AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

SmartNet AI: A Unified Framework for Cyber Threat Detection and Network Performance Optimization

P. Sravan Kumar[1], Kancharla Teja Malleshwari[1], Ragam Poojitha[1], Malyala Hasini[1], Devanaka Bharath Kumar[1]

[1]Department of Electronics and Communication Engineering, [1]Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, 501510, Telangana, India.

ABSTRACT

The advancement of 6G networks brings increasing requirements for secure, flexible, and high-efficiency communication infrastructures. Traditional network monitoring and intrusion detection methods, which rely heavily on fixed rules and manual analysis, are no longer adequate for handling the growing complexity and scale of modern network systems. These approaches often struggle to identify sophisticated cyber threats and fail to maintain optimal performance in highly dynamic environments. This study introduces a Machine Learning (ML)-based framework grounded in Classification and Regression Tree (CART) methodology, designed for dual-function analysis encompassing both attack detection and throughput estimation. The proposed system incorporates various ML algorithms, including Support Vector Machine (SVM), k-Nearest Neighbors (KNN), and a novel Tree-based Adaptive Optimization (TAO) ensemble model influenced by Random Forest (RF) techniques. These models are trained to effectively detect malicious network behavior while also forecasting network throughput. To enhance model efficiency, several preprocessing strategies are employed, such as label encoding, feature scaling through standardization, and dataset balancing using the Synthetic Minority Over-sampling Technique (SMOTE). These steps contribute to improved robustness and generalization across varying network conditions. Experimental evaluations demonstrate that the TAO ensemble model outperforms individual models in terms of classification accuracy while maintaining strong regression capabilities. Additionally, the system is deployed through a web-based platform using the Flask framework, allowing real-time analysis and user interaction. Overall, the proposed framework offers a scalable and intelligent solution for strengthening network security and improving performance in next-generation communication environments.

Keywords: 6G Networks, Intrusion Detection, Machine Learning (ML), Classification and Regression Tree (CART), Tree-based Adaptive Optimization (TAO).

1. INTRODUCTION

Network management and monitoring depend on data acquisition protocols such as Simple Network Management Protocol (SNMP), NetFlow, IP Flow Information Export (IPFIX), and Network Configuration Protocol (NETCONF) [1]. Organizations often design tailored tools built on these protocols to obtain detailed insights into network status and to efficiently address faults and performance-related issues. As the demand for network services continues to grow rapidly, the expectations placed on network components and monitoring systems have increased accordingly. As a result, modern network devices generate enormous volumes of data including control signals, performance statistics, and user traffic—at an ever-increasing pace [2].

Processing and analyzing such large-scale and complex datasets through manual or semi-automated methods require significant expertise, time, and operational resources. With the continuous expansion of network infrastructures in both size and complexity, these traditional approaches are becoming less

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com

practical and more difficult to maintain. This has driven a transition toward automated and intelligent systems capable of handling high-dimensional data and supporting faster, more accurate decision-making in contemporary network environments.

One of the key technologies facilitating advanced network management and monitoring is Software-Defined Networking (SDN) [3], which provides a centralized and programmable framework for controlling network operations. This architecture simplifies configuration processes and improves flexibility; however, it still necessitates ongoing monitoring and effective anomaly detection mechanisms. Centralized data collection offers notable benefits, such as improved coordination, aggregation, and analysis of network information. Nevertheless, managing and processing these large-scale datasets introduces significant computational challenges, commonly associated with *big data analytics* [4].

To overcome these challenges, several platforms and tools have been introduced to support the handling, deployment, and analysis of extensive datasets. An example is the Platform for Network Data Analytics (PNDA), an open-source framework designed for efficient data collection, storage, and real-time processing. Given the sheer volume of generated network data, the incorporation of Artificial Intelligence (AI) and Machine Learning (ML) techniques is crucial for deriving valuable insights and enhancing decision-making capabilities.

Continuous data collection is essential for effective network monitoring; however, it may increase the workload on network devices and negatively affect throughput, especially within transmission and management networks. To address this issue, adaptive data collection approaches can be implemented, where polling intervals are dynamically modified based on network conditions. For example, increasing the frequency of data collection when anomalies are detected can improve responsiveness while maintaining overall system efficiency [5].

- To develop an intelligent intrusion detection system for network slicing environments using ML techniques to accurately identify different types of network attacks
- To implement classification models such as SVM, KNN, and TAO Tree for effective detection and categorization of malicious network activities
- To design a regression model for predicting network throughput, enabling simultaneous analysis of network performance and security
- To apply data preprocessing and class balancing techniques to enhance model accuracy and ensure reliable performance in large-scale network environments.

