Sophisticated Machine Learning Methods for Reliable Network Traffic Data Categorization Models

Karthikeyan Kaliyaperumal[1], Rajendran Bhojan[2], Mohsen Aghaeiboorkheili[2*]

[1]IoT- HH Campus, Ambo University, Ethiopia
[2] School of Mathematics & Computer Science,
Papua New Guinea University of Technology, Lae, Papua New Guinea

*Corresponding Author: mohsen.aghaeiboorkheili@pnguot.ac.pg

Abstract: Network traffic classification is critical for efficient network management, resource optimization, and security enhancement. The complexity of modern traffic patterns, driven by increasing user demands and diverse applications, poses challenges for traditional methods. This study explores advanced machine learning techniques to address these challenges, focusing on precise classification to improve network performance and detect anomalies effectively. The main key with machine learning such as Support Vector Machines (SVM), K-Nearest Neighbours (KNN), and Logistic Regression were evaluated for their categorization of the capabilities. SVM achieved an accuracy of 99.30%, while KNN and Logistic Regression excelled with accuracies of 99.92%. These results highlight the robustness and adaptability of these models to dynamic and complex network traffic scenarios. Accurate traffic classification facilitates informed decision-making in bandwidth allocation, congestion control, and service prioritization. Furthermore, these scalable models can adapt to evolving network environments and support data-intensive applications. This research demonstrates the transformative potential of machine learning in advancing network operations, offering a foundation for future innovations in intelligent, efficient, and secure network management.

Keywords: Network Traffic Classification, SVM, K-NN, Network Security, Resource Optimization, Traffic Pattern Analysis.

1. INTRODUCTION

Efficient network traffic classification is critical to modern network management, ensuring operational efficiency, optimal resource utilization, and enhanced security. The rapid growth of user demands and the increasing diversity of applications and services have introduced unprecedented complexity to traffic patterns. Traditional network management approaches often struggle to address these dynamic and intricate patterns, necessitating the development of more advanced methods for classification and forecasting.

This research focuses on leveraging state-of-the-art machine learning techniques to address the challenges of network traffic classification. Machine learning has proven highly effective in identifying patterns, adapting to diverse scenarios, and offering robust classification performance. In this study, three key algorithms such as Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Logistic Regression are evaluated for their ability to accurately classify network traffic. These models were chosen for their established strengths in pattern recognition and adaptability to evolving network conditions.

The study demonstrates that SVM achieves an accuracy of 99.30%, while both KNN and Logistic Regression reach an impressive 99.92% (Goyal, et al.). These results underscore the effectiveness of these machine learning models in managing the dynamic and unpredictable nature of network traffic. By accurately classifying traffic, these models enable network administrators to make informed decisions about bandwidth allocation, congestion management, and service prioritization, ultimately improving network performance and security (Goyal, et al.).

Sophisticated Machine Learning Methods for Reliable Network Traffic Data Categorization Models
Karthikeyan Kaliyaperumal, Rajendran Bhojan, Mohsen Aghaeiboorkheili | 2 (2) : 144 - 152 | Received: 29/06/2025 | Reviewed: 06/08/2025 | Accepted: 02/09/2025 |
DOI: https://doi.org/10.63900/cm3v2t81

In addition to classification, accurate network traffic forecasting is essential for proactive management and resource optimization. Advanced models, such as Enhanced Autoregressive Integrated Moving Average (ARIMA), play a pivotal role in predicting future traffic patterns. By incorporating historical data, time series analysis, and external influencing factors, Enhanced ARIMA models can capture seasonal trends and dynamic shifts in traffic, achieving high levels of forecasting accuracy.

This research highlights the transformative potential of combining machine learning techniques with advanced statistical models to revolutionize network management. These approaches provide scalable and adaptable solutions to meet the demands of modern, data-intensive environments. By addressing challenges such as non-linear traffic dynamics, resource constraints, and security risks, this study lays the foundation for intelligent, efficient, and secure network operations in an increasingly interconnected world.

