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

P2P Traffic Intelligence System Employing Wavelet Bandwidth Analytics for Multivariate Anomaly Reasoning

N. Sai Sindhuri[1], Sk. Khadar Basha[2], Sk. Thoufeq Ahamed [2], T. V. Gopal Krishna[2], V. Rupesh[2]

[1]Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering (AI & ML)

[1,2]Geethanjali Institute of Science and Technology, Nellore-Bombay Highway, S.P.S.R, Andhra Pradesh 524137, India

ABSTRACT

Modern digital infrastructures including enterprise networks, cloud computing platforms, IoT ecosystems, and online service environments continuously generate vast volumes of real-time data such as network packets, authentication logs, and system performance metrics. This rapid data generation necessitates efficient, intelligent, and real-time security monitoring mechanisms. To address these challenges, this work proposes an automated and scalable AI-driven security framework for real-time anomaly detection and authentication threat analysis. Initially, machine learning models such as K-Nearest Neighbor (KNN) and Support Vector Classifier (SVC) are utilized to learn network behavior patterns and distinguish between normal and malicious activities. Although effective, these models exhibit limitations including high computational complexity, sensitivity to feature scaling, and inefficiency in handling large-scale or probabilistic data scenarios. To overcome these constraints, a Naive Bayes Classifier (NBC) is adopted as the primary probabilistic inference model within the framework. By leveraging Bayesian decision theory and modeling conditional feature dependencies, NBC enables efficient estimation of threat probabilities with reduced computational overhead and improved scalability for high-dimensional datasets. The proposed system incorporates data preprocessing, class balancing techniques, multi-model training, and deployment through a web-based Flask interface to facilitate real-time threat detection. Performance evaluation is conducted using standard metrics such as accuracy, precision, recall, and F1-score, demonstrating reliable anomaly detection and classification capabilities. The results validate that the proposed framework provides a robust, scalable, and efficient solution for enhancing real-time security intelligence in modern digital environments.

Keywords: Network security, Anomaly detection, Real time monitoring, Wavelet bandwidth, Authentication logs.

1. INTRODUCTION

In today's rapidly advancing technological environment, sensors play a crucial role in supplying essential data for decision-making across a wide range of applications. Maintaining the reliability and accuracy of this sensor data is vital, as even minor inconsistencies can result in significant errors and potential system failures [1]. This concern becomes even more critical within embedded systems and Internet of Things (IoT) environments, where sensors function under diverse and often harsh conditions. Ensuring data integrity in such settings is particularly challenging due to continuous exposure to dynamic and unpredictable environments [2]. As shown as Fig 1. Conventional anomaly detection techniques, including signature-based Intrusion Detection Systems (IDS), have demonstrated effectiveness in identifying known threats. However, they face limitations when dealing with new and sophisticated attack patterns.

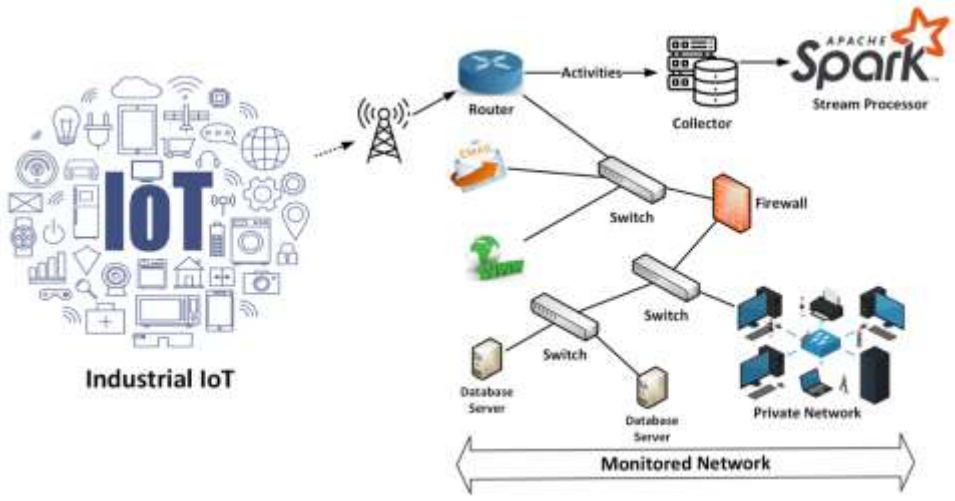

Fig. 1. Monitoring of IoT-based network traffic flows.