2. RELATED WORK

The rapid evolution of 6G communication systems has introduced new challenges in network security, traffic management, and real-time analytics. Traditional rule-based monitoring systems are increasingly inadequate for handling high-dimensional, dynamic network environments. As a result, recent research has focused on integrating Machine Learning (ML) and Artificial Intelligence (AI) techniques to enable intelligent intrusion detection and performance optimization. This section reviews key contributions in this domain and identifies existing research gaps.

2.1 Machine Learning-Based Intrusion Detection in 6G

Saeed et al. [6] proposed an ensemble learning-based anomaly detection system for 6G networks, incorporating preprocessing, feature selection using hybrid CFS-RF, and classification through modified SVM and Random Forest models. Their approach demonstrated improved detection accuracy across multiple benchmark datasets.

Similarly, Ismail et al. [8] introduced a lightweight deep learning framework combining a convolutional neural network (CSO-2D-CNN) with an attention-based XGBoost classifier. This model effectively handled high-dimensional traffic data and achieved strong generalization in wireless network environments. emphasized the importance of real-time intrusion detection systems due to the increasing number of connected devices and rising security threats, proposing a novel IDS approach for rapid threat identification.

2.2 Ensemble and Deep Learning Approaches

Damaševičius et al. [14] developed an ensemble-based malware detection model combining convolutional neural networks and dense neural networks with a meta-learning classifier. Their results highlighted the effectiveness of ensemble strategies in improving classification performance.

Mahmoud et al. [15] proposed a hybrid deep learning framework integrated with physical layer security (PLS) for detecting spoofing, jamming, and eavesdropping attacks. Their multi-stage detection model significantly improved accuracy and reduced bit error rates under attack conditions.

However, as noted by Zahid et al. [9], the application of deep ensemble learning in emerging 6G scenarios, particularly for unconventional threats such as drone-based attacks, remains insufficiently explored.

2.3 ML Integration in 6G Network Optimization

Rekkas et al. [7] provided a comprehensive survey of ML techniques—including supervised, unsupervised, and reinforcement learning in 6G communication systems, highlighting open challenges and future directions.

Puspitasari et al. [10] further emphasized the role of ML in optimizing emerging 6G technologies, identifying its importance in addressing scalability, latency, and performance challenges.

Okere et al. [13] explored enabling technologies such as digital twins, intelligent reflecting surfaces, and blockchain, stressing that ML integration is essential for managing complexity and optimizing network performance in 6G environments.

2.4 SDN-Based Monitoring and Intelligent Security Frameworks

Rzym et al. [11] proposed a deep learning-based anomaly detection system for Software-Defined Networking (SDN), utilizing centralized control and dynamic telemetry for automated monitoring.

Kaur et al. [12] highlighted security risks associated with advanced 6G technologies such as O-RAN and AI-driven systems. They proposed a dynamic framework integrating Explainable AI (XAI) techniques like SHAP and LIME to enhance transparency and robustness in threat detection.

2.5 Research Gap

Although existing studies extensively explore ML-based intrusion detection, ensemble learning, and 6G network optimization, several limitations remain. Most current approaches focus primarily on either classification (attack detection) or performance analysis, but not both simultaneously. Additionally, many models rely heavily on deep learning architectures, which often introduce high computational complexity and reduced interpretability, making them less suitable for real-time deployment.

Furthermore, limited research has been conducted on lightweight, tree-based hybrid models that can efficiently handle both classification and regression tasks within a unified framework. There is also a lack of systems that integrate throughput prediction alongside intrusion detection, which is critical for holistic network management.

To address these gaps, the proposed work introduces a CART-based dual-purpose framework that combines classification and regression capabilities using a novel Tree-based Adaptive Optimization (TAO) ensemble model. This approach aims to achieve high accuracy, improved interpretability, and efficient real-time performance, making it suitable for next-generation 6G network environments.

3. PROPOSED METHODOLOGY

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

This study presents a unified analytical framework designed to simultaneously address security threat detection and network performance prediction. Rather than handling intrusion detection and performance assessment as independent processes, the proposed approach integrates classification and regression techniques to capture the relationship between cyberattacks and their impact on network throughput. This allows concurrent evaluation of security status and performance dynamics within modern communication systems. The framework employs Machine Learning models such as Support Vector Machine (SVM), k-Nearest Neighbors (KNN), and a customized Tree-based Adaptive Optimization (TAO) ensemble model inspired by Random Forest (RF). These models are trained to accurately classify various types of network attacks while also predicting throughput under different network conditions. To enhance usability, the system is implemented as a web-based platform using the Flask framework, offering an interactive and user-friendly interface. It provides a comprehensive processing pipeline that includes dataset upload, preprocessing, Exploratory Data Analysis (EDA), model training, performance evaluation, and real-time prediction, as illustrated in Fig. 1. This integrated architecture ensures efficient handling of large-scale network data and facilitates informed decision-making, ultimately contributing to improved network security and optimized performance in next-generation communication environments.