This paper is organized as follows as Section 2 reviews related work in network traffic classification, emphasizing the evolution of machine learning techniques and their application in modern network environments (Goyal, et al.). Section 3 explores the challenges of traffic classification, including the complexities of dynamic traffic patterns, resource constraints, and security vulnerabilities in real-world scenarios. Section 4 outlines the methodology, covering data collection, preprocessing, feature selection, and the design of classification models using advanced machine learning techniques. Section 5 presents experimental results, analyzing the performance of the proposed models and comparing their accuracy and adaptability to existing approaches. Finally, Section 6 concludes the study by summarizing the findings and proposing future research directions for enhancing network traffic classification in increasingly complex digital ecosystems (Ouaissa, et al., 2025).

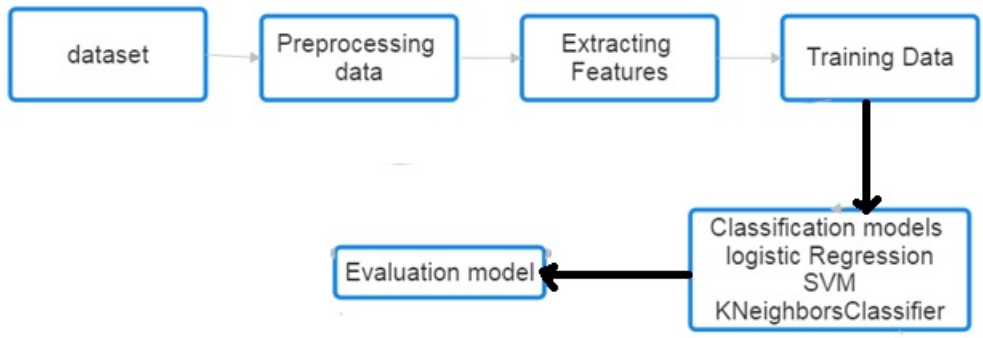

Figure – 1 Research Flow of Network Traffic Model

Figure – 1 is shown outlines a simplified workflow for a network traffic classification system using machine learning techniques. The process begins with the collection of raw data, typically in the form of network traffic logs containing attributes such as packet size, protocols, and flow durations. The data undergoes preprocessing to remove inconsistencies, handle missing values, and normalize the information, ensuring it is ready for feature extraction (Rana, Hossain, & Li, 2025). Relevant features are then extracted to capture critical characteristics of the traffic, such as protocol type, packet length, and flow statistics. These extracted features are split into training and testing datasets for model building.

The classification step involves training three machine learning models: Logistic Regression, Support Vector Machine (SVM), and K-Neighbors Classifier. Logistic Regression is effective for binary classification tasks, distinguishing between categories like normal and suspicious traffic. SVM is a robust classifier capable of handling complex decision boundaries in high-dimensional feature spaces. KNeighbors Classifier, a similarity-based algorithm, assigns labels based on the majority class among the closest data points. These models are trained using the training dataset to ensure they can accurately classify network traffic (Detection).

Finally, the trained models are evaluated using metrics such as accuracy, precision, recall, and F1 score to assess their performance and reliability in real-world scenarios. The updated diagram emphasizes classification-focused workflows by removing forecasting models and linking the classification outputs directly to evaluation. This end-to-end workflow provides a systematic and efficient approach to classify network traffic into predefined categories, enabling network administrators to make informed decisions about resource allocation, anomaly detection, and security management (Goyal, et al.).

2. LITERATURE SURVEY

Network traffic classification is a critical aspect of modern network management, facilitating efficient resource allocation, Quality of Service (QoS), and enhanced security. Over time, various classification algorithms have been developed to address the increasing complexity of traffic patterns. These algorithms range from traditional probabilistic models to advanced machine learning techniques, each contributing significantly to improving the accuracy and adaptability of traffic classification systems. Naive Bayes Classifier, for example, is a probabilistic model that assumes feature independence. Its computational efficiency and simplicity make it suitable for real-time traffic analysis, particularly in packet-level and flow-level classification scenarios.

Support Vector Machines (SVM) have been widely adopted for both linear and non-linear classification tasks. Known for their effectiveness in separating normal and anomalous traffic, SVMs are particularly valuable in intrusion detection systems due to their ability to handle high-dimensional feature spaces. Decision Trees and their ensemble extension, Random Forests, offer intuitive classification mechanisms. While Decision Trees provide transparency in rule interpretation, Random Forests enhance robustness and excel in managing complex, noisy datasets, commonly observed in network traffic.