With the continuous evolution of cyber threats and system vulnerabilities, there is an increasing demand for advanced detection mechanisms that can adapt to emerging risks while maintaining system reliability and security [3]. This research addresses the identified challenges by proposing a novel approach that incorporates discrete wavelet transforms (DWT) within microcontroller-based systems for real-time anomaly detection and fault isolation [4]. Wavelet transforms, especially DWT, are widely recognized as effective tools in signal processing, enabling the decomposition of signals into multiple frequency components for localized analysis. The Haar wavelet, a member of the DWT family, is selected for this study due to its simplicity and efficiency in handling non-stationary signals. It facilitates the detection of both transient and persistent anomalies in sensor data by providing precise time and frequency localization. Furthermore, the computational simplicity of Haar wavelets makes them highly suitable for real-time implementation in resource-constrained environments such as microcontrollers [5]. To enhance anomaly detection, Euclidean distance is employed alongside DWT to measure deviations between transformed sensor data and a reference model, offering an efficient and straightforward mechanism for fault identification.

Network environments today generate enormous volumes of heterogeneous data from various sources such as sensors, servers, and connected devices. Within this high-speed data flow, distinguishing between normal operational fluctuations and actual malicious activities is a challenging task. Traditional monitoring systems often rely on static rule-based detection, which is limited in adaptability and fails to detect evolving or complex intrusion patterns. The high diversity of network environments also means that intrusion detection must work across varied traffic loads, user behaviours, and device capabilities. Inconsistent data formats, missing values, and noisy readings further complicate the analysis process.

2. LITERATURE SURVEY

2.1 AI/ML-Based Intrusion Detection and Network Forensics

Paracha *et al.* [6] proposed an AI/ML-based network forensics model capable of analyzing network traffic and behavioral patterns to detect prior and potential cyberattacks. The system enhances investigation speed and enables automated monitoring without human intervention, providing timely insights for

network administrators. Similarly, Chiriac *et al.* [7] introduced a modular intrusion detection system (IDS) for Industry 4.0 using the Nvidia Morpheus AI framework, integrating a pre-trained XGBoost model that achieved up to 90% accuracy while processing over 500,000 inputs within 10 seconds. Abuali *et al.* [8] developed a support vector machine (SVM)-based deep learning IDS using the CSE-CIC-IDS 2018 dataset, focusing on multiclass classification of intrusion incidents in social media environments. These works highlight the effectiveness of AI/ML techniques in improving detection speed, automation, and decision-making in cybersecurity systems.

2.2 Deep Learning-Based Intrusion Detection Models

Ali *et al.* [11] implemented a comparative study involving multiple deep learning models such as multilayer perceptron (MLP), convolutional neural networks (CNN), and long short-term memory (LSTM), alongside traditional machine learning algorithms. Thapa *et al.* [14] also explored hybrid ML and DL approaches, achieving up to 99% accuracy on the CIDDS dataset with low false alarm rates and efficient training. Mohammad *et al.* [15] emphasized the integration of deep learning models into cybersecurity frameworks, achieving up to 91% accuracy on augmented CIC-IDS-2017 data. Elmasry *et al.* [16] further improved IDS performance, achieving accuracies between 92% and 99.5% while reducing model complexity significantly. These studies demonstrate the robustness and scalability of deep learning techniques in detecting sophisticated cyber threats.

2.3 Advanced Hybrid and Transformer-Based IDS Approaches

Mao *et al.* [12] proposed MFEI-IDS, incorporating a dynamic routing mechanism and inductive learning to handle imbalanced datasets and unseen attack types, outperforming traditional FCN–Transformer models. Cao *et al.* [17] introduced WTDBNet, a hybrid model combining Transformer-based global feature extraction, CNN-based local feature learning, and wavelet transforms for enhanced feature representation. Similarly, Sun *et al.* [18] developed a CNN-Transformer hybrid framework integrated with wavelet encoding and decoding mechanisms, improving feature reconstruction and edge preservation. These approaches demonstrate the growing trend of combining multiple architectures to enhance detection accuracy and generalization.

2.4 Image-Based and Feature Transformation Techniques for IDS

Toldinas *et al.* [9] proposed a novel approach that transforms network traffic features into RGBA images and applies a ResNet50 model for classification, achieving up to 99.8% accuracy on UNSW-NB15 and 99.7% on BOUN DDoS datasets. Zhang *et al.* [10] utilized wavelet leader multifractal (WLM) analysis combined with machine learning to detect anomalies such as spoofing and flooding attacks in UAV networks. These methods emphasize the effectiveness of transforming network data into alternative representations to improve classification performance.