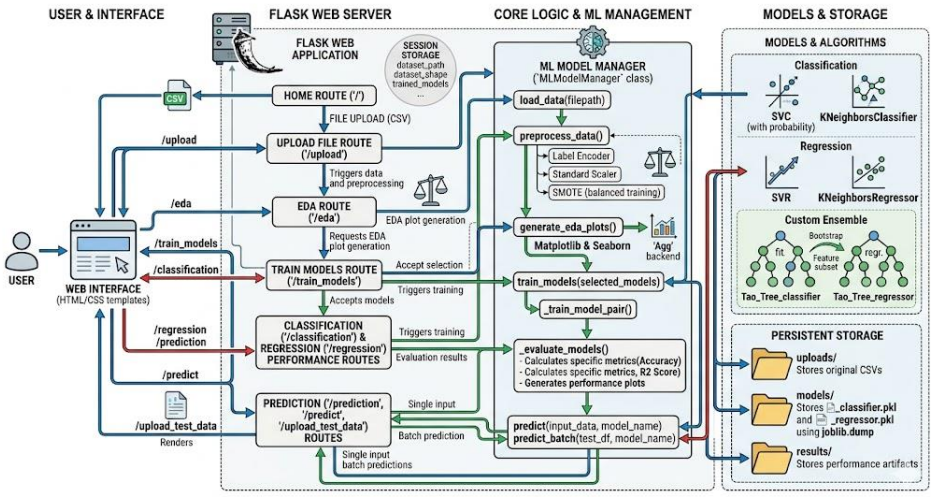


Figure 1: Proposed system architecture

Data Acquisition and Upload: The process begins with the user uploading a network traffic dataset, typically in a CSV format, through the web application's main interface. The system is configured to validate the file type to ensure it is a .csv file, and it uses secure filename handling to prevent malicious uploads. This step acts as the primary entry point for all subsequent analysis and model training activities. Upon successful upload, the system saves the dataset to a dedicated uploads directory and stores its path and basic information, like its shape, in the user's session for continuous access throughout the workflow.

Data Preprocessing and Splitting: In the background, the ML Model Manager performs a series of essential preprocessing tasks to prepare the raw data for machine learning. First, it identifies and drops any irrelevant columns, such as "Unnamed" columns that often appear in datasets. Next, it handles categorical features, like different network services or protocols, by converting them into numerical representations using a Label Encoder. Missing values are filled using the mean of their respective columns. The prepared data is then split into two distinct parts: a training set (80%) and a testing set (20%). The data is also split into two target variables: a categorical one for Intrusion Detection (Attack Type) and a numerical one for Performance Prediction (Throughput). Finally, the system addresses class imbalance in the intrusion

detection dataset by applying SMOTE on the training data. This ensures that the machine learning models do not become biased toward the majority class (normal traffic) and can effectively detect rare attack instances.

EDA: Once the data is loaded, the system automatically redirects the user to the EDA page. This crucial step provides a quick and informative overview of the dataset's characteristics. The system's ML Model Manager generates several key visualizations, including histograms to show the distribution of attack types and network throughput, box plots to analyze the relationship between categorical features (like signal strength) and numerical ones (like throughput), and scatter plots to visualize relationships between continuous variables. A correlation heatmap is also generated to identify which features are most strongly related to the target variables (attack type and throughput). These plots are then displayed on the web page, allowing the user to gain an immediate understanding of the data's structure, potential issues like class imbalance, and key relationships before proceeding to model training.

Model Training and Selection: The user can choose from a variety of machine learning models to train, including SVM, KNN, and a custom ensemble model called TAO Tree. Upon selection, the ML Model Manager trains a classifier for intrusion detection and a regressor for throughput prediction for each chosen model. To enhance efficiency and reusability, the trained models are saved as .pkl files using joblib. This allows the system to load pre-trained models in subsequent sessions, eliminating the need for retraining and significantly reducing processing time.

Performance Evaluation: After training, the system evaluates the performance of each model on the held-out test data. For the classification models, it calculates key metrics such as accuracy, precision, recall, and F1-score. It also generates a confusion matrix, which visually represents the number of correct and incorrect predictions for each attack type. For the regression models, it calculates metrics like Mean Absolute Error (MAE), Mean Squared Error (MSE), and R-squared (R^2) to assess the accuracy of throughput predictions. These detailed performance results, including the visual plots, are then displayed on dedicated pages, allowing the user to compare the effectiveness of different models and choose the best one for their specific needs.

