow duration and mean packet size to be separated reliably, and the remaining errors in the best scenario occur only between File Transfer and Video Streaming, which both carry large packets in long sessions. Because port and protocol attributes were removed, these results reflect genuine traffic behavior rather than memorized port numbers, which makes the approach suitable for encrypted traffic. This study therefore recommends combining QoS parameters and flow statistics, without relying on port numbers, as the basis of a traffic classification system for adaptive QoS management in campus and institutional networks, with lightweight models such as SVM or XGBoost that can be retrained in seconds. The main limitations are the use of a single network environment and only four application classes. Future research is suggested to validate the model on other networks and on public encrypted traffic datasets, to add application classes such as video conferencing, online gaming, and IoT, to evaluate robustness against zero-day applications, and to apply Explainable AI methods such as SHAP to explain model decisions to network administrators.

REFERENCES

[1] A. Azab, M. Khasawneh, S. Alrabaee, K.-K. R. Choo, and M. Sarsour, "Network traffic classification: Techniques, datasets, and challenges," *Digital Communications and Networks*, vol. 10, no. 3, pp. 676–692, 2024. https://doi.org/10.1016/j.dcan.2022.09.009

[2] D. Nuñez-Agurto, W. Fuertes, L. Marrone, and M. Macas, "Machine learning-based traffic classification in software-defined networking: A systematic literature review, challenges, and future research directions," *IAENG International Journal of Computer Science*, vol. 49, no. 4, 2022.

[3] Y.-F. Huang, C.-B. Lin, C.-M. Chung, and C.-M. Chen, "Research on QoS classification of network encrypted traffic behavior based on machine learning," *Electronics*, vol. 10, no. 12, Art. no. 1376, 2021. https://doi.org/10.3390/electronics10121376

[4] H. Hermansyah, A. Khaidar, N. Nurdin, and S. Kurnia, "Implementation of static routing and quality of service for optimization of network traffic management on Cisco routers," *Journal of Artificial Intelligence and Software Engineering*, vol. 5, no. 3, pp. 1222–1230, 2025.

[5] Hermansyah, Al-Khaidar, and Husni, "Quality of service-based analysis of internet network performance and the reliability of digital learning services in higher education," *Journal of International Multidisciplinary Research*, vol. 4, no. 10, pp. 10–25, 2026.

[6] I. S. N. Nisa, R. M. Saputro, T. F. Nugroho, and A. R. Lahitani, "Analisis quality of service (QoS) menggunakan standar parameter TIPHON pada jaringan internet berbasis Wi-Fi Kampus 1 Unjaya," *Teknomatika: Jurnal Informatika dan Komputer*, vol. 17, no. 1, pp. 1–9, 2024. https://doi.org/10.30989/teknomatika.v17i1.1307

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*. Page 177
This work is licensed under a Creative Commons Attribution 4.0 International License.

ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

[7] A. Khaidar, "Design and implementation of internet failover with automated email notification for network continuity," *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, vol. 5, no. 1, 2025.
[8] W. Dong, J. Yu, X. Lin, G. Gou, and G. Xiong, "Deep learning and pre-training technology for encrypted traffic classification: A comprehensive review," *Neurocomputing*, vol. 617, Art. no. 128444, 2025. https://doi.org/10.1016/j.neucom.2024.128444
[9] I. Akbari, M. A. Salahuddin, L. Ven, N. Limam, R. Boutaba, B. Mathieu, S. Moteau, and S. Tuffin, "A look behind the curtain: Traffic classification in an increasingly encrypted web," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 5, no. 1, Art. no. 4, 2021. https://doi.org/10.1145/3447382
[10] I. A. Alwhbi, C. C. Zou, and R. N. Alharbi, "Encrypted network traffic analysis and classification utilizing machine learning," *Sensors*, vol. 24, no. 11, Art. no. 3509, 2024. https://doi.org/10.3390/s24113509
[11] A. Antari, Y. Abo-Aisheh, J. Shamasneh, and H. I. Ashqar, "Network traffic classification using machine learning, transformer, and large language models," *arXiv preprint* arXiv:2503.02141, 2025.
[12] M. Shen, K. Ye, X. Liu, L. Zhu, J. Kang, S. Yu, Q. Li, and K. Xu, "Machine learning-powered encrypted network traffic analysis: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 791–824, 2023. https://doi.org/10.1109/COMST.2022.3208196
[13] J. Zhao, X. Jing, Z. Yan, and W. Pedrycz, "Network traffic classification for data fusion: A survey," *Information Fusion*, vol. 72, pp. 22–47, 2021. https://doi.org/10.1016/j.inffus.2021.02.009
[14] X. Lin, G. Xiong, G. Gou, Z. Li, J. Shi, and J. Yu, "ET-BERT: A contextualized datagram representation with pre-training transformers for encrypted traffic classification," in *Proceedings of the ACM Web Conference 2022 (WWW '22)*, 2022, pp. 633–642. https://doi.org/10.1145/3485447.3512217
[15] R. Zhao, M. Zhan, X. Deng, Y. Wang, Y. Wang, G. Gui, and Z. Xue, "Yet another traffic classifier: A masked autoencoder based traffic transformer with multi-level flow representation," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 4, 2023, pp. 5420–5427. https://doi.org/10.1609/aaai.v37i4.25674
[16] J. H. Kalwar and S. Bhatti, "Deep learning approaches for network traffic classification in the Internet of Things (IoT): A survey," *arXiv preprint* arXiv:2402.00920, 2024.
[17] T. Shapira and Y. Shavitt, "FlowPic: A generic representation for encrypted traffic classification and applications identification," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1218–1232, 2021. https://doi.org/10.1109/TNSM.2021.3071441
[18] G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescapé, "DISTILLER: Encrypted traffic classification via multimodal multitask deep learning," *Journal of Network and Computer Applications*, vol. 183–184, Art. no. 102985, 2021. https://doi.org/10.1016/j.jnca.2021.102985
[19] L. Yang, A. Finamore, F. Jun, and D. Rossi, "Deep learning and zero-day traffic classification: Lessons learned from a commercial-grade dataset," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4103–4118, 2021. https://doi.org/10.1109/TNSM.2021.3122940
[20] R. H. Serag, M. S. Abdalzaher, H. A. E. A. Elsayed, M. Sobh, M. Krichen, and M. M. Salim, "Machine-learning-based traffic classification in software-defined networks," *Electronics*, vol. 13, no. 6, Art. no. 1108, 2024. https://doi.org/10.3390/electronics13061108
[21] A. M. Eldhai, M. Hamdan, A. Abdelaziz, I. A. T. Hashem, S. F. Babiker, M. N. Marsono, M. Hamzah, and N. Z. Jhanjhi, "Improved feature selection and stream traffic classification based on machine learning in software-defined networks," *IEEE Access*, vol. 12, pp. 34141–34159, 2024.
[22] R. Dangi and P. Lalwani, "Feature selection based machine learning models for 5G network slicing approximation," *Computer Networks*, vol. 237, Art. no. 110093, 2023. https://doi.org/10.1016/j.comnet.2023.110093
[23] N. A. Mohammedali, T. Kanakis, A. Al-Sherbaz, and M. O. Agyeman, "Traffic classification using deep learning approach for end-to-end slice management in 5G/B5G," in *13th International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, 2022. https://doi.org/10.1109/ICTC55196.2022.9952446
[24] K. B. Ajeyprasaath and P. Vetrivelan, "Machine learning based classifiers for QoE prediction framework in video streaming over 5G wireless networks," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 1919–1939, 2023. https://doi.org/10.32604/cmc.2023.036013
[25] L. Wang, M. Yang, B. Li, and Z. Yan, "A method of combining traffic classification and traffic prediction based on machine learning in wireless networks," *arXiv preprint* arXiv:2304.01590, 2023.
[26] A. Shahraki, M. Abbasi, A. Taherkordi, and A. D. Jurcut, "A comparative study on online machine learning techniques for network traffic streams analysis," *Computer Networks*, vol. 207, Art. no. 108836, 2022. https://doi.org/10.1016/j.comnet.2022.108836
[27] P. Adytia, Wahyuni, K. Sussolaikah, and Y. Satria, "Klasifikasi penggunaan data trafik internet menggunakan algoritma support vector machine," *J-ICON: Jurnal Komputer dan Informatika*, vol. 11, no. 1, pp. 96–102, 2023. https://doi.org/10.35508/jicon.v11i1.10039
[28] A. Nurdiyansah, D. Robiul R, Sururi, and N. Sujana, "Analisis SelectKBest pada klasifikasi trafik VPN menggunakan random forest dan SVM," *Terapan Informatika Nusantara (TIN)*, vol. 6, no. 8, pp. 1533–1541, 2026. https://doi.org/10.47065/tin.v6i8.9136
[29] Y. B. Gudare, Y. P. Bria, and F. Tedy, "Penerapan algoritma random forest untuk analisis dan deteksi dini serangan siber pada lalu lintas jaringan," *Prosiding Seminar Nasional KONSTELASI*, vol. 3, no. 1, pp. 100–113, 2026.
[30] A. H. Nurmakhlufi and E. Zuliarso, "Penerapan machine learning dalam analisis pola penggunaan bandwidth pada provider internet," *Jurnal Inovtek Polbeng – Seri Informatika*, vol. 10, no. 3, pp. 1331–1341, 2025.
[31] N. F. Hasani, "Network traffic classification using machine learning techniques: An applied flow-based study," *Academia Open*, vol. 12, no. 1, 2027 (published online 2026). https://doi.org/10.21070/acopen.12.2027.15227
[32] L. Grinsztajn, E. Oyallon, and G. Varoquaux, "Why do tree-based models still outperform deep learning on typical tabular data?," in *Advances in Neural Information Processing Systems 35 (NeurIPS 2022), Datasets and Benchmarks Track*, 2022, pp. 507–520.