Extreme Learning Machine Algorithms generally have a single layer hidden nodes whereby weights are assigned randomly in connecting. In order to reduce the computational complexity, Improved Error Reduced Extreme Learning Machine methodology was proposed as enhancement and also handle huge volumes of data. The results shown prove good improvement over traditional ELMs (Rajendran & Saravanan, Improved Error Reduced Extreme Learning Machine (IERELM) Classifier for Big Data Analytics, 2017, February; Vol 95; No 4;).

K-Nearest Neighbors (KNN) further contributes to network traffic classification by leveraging similarity measures in feature vectors. Its simplicity and dynamic adaptability make it reliable for diverse traffic scenarios. Neural Networks, particularly deep learning architectures like Convolutional Neural Networks (CNNs), have gained traction in recent years. CNNs excel in extracting spatial and temporal features, making them ideal for analyzing packet headers and traffic sequences. Logistic Regression, a binary classification algorithm, stands out for its straightforward implementation and efficiency in classifying traffic into normal versus suspicious categories. Bayesian Networks, with their probabilistic reasoning capabilities, model relationships between network features, offering strong anomaly detection capabilities.

Ensemble learning methods, including AdaBoost and Gradient Boosting, have been employed to enhance classification performance. These methods combine predictions from multiple classifiers to improve overall accuracy and robustness, making them ideal for network intrusion detection systems (Mohan, Sekhar, & Gupta, 2024). Recent advancements in machine learning have focused on integrating multiple algorithms, such as SVM, KNN, and Logistic Regression, to achieve classification accuracies exceeding 99% in real-world scenarios (Mohan, Sekhar, & Gupta, 2024). Furthermore, the incorporation of advanced forecasting models, such as Enhanced ARIMA, has demonstrated success in predicting traffic trends, addressing challenges posed by evolving and dynamic traffic patterns (Latifa, Ameni, Asma, & ribi, 2024).

A model developed on network intrusion detection using high performance deep neural networks proposed exhaustively evaluated the enhanced NSL-KDD dataset, giving a robust solution of ever evolving cyber threats (Rajendran & Saravanan, Big Data Analysis on Network Intrusion Detection using High Performance Deep Neural Networks, 2025, January;)

These research efforts underscore the transformative potential of machine learning and ensemble techniques in network traffic classification (Mohan, Sekhar, & Gupta, 2024). By combining computational efficiency, robustness, and adaptability, these methods address the challenges of increasingly complex and data-intensive network environments, ensuring secure and efficient operations while paving the way for future innovations in network management.

3. METHODOLOGY

The dataset for this research is collected using Wireshark, a widely-used tool for network protocol analysis. Network traffic data is gathered over six months during three specific time periods: morning, lunch hours, and afternoon (5 PM). The resulting dataset comprised approximately 50,000 entries and included attributes such as traffic volume, packet rates, and protocol types. The raw data is stored in formats like CSV and ZIP for ease of preprocessing and analysis. This comprehensive dataset served as the foundation for training and testing the classification and forecasting models.

Data preprocessing is critical to ensure the quality and usability of the collected dataset. Key steps included data cleaning, which involved removing duplicates, handling missing values, and correcting inconsistencies. Data transformation is carried out to aggregate data into meaningful time intervals (e.g., hourly or daily), normalize values, and handle outliers. Finally, feature extraction is performed to identify and extract relevant attributes such as traffic volume, packet rates, and protocol types. These steps optimized the dataset for the training of machine learning models.