Prediction Interface: The final step provides two methods for making predictions on new data. The single prediction interface allows users to manually input values for each network feature via a form. The system preprocesses this single data point and feeds it to the selected trained models to predict the attack type and network throughput. The batch prediction interface enables users to upload a new CSV file containing multiple instances of network data. The system automatically preprocesses the entire file and returns a table with the predicted attack type and throughput for each instance, providing a powerful tool for large-scale network security and performance analysis.

TAO Tree CART Model

The TAO Tree model is a proposed ML-based ensemble approach designed to perform both classification and regression tasks within a unified framework. It is inspired by RF and built upon CART principles, enabling simultaneous prediction of network attack types and throughput values using the same input features.

Unlike individual models, the TAO model combines multiple decision trees trained on different subsets of data and features. This ensemble strategy improves prediction accuracy, reduces overfitting, and enhances generalization across complex network conditions as shown in Fig. 2. The model is specifically designed to handle non-linear relationships present in network traffic data, making it suitable for next-generation network environments.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

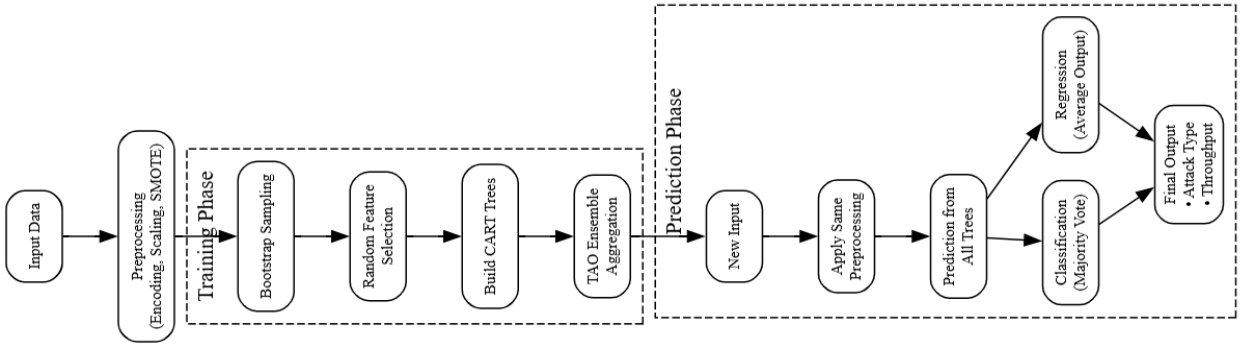


Fig. 2: Internal working of TAO Tree model.

Data Sampling (Bootstrap Aggregation): During training, multiple subsets of the dataset are created using random sampling with replacement. Each subset is used to train an individual decision tree. This process ensures diversity among trees and improves robustness.

Feature Subset Selection: For each tree, a random subset of features is selected instead of using all features. This reduces correlation between trees and allows the model to capture different patterns in the data.

Tree Construction (CART Logic): Each decision tree is built using CART principles:

- For classification: splits are chosen to reduce impurity (e.g., Gini index)
- For regression: splits are chosen to minimize prediction error (e.g., MSE)

The tree recursively splits the data until stopping criteria are met.

Ensemble Learning (TAO Strategy): The TAO model combines predictions from all trees:

- Classification: majority voting across trees determines attack type
- Regression: average of outputs from all trees predicts throughput

This aggregation improves stability and accuracy compared to single-tree models.

Model Optimization: By combining bootstrap sampling and feature randomness, the TAO model reduces overfitting and improves performance on unseen data. It balances bias and variance effectively.

Prediction Process: During inference, new input data is pre-processed and passed through all trained trees. Each tree independently produces classification and regression outputs, which are then aggregated to generate final predictions.

Output Prediction

For each input sample, the model produces:

- Predicted attack type (classification output)
- Predicted throughput value in Mbps (regression output)

These outputs are generated simultaneously, providing a comprehensive understanding of network security and performance.

4. Results Description

Fig. 3 illustrates the Flask-based web interface designed for integrated network security analysis and performance prediction. The interface provides a structured workflow that includes dataset upload, preprocessing, EDA visualization, model training, and prediction within a single platform. It displays analytical plots such as attack type distribution, throughput distribution, latency relationships, and correlation heatmaps, enabling clear understanding of network data. The interface also presents classification metrics and regression results, along with a prediction section that outputs both attack type and throughput, ensuring simultaneous analysis of network security and performance in an organized and user-friendly manner.

AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

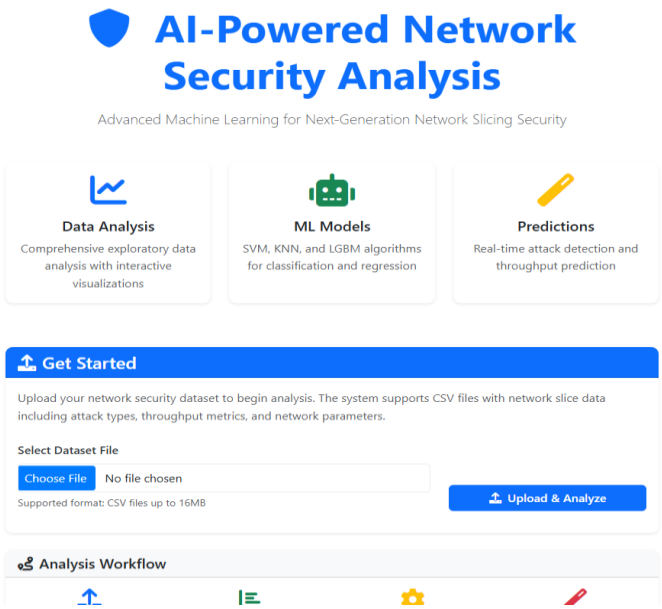
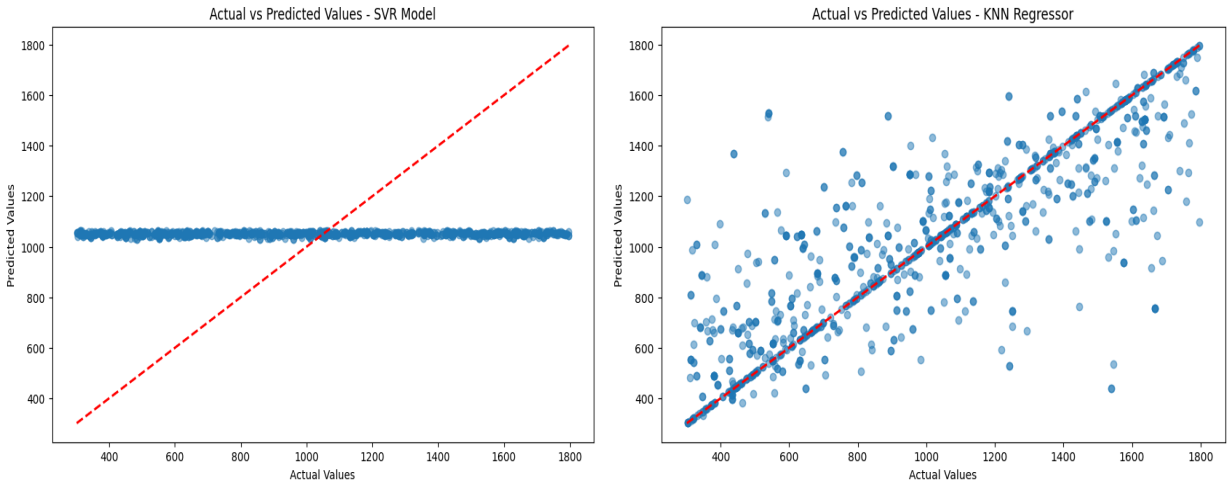


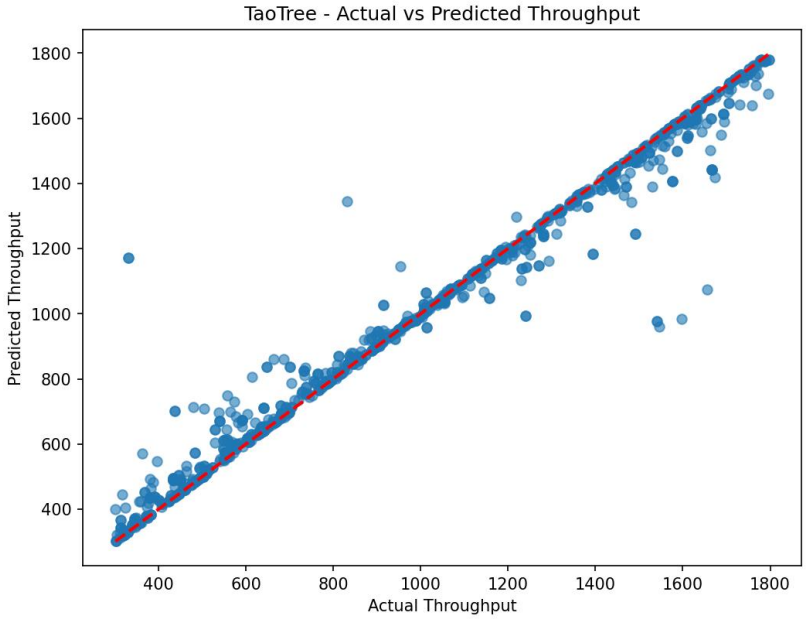
Fig. 3: Proposed network security analysis interface.