2.5 Adversarial Learning and Data Augmentation Techniques

Mari *et al.* [13] explored the use of generative adversarial networks (GANs) to create adversarial network traffic capable of evading detection systems. The generated data was also used to improve IDS robustness against unseen attacks. This approach highlights the importance of adversarial training and data augmentation in strengthening cybersecurity defenses.

2.6 Wavelet and Signal Processing-Based Learning Approaches

Kim *et al.* [19] addressed multipath error detection in GNSS systems using wavelet transforms combined with shallow and deep neural networks, achieving detection accuracies of up to 87.1%. Yang *et al.* [20] proposed a multi-wavelet 3D CNN (MW-3D-CNN) for hyperspectral image super-resolution, leveraging wavelet sub-band decomposition for enhanced feature extraction. These studies demonstrate the versatility of wavelet-based feature extraction in improving learning performance across different domains, including cybersecurity.

3. PROPOSED METHODOLOGY

The proposed system architecture converts raw network traffic into meaningful and discriminative features through structured preprocessing, followed by machine learning–based classification for detecting anomalies and authentication failures with high accuracy. The workflow is designed to capture variations in network behaviour, identify deviations in authentication patterns, and analyse packet-level characteristics that are often difficult to detect using traditional approaches. By integrating preprocessing techniques with multiple machine learning models, the system improves detection capability, minimizes false alarms, and supports efficient real-time intrusion detection, as illustrated in Fig 2.

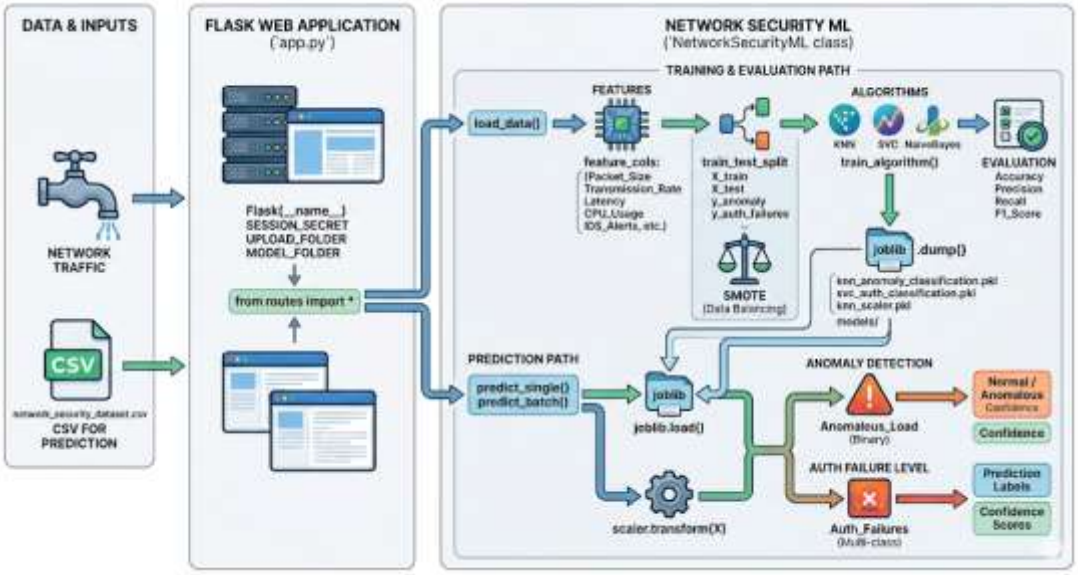

Fig 2. Proposed system architecture for anomaly detection and authorization level classification

The process begins with raw network data acquisition, where traffic streams and CSV-based datasets containing packet-level information and security-related attributes are collected to represent both normal and anomalous network conditions. This data then undergoes preprocessing and cleaning to remove incomplete or redundant entries, followed by normalization and structuring of key features such as packet size, transmission rate, latency, CPU usage, and IDS alerts to ensure consistency and quality. In the feature engineering and dataset preparation stage, relevant attributes are selected to effectively capture network behavior, and the dataset is split into training and testing subsets, while class imbalance is addressed using SMOTE to ensure balanced learning. The prepared data is then used to train multiple machine learning models, including KNN, SVC, and Naive Bayes, where each model learns to classify

normal and abnormal activities based on extracted patterns, with performance evaluated using metrics such as accuracy, precision, recall, and F1-score, and trained models stored using joblib for future use. During real-time prediction and intrusion detection, a Flask-based web application processes incoming data through single and batch prediction functions, loads the stored models, applies feature scaling, and performs binary and multi-class classification to detect anomalies and authentication failures, generating prediction labels along with confidence scores. The entire system is deployed and integrated within the Flask framework, enabling seamless interaction between data input, processing, model execution, and result visualization, while continuous monitoring and feedback mechanisms ensure that incoming data is consistently analyzed and predictions are updated, maintaining reliable and adaptive intrusion detection performance in real-time environments.