The research employed advanced machine learning algorithms for traffic classification, including Support Vector Machines (SVMs), Logistic Regression, and K-Nearest Neighbors (KNN). SVMs were enhanced with a feature-weighted-degree (FWD-SVM) kernel to reduce the influence of weakly correlated and redundant features. Logistic Regression is applied to binary classification tasks, distinguishing between normal and malicious traffic, while KNN classified data points based on the majority class among their nearest neighbors in the feature space and the models were evaluated using metrics like accuracy, precision, recall, and F1 score for classification, Experiments were conducted under various network scenarios, including dynamic traffic patterns, peak usage times, and anomalous events resource allocation and detect security threats. The comprehensive methodology ensured robust and. These experiments assessed the adaptability of the models and their ability to optimize accurate models capable of addressing modern network management challenges. The Support Vector Machines (SVMs) with the enhanced feature-weighted-degree kernel can be expressed as:

$$\min \frac{1}{2}\|w\|^2 \quad \text{subject to} \quad y_i\,(w \cdot x_i + b) \geq 1,\ \forall i \tag{1}$$

where the kernel function K (xi, xj) is defined as:

$$K(x_i, x_j) = f_t \cdot (x_i \cdot x_j) \tag{2}$$

with ft representing feature importance calculated via information gain. This enhanced kernel ensures that features with higher classification importance are given more weight, improving overall model accuracy and robustness in handling network traffic data and Logistic Regression was employed for binary classification tasks, such as distinguishing between normal and malicious traffic. The model predicts the probability P (y = 1 | x) using this algorithm is particularly effective for tasks with clear binary outcomes and provides interpretable results, making it a reliable choice for identifying malicious traffic in network data. Its simplicity and efficiency make it well-suited for real-time classification which is define as

$$P(y = 1 \mid x) = \frac{1}{1 + e^{-(w \cdot x + b)}}. \tag{3}$$

and KNN classified traffic data based on similarity in feature space. For a given data point *x*, the Euclidean distance to its neighbors is calculated where xj and xi, j are the j-th features of x and xi, respectively. The data point is assigned the label of the majority class among its k nearest neighbors.

$$d(x, x_i) = \sqrt{\sum_{j=1}^{m} (x_j - x_{i,j})^2} \tag{4}$$

KNN is effective for locally smooth decision boundaries, though its performance depends on careful hyperparameter tuning and feature scaling for computer network classifications.

4. MODEL EVALUATION

The models are evaluated using the following metrics for accuracy where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives as follows as

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \tag{5}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}. \tag{6}$$

$$\text{F1 Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}. \tag{7}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{8}$$

5. EXPERIMENTAL RESULTS

Protocols play a vital role in network traffic classification within local area networks (LANs), significantly influencing traffic nature and optimization (Vajjhala & Strang, 2025). UDP is heavily used for quick, connectionless communication, often in time-sensitive applications like video streaming and DNS lookups, while TCP ensures reliable, connection-oriented data transmission for resource-intensive applications such as HTTP and email. Packet length analysis, with an average of ~1400 bits, provides insights into client-server and server-client communication, enabling the distinction between real-time and bulk data transfers. Application-specific protocols like HTTP/HTTPS, DNS, SMTP, and streaming protocols further refine traffic categorization. Accurate protocol analysis supports resource allocation, congestion control, anomaly detection, and bandwidth prioritization, forming a robust foundation for leveraging machine learning models in dynamic and complex network environments.

Figure – 2 the bar chart shown that distribution of network traffic across various protocols in a local area network (LAN). ARP is the most frequent protocol, exceeding 2000 occurrences, highlighting its role in resolving IP to MAC addresses, followed by DNS, which indicates frequent domain name resolution requests.

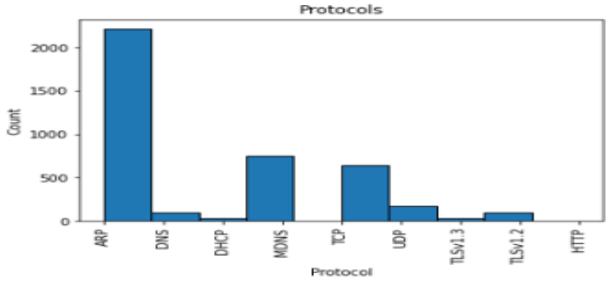

Figure – 2 List of Protocols

Moderate usage of DHCP and MDNS suggests dynamic IP assignment and local name resolution, respectively. TCP shows significant usage, reflecting its role in reliable communication for applications like HTTP and email, while UDP, though lower, supports lightweight and latency-sensitive applications such as video streaming. TLS and HTTP have relatively low occurrences, indicating limited secure traffic or browsing activity. The chart reveals a mix of communication, resolution, and secure protocols, offering insights for optimizing resource allocation and enhancing network security.