(a) (b)

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com

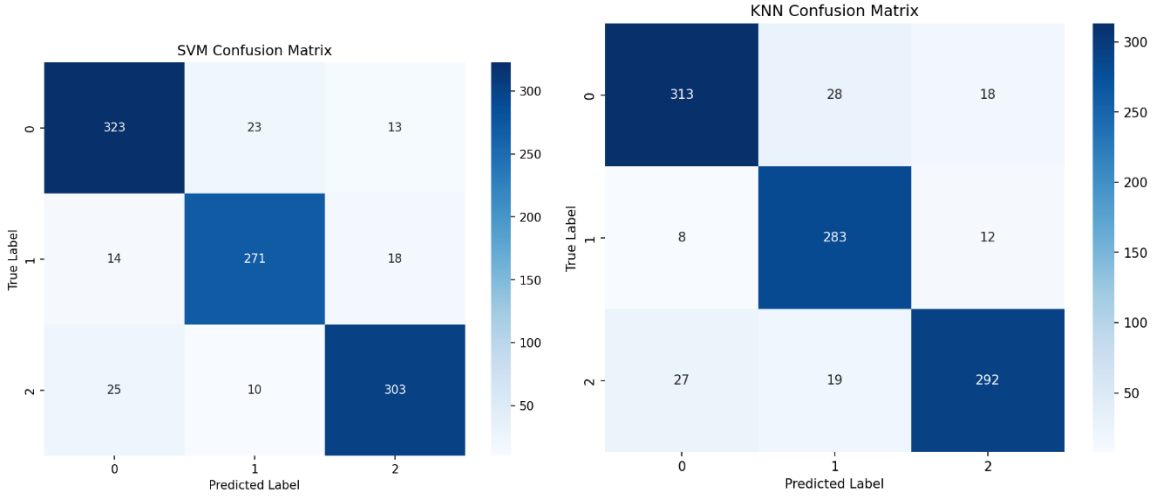
AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)



(c)

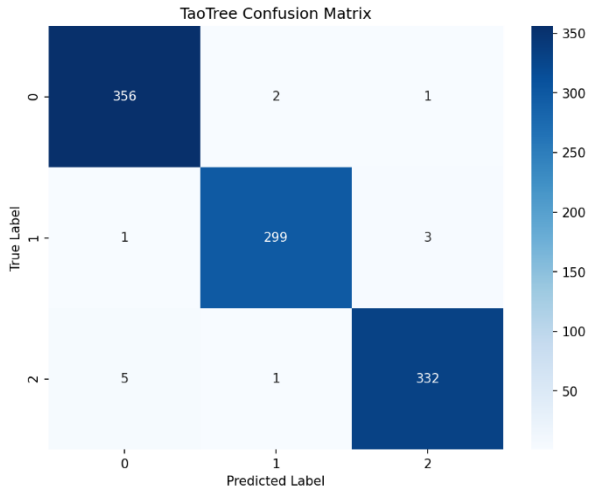
Fig. 4: Scatter plot of actual vs predictions obtained using (a) SVM model. (b) KNN model. (c) Proposed TAO Tree Regressor

The scatter plots in Fig. 4 compare actual vs. predicted values for four models: (a) SVM, (b) KNN, and (c) TAO Tree Regressor. The SVM plot shows a flat predicted value trend, indicating poor performance. The KNN plot shows predictions closely aligned with the diagonal, suggesting good accuracy.



(a) (b)

Received: 07-05-2026 | Accepted: 15-06-2026 | Published: 22-06-2026 | www.ajaccm.com



(c)

Fig. 5: Confusion matrix obtained using (a) SVM model.
(b) KNN model. (c) Proposed TAO Tree Classifier

The confusion matrices in Fig. 5 illustrate the performance of four models (a) SVM, (b) KNN, and (c) TAO Tree in classifying DDoS, Eavesdropping, and Spoofing. The SVM matrix shows poor differentiation, with high misclassifications (e.g., 198 Spoofing predicted as Eavesdropping). The KNN matrix performs better, with 264 correct Eavesdropping predictions but 316 DDoS misclassifications. The TAO Tree matrix excels, with 299 correct Eavesdropping, 335 correct Spoofing, and 356 correct DDoS predictions, showing minimal errors.