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*. Page 178
This work is licensed under a Creative Commons Attribution 4.0 International License.

ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 7, No. 4, August 2026, Page 170-179
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v7i4.10932

[33] R. Shwartz-Ziv and A. Armon, "Tabular data: Deep learning is not all you need," *Information Fusion*, vol. 81, pp. 84–90, 2022. https://doi.org/10.1016/j.inffus.2021.11.011
[34] A. Khaidar, N. Nurdin, F. Fajriana, T. Taufiq, and D. Hamdhana, "Classification analysis of single tuition fees using the random forest method with k-fold cross validation," *Journal of Applied Informatics and Computing*, vol. 10, no. 1, pp. 125–133, 2026.
[35] N. C. Ramadani, I. Tahyudin, and A. S. Barkah, "Perbandingan algoritma support vector machine, decision tree, dan logistic regression pada analisis sentimen ulasan aplikasi Netflix," *Jurnal Nasional Teknologi dan Sistem Informasi (TEKNOSI)*, vol. 10, no. 2, pp. 110–117, 2024. https://doi.org/10.25077/TEKNOSI.v10i2.2024.110-117
[36] R. Oktafiani and R. Rianto, "Perbandingan algoritma support vector machine (SVM) dan decision tree untuk sistem rekomendasi tempat wisata," *Jurnal Nasional Teknologi dan Sistem Informasi (TEKNOSI)*, vol. 9, no. 2, pp. 113–121, 2023. https://doi.org/10.25077/TEKNOSI.v9i2.2023.113-121
[37] S. Kapoor and A. Narayanan, "Leakage and the reproducibility crisis in machine-learning-based science," *Patterns*, vol. 4, no. 9, Art. no. 100804, 2023. https://doi.org/10.1016/j.patter.2023.100804
[38] G. James, D. Witten, T. Hastie, R. Tibshirani, and J. Taylor, *An Introduction to Statistical Learning: With Applications in Python*. Cham, Switzerland: Springer, 2023. https://doi.org/10.1007/978-3-031-38747-0
[39] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.
[40] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, pp. 785–794. https://doi.org/10.1145/2939672.2939785
[41] Al-Khaidar, *Explainable Artificial Intelligence (XAI): Teori, Metode, dan Implementasi*. CV. Madza Media, 2026.
[42] S. M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," in *Advances in Neural Information Processing Systems 30 (NIPS 2017)*, 2017, pp. 4765–4774.
[43] M. M. S. Ghaleb, M. Hamdan, A. Y. Barnawi, M. Gambo, A. Danasabe, S. Bello, and A. Habib, "Explainable AI for lightweight network traffic classification using depthwise separable convolutions," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 908–920, 2025. https://doi.org/10.1109/OJCS.2025.3576495

Copyright © 2026 The Author(s). Published by *Forum Kerjasama Pendidikan Tinggi*.
This work is licensed under a Creative Commons Attribution 4.0 International License.