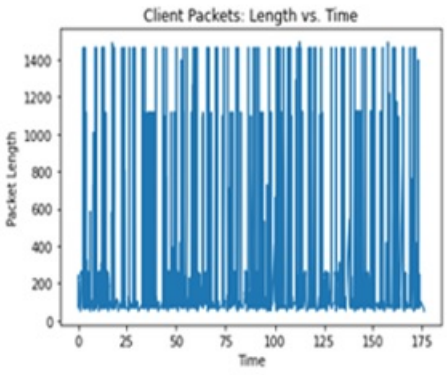

Figure – 3 (a) Client Packets

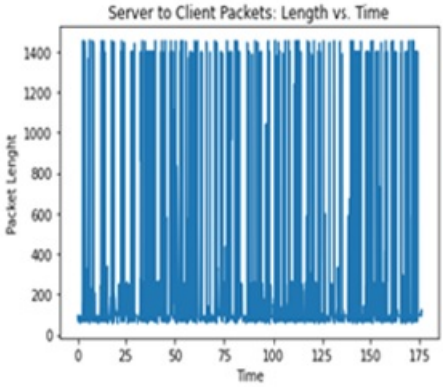

Figure – 3 (b) Server to Client Packets

Figure 3(a) illustrates the relationship between packet length and time for client-to-server transmissions in a local area network (LAN). The packet lengths range from 200 bits to 1400 bits, with frequent occurrences of shorter packets, indicating lightweight operations such as DNS lookups. Occasional spikes to the maximum packet length (~1400 bits) suggest data-heavy operations like file uploads. In contrast, Figure 3(b) represents server-to-client transmissions, where packets also range between 200 bits and 1400 bits. However, server packets exhibit a higher frequency of maximum-length packets, reflecting bulk data transfers or file downloads. Shorter packets interspersed with larger ones likely correspond to acknowledgments or control messages.

5.1 Network Traffic Classification Analysis

The Logistic Regression model (Xiaonan, Yon, Zhewen, & Kaiyuan, 2019) achieved an impressive overall accuracy of 99.92% in classifying six network traffic types: File Sharing, Instant Message, Video, Voice OverIP, Email, and P2P. Most classes, including Instant Message, Video, Voice Over IP, and Email, demonstrated perfect precision, recall, and F1-scores, reflecting flawless classification.

```
Confusion matrix:
 [[  46    0    0    0    0    0]
 [   0 1677    0    0    0    0]
 [   0    0    7    0    0    0]
 [   0    0    0    4    0    0]
 [   0    0    0    0  840    0]
 [   2    0    0    0    0   30]]
                precision    recall  f1-score   support

   FileSharing       0.96      1.00      0.98        46
InstantMessage       1.00      1.00      1.00      1677
         Video       1.00      1.00      1.00         7
   VoiceOverIP       1.00      1.00      1.00         4
         email       1.00      1.00      1.00       840
           p2p       1.00      0.94      0.97        32

   avg / total       1.00      1.00      1.00      2606

   Accuracy Score: 0.9992325402916347
```

Figure – 4 Logistic Regression Model

File Sharing achieved high scores with a precision of 0.96 and an F1-score of 0.98, while P2P traffic showed minor misclassification, with a recall of 0.94 and an F1-score of 0.97. The confusion matrix indicates

only two misclassified instances, emphasizing the model's reliability. This exceptional performance underscores the suitability of Logistic Regression for network traffic classification, particularly in datasets with well-defined and distinct traffic categories, providing robust support for efficient network management and security (Goyal, et al.).

```
Confusion matrix:
 [[  42    4    0    0    0    0]
 [   0 1677    0    0    0    0]
 [   0    0    7    0    0    0]
 [   0    0    0    4    0    0]
 [   0   14    0    0  826    0]
 [   0    0    0    0    0   32]]
                precision    recall  f1-score   support

    FileSharing       1.00      0.91      0.95        46
InstantMessage       0.99      1.00      0.99      1677
         Video       1.00      1.00      1.00         7
   VoiceOverIP       1.00      1.00      1.00         4
         email       1.00      0.98      0.99       840
           p2p       1.00      1.00      1.00        32

   avg / total       0.99      0.99      0.99      2606

 Acc= 0.9930928626247122
```