Table 1: Performance evaluation obtained using existing SVM, KNN regressors and proposed TAO Tree regression models.

Model/Metric	MAE	MSE	RMSE	R2-score
SVR Model	370.871	18.8609	431.828	0.009
KNN Model	133.998	49133.987	221.662	0.739
TAO Tree Regressor	0.0297	5787.744	76.007	0.969

Table 1 presents performance metrics for four different regression models evaluated on a dataset. The metrics included are Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and R2 Score.

The models listed are:

- **SVR Model**: MAE is 370.851, MSE is 18.8609, RMSE is 431.828, and R2 Score is -0.009, indicating poor predictive performance with a negative R2 score suggesting the model is not better than a mean baseline.
- **KNN Regressor**: MAE is 133.998, MSE is 49133.987, RMSE is 221.662, and R2 Score is 0.739, indicating a significant improvement in predictive accuracy and a substantial positive R2 score.
- **TAO Tree Regressor**: MAE is 29.042, MSE is 5787.744, RMSE is 76.007, and R2 Score is 0.969, demonstrating the best performance among the models with the lowest errors and a very high R2 score, suggesting excellent predictive capability.

Table 2: Performance evaluation obtained using existing SVM, LR, KNN regressors and proposed TAO Tree classification models.

Algorithm	Accuracy	Precision	Recall	F1-Score
SVC Model	89.7	89.7	89.7	89.7
KNN Model	88.9	88.907	88.857	88.876
TAO Tree Classifier	98.7	98.7	98.7	98.7

Table 2 presents performance metrics for four different classification algorithms evaluated on a dataset. The metrics included are Accuracy, Precision, Recall, and F1-Score.

- **SVC Model**: Accuracy is 89.7%, Precision is 89.7%, Recall is 89.7%, and F1-Score is 89.7%, indicating relatively average performance across all metrics, suggesting limited ability to correctly classify instances.
- **KNN Classifier**: Accuracy is 88.9%, Precision is 88.907%, Recall is 88.857%, and F1-Score is 88.876%, demonstrating strong performance with high values across all metrics, indicating effective classification.
- **TAO Tree Classifier**: Accuracy is 98.7%, Precision is 98.7%, Recall is 98.7%, and F1-Score is 98.7%, showcasing the best performance among the algorithms with near-perfect scores, suggesting excellent classification capability.

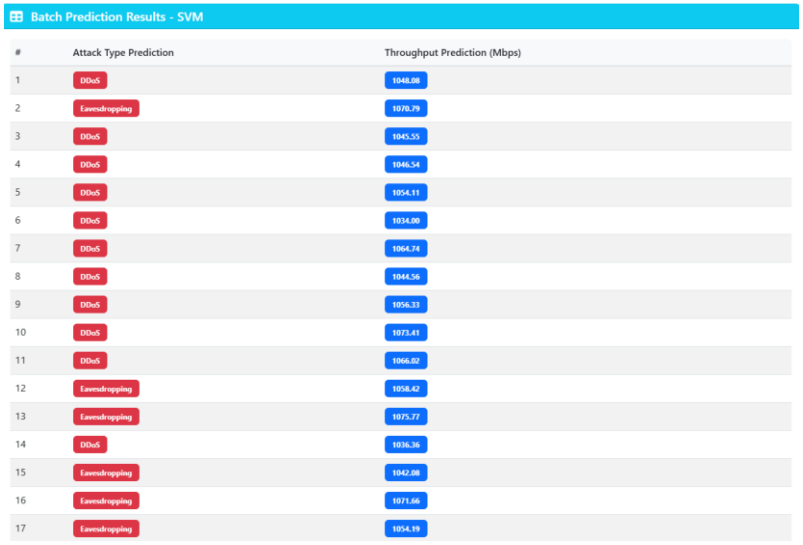


Fig. 6: Predictions on test data.

Fig. 6 shows the batch prediction output generated by the system for test data inputs. The results are presented in a tabular format where each record includes the predicted attack type and corresponding throughput value. The predictions are produced after applying consistent preprocessing steps, including encoding and scaling, ensuring accuracy and uniformity across all inputs. This output provides a clear representation of how different network conditions are classified and how throughput is estimated, supporting effective analysis and validation of the system's performance.