Figure – 5 Support Vector Machine (SVM) model

The Figure – 5 shown that Support Vector Machine (SVM) model [30] demonstrated outstanding performance in classifying six types of network traffic—File Sharing, Instant Message, Video, Voice OverIP, Email, and P2P—achieving an overall accuracy of 99.30%. Most traffic types, including Instant Message, Video, Voice OverIP, and P2P, showed near-perfect precision, recall, and F1-scores, indicating exceptional classification accuracy. File Sharing and Email traffic had minor misclassifications, with four and 14 instances misclassified, respectively, resulting in slightly lower recall scores of 0.91 and 0.98. Despite these minor errors, the model's high precision and recall across all categories highlight its robustness and effectiveness in managing well-defined network environments. These results underscore SVM's suitability for efficient resource allocation and enhanced network security in diverse and complex traffic.

Figure 6 visualized that the K-Nearest Neighbors (KNN) model achieved an impressive overall accuracy of 99.92% in classifying six types of network traffic: File Sharing, Instant Message, Video, Voice OverIP, Email, and P2P. Most traffic types, including Instant Message, Video, Voice OverIP, and Email, demonstrated perfect precision, recall, and F1-scores, reflecting flawless classification. File Sharing showed high recall (1.00) with a precision of 0.96 and F1-score of 0.98, while P2P traffic had minor misclassifications, with two instances incorrectly classified, resulting in a recall of 0.94 and F1-score of 0.97. The model's ability to handle distinct traffic categories with minimal errors highlights its robustness and suitability for network traffic classification.

```
Confusion matrix:
 [[  46    0    0    0    0    0]
 [   0 1677    0    0    0    0]
 [   0    0    7    0    0    0]
 [   0    0    0    4    0    0]
 [   0    0    0    0  840    0]
 [   2    0    0    0    0   30]]
                precision    recall  f1-score   support

    FileSharing       0.96      1.00      0.98        46
InstantMessage       1.00      1.00      1.00      1677
         Video       1.00      1.00      1.00         7
   VoiceOverIP       1.00      1.00      1.00         4
         email       1.00      1.00      1.00       840
           p2p       1.00      0.94      0.97        32

   avg / total       1.00      1.00      1.00      2606

   Accuracy Score: 0.9992325402916347
```

Figure 6 K-Nearest Neighbors (KNN) model

This performance confirms KNN as a reliable tool for efficient network management, resource allocation, and enhancing network security (Goyal, et al.).

Table 1: Comparison of Logistic Regression, SVM, and KNN Models

Model	Overall Accuracy	Perfectly Classified Traffic Types	Strengths
Logistic Regression	99.92%	Instant Message, Video, Voice OverIP, Email	High accuracy, simple implementation, reliable for well-defined datasets, suitable for network security and resource management.
Support Vector Machine (SVM)	99.30%	Instant Message, Video, Voice OverIP, P2P	Exceptional handling of complex traffic patterns, robust precision and recall, effective in diverse environments.
K-Nearest Neighbors (KNN)	99.92%	Instant Message, Video, Voice OverIP, Email	Reliable for distinct traffic categories, adaptable to well-separated datasets, suitable for efficient network security.

Table 1 show that Logistic Regression and KNN both achieved the highest accuracy of 99.92%, outperforming SVM, which had an accuracy of 99.30%. All models demonstrated excellent performance on Instant Message, Video, Voice OverIP, and Email traffic (Joice & Selvi, 2025). Logistic Regression and KNN had minimal misclassifications (2 P2P instances each), whereas SVM showed higher misclassification rates, particularly for File Sharing and Email traffic. While Logistic Regression and KNN are better suited for datasets with clearly defined traffic categories, SVM excels in handling complex and diverse traffic patterns. This comparison highlights the strengths and weaknesses of each model, aiding in selecting the most appropriate approach for specific network traffic classification needs (Goyal, et al.).