5. Conclusion

This study presents a web-based Machine Learning framework for intelligent network monitoring that simultaneously performs attack classification and throughput prediction. The proposed system integrates multiple ML algorithms, including Support Vector Machine (SVM), k-Nearest Neighbors (KNN), and the proposed Tree-based Adaptive Optimization (TAO) ensemble model, enabling efficient analysis of network

data and providing valuable insights into both security and performance aspects. The implementation encompasses a complete processing pipeline, including dataset upload, preprocessing, Exploratory Data Analysis (EDA), model training, evaluation, and real-time prediction through an interactive Flask-based interface. Data preprocessing techniques such as label encoding, standardization, and Synthetic Minority Over-sampling Technique (SMOTE) are applied to enhance data quality and improve model effectiveness. By combining classification and regression tasks, the framework is capable of identifying various types of network attacks while simultaneously estimating throughput, offering a comprehensive view of network behavior. Among the evaluated models, the TAO ensemble model demonstrates superior performance due to its ability to capture complex, non-linear patterns and leverage ensemble learning advantages. Overall, the proposed system achieves its goal of delivering a scalable, efficient, and intelligent solution suitable for next-generation network environments. This work highlights the significance of ML-driven approaches in strengthening network security while optimizing performance management.

REFERENCES

[1] Fernandes, G.; Rodrigues, J.J.; Carvalho, L.F.; Al-Muhtadi, J.F.; Proença, M.L. A Comprehensive Survey on Network Anomaly Detection. Telecommun. Syst. **2019**, 70, 447–489.

[2] Cisco Annual Internet Report (2018–2023) White Paper; Technical Report; Cisco: San Jose, CA, USA, 2023.

[3] 2022 Global Networking Trends Report; Technical Report; Cisco: San Jose, CA, USA, 2022.

[4] 2023 Global Internet Phenomena Report; Technical Report, Sandvine Intelligent Broadband Networks; Sandvine Inc.: Waterloo, ON, Canada, 2022.

[5] Ericsson Mobility Report; Technical Report; Ericsson: Stockholm, Sweden, 2022.

[6] Saeed, M.M.; Saeed, R.A.; Abdelhaq, M.; Alsaqour, R.; Hasan, M.K.; Mokhtar, R.A. Anomaly Detection in 6G Networks Using Machine Learning Methods. *Electronics* **2023**, *12*, 3300. https://doi.org/10.3390/electronics12153300.

[7] Rekkas, V.P.; Sotiroudis, S.; Sarigiannidis, P.; Wan, S.; Karagiannidis, G.K.; Goudos, S.K. Machine Learning in Beyond 5G/6G Networks—State-of-the-Art and Future Trends. *Electronics* **2021**, *10*, 2786. https://doi.org/10.3390/electronics10222786.

[8] Ismail, W.N. A Novel Metaheuristic-Based Methodology for Attack Detection in Wireless Communication Networks. *Mathematics* **2025**, *13*, 1736. https://doi.org/10.3390/math13111736.

[9] Zahid, M.U.; Nisar, M.D.; Fazil, A.; Ryu, J.; Shah, M.H. Composite Ensemble Learning Framework for Passive Drone Radio Frequency Fingerprinting in Sixth-Generation Networks. *Sensors* **2024**, *24*, 5618. https://doi.org/10.3390/s24175618.

[10] Puspitasari, A.A.; An, T.T.; Alsharif, M.H.; Lee, B.M. Emerging Technologies for 6G Communication Networks: Machine Learning Approaches. *Sensors* **2023**, *23*, 7709. https://doi.org/10.3390/s23187709.

[11] Rzym, G.; Masny, A.; Chołda, P. Dynamic Telemetry and Deep Neural Networks for Anomaly Detection in 6G Software-Defined Networks. *Electronics* **2024**, *13*, 382. https://doi.org/10.3390/electronics13020382.

[12] Kaur, N.; Gupta, L. Securing the 6G–IoT Environment: A Framework for Enhancing Transparency in Artificial Intelligence Decision-Making Through Explainable Artificial Intelligence. *Sensors* **2025**, *25*, 854. https://doi.org/10.3390/s25030854.

[13] Okere, E.E.; Balyan, V. Sixth Generation Enabling Technologies and Machine Learning Intersection: A Performance Optimization Perspective. *Future Internet* **2025**, *17*, 50. https://doi.org/10.3390/fi17020050.

[14] Damaševičius, R.; Venčkauskas, A.; Toldinas, J.; Grigaliūnas, Š. Ensemble-Based Classification Using Neural Networks and Machine Learning Models for Windows PE Malware Detection. *Electronics* **2021**, *10*, 485. https://doi.org/10.3390/electronics10040485.

[15] Mahmoud, H.; Ismail, T.; Baiyekusi, T.; Idrissi, M. Advanced Security Framework for 6G Networks: Integrating Deep Learning and Physical Layer Security. *Network* **2024**, *4*, 453-467. https://doi.org/10.3390/network4040023.