6. CONCLUSIONS

This research demonstrates the transformative potential of advanced machine learning techniques for network traffic classification, addressing the challenges posed by modern, dynamic traffic patterns. The models evaluated—Logistic Regression, Support Vector Machines (SVM), and K-Nearest Neighbors (KNN)—exhibited exceptional classification performance, achieving overall accuracies of 99.92% for Logistic Regression and KNN, and 99.30% for SVM. Logistic Regression and KNN proved particularly effective for datasets with clearly defined traffic categories, while SVM excelled in handling complex and diverse traffic patterns. All three models showed outstanding results in classifying traffic types such as Instant Message, Video, VOIP, and Email, with minimal misclassifications observed in File Sharing and P2P traffic. These findings highlight the robustness and adaptability of these algorithms for real-world applications, enabling efficient resource allocation, congestion control, and anomaly detection. Furthermore, the integration of advanced preprocessing, feature extraction, and evaluation metrics underscores the importance of systematic workflows in achieving reliable classification outcomes.

The research underscores the critical role of machine learning in advancing network management, offering scalable solutions to meet the demands of data-intensive environments while ensuring security and operational efficient (Goyal, et al.). Future work can focus on enhancing model performance by incorporating hybrid models, optimizing feature selection, and addressing evolving traffic patterns in increasingly complex networks. This study provides a robust foundation for leveraging machine learning in network management, fostering innovation, and supporting intelligent and secure network operations.

REFERENCES

Detection, H. S. (n.d.). Text and Social Media Analytics for Fake News and Hate Speech Detection.

Goyal, D., Pratap, B., Gupta, S., Raj, S., Agrawal, R. R., & Kishor, I. (n.d.). Recent Advances in Sciences, Engineering, Information Technology & Management: Proceedings of the 6th International Conference "Convergence2024" Recent Advances in Sciences, Engineering, Information Technology & Management, April 24–25, 2024, Jaipur, India.

Joice, C. S., & Selvi, M. (2025). Pedagogical Revelations and Emerging Trends.

Latifa, G., Ameni, M., Asma, R., & ribi, K. (2024). Advanced Predictive Modeling For Enhancing Traffic Forecasting in Emerging Cellular Networks. *15th International Conference in Network of the Future.* Castelldefels, Spain.

Mane, D., Kaliyaperumal, K., Khurram, S., Regin, R., Aarthi, R., & Gawish, A. (2021). Brain Tumor Analysis Using Advanced Textural Feature Extraction Algorithm. *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, (pp. 1635–1640).

Mohan, R. J., Sekhar, V. C., & Gupta, V. M. (2024). *Algorithms in Advanced Artificial Intelligence: ICAAAI-2023.* CRC Press.

Oruganti, S. K., Karras, D., Thakur, S., Chaithanya, J. K., Metta, S., & Lathigara, A. (2025). Digital Transformation and Sustainability of Business. *Digital Transformation and Sustainability of Business*. CRC Press.

Ouaissa, M., Ouaissa, M., Lamaazi, H., Slimani, K., Khan, I. R., & Sundaravadivazhagan, B. (2025). Machine Learning for Radio Resource Management and Optimization in 5G and Beyond.

Rajendran, B., & Saravanan, V. (2017, February; Vol 95; No 4;). Improved Error Reduced Extreme Learning Machine (IERELM) Classifier for Big Data Analytics. *Journal of Theoritical and Applied Information Technology*, 840 - 848.

Rajendran, B., & Saravanan, V. (2025, January;). Big Data Analysis on Network Intrusion Detection using High Performance Deep Neural Networks. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 167 - 176.

Rana, M. S., Hossain, M. M., & Li, F. (2025). Comparative analysis of machine learning models for predicting the compressive strength of ultra-high-performance steel fiber reinforced concrete. *Journal of Engineering Research*. doi:https://doi.org/10.1016/j.jer.2025.01.004

Vajjhala, N. R., & Strang, K. D. (2025). *Cybersecurity in Knowledge Management: Cyberthreats and Solutions.* CRC Press.

Xiaonan, Z., Yon, H., Zhewen, T., & Kaiyuan, S. (2019). Loristic Regression Model Optimization and Case Analysis. *7th International Conference on Computer Science and Network Technology (ICCSNT).* Dalian, China.