NBC

NBC is a probabilistic classifier that uses Bayes' theorem to predict the probability of a class given the observed features, assuming feature independence. In the Defense Wave: Multi-Scale Wavelet-Enhanced AI for Long-Range Network Intrusion Detection**,** NBC leverages wavelet-enhanced network features to identify anomalous traffic and classify authentication failures as Positive, Negative, or Neutral. By estimating the conditional probability of each feature under each class, as shown in Figure.4.6, NB provides fast and interpretable predictions for both anomaly detection and authentication failure classification, even in complex, high-dimensional network datasets.

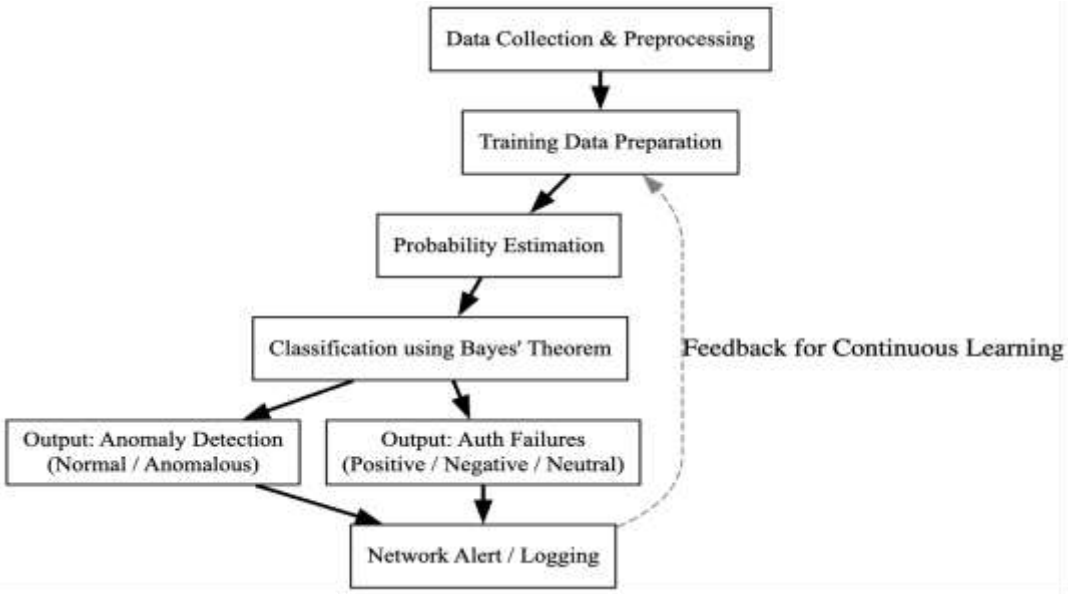

Fig. 3. Internal operations workflow of NBC model.

Probability Estimation: For each class, NBC computes the prior probability (frequency of the class in training data) and conditional probability for each feature. Continuous features are usually modeled with a Gaussian distribution, while discrete features can use multinomial or Bernoulli distributions. These probabilities capture the likelihood of observing certain feature values given a class, forming the basis for classification.

Classification Using Bayes' Theorem: For a new network instance, NBC applies Bayes' theorem to compute the posterior probability of each class given the observed features. The predicted class is the one with the highest posterior probability**.** For anomaly detection, the class is Normal or Anomalous. For authentication failures, the class can be Positive, Negative, or Neutral. NB outputs both the predicted label and the associated confidence score (posterior probability).

Prediction and Integration with Defense Wave: Predictions are integrated into Defense Wave for real-time monitoring. High-confidence anomalous predictions trigger alerts to administrators, while authentication failure classifications help prioritize security responses. The probabilistic nature of NBC allows administrators to quantify the uncertainty of each prediction, improving operational decision-making.

Continuous Learning and Feedback: Prediction results and feedback from administrators are logged and can be used to update prior and likelihood probabilities. This allows NBC to adapt to evolving network traffic patterns, enhancing detection accuracy for long-range and subtle intrusions over time.

4. RESULTS AND DESCRIPTION

Fig. 4. illustrates the main dashboard of the Network Security ML Analysis application, which serves as the central interface for accessing the system functionalities. The dashboard integrates different modules including exploratory data analysis, model performance comparison, and network security prediction within a unified environment. Through this interface, users can navigate to different analytical sections of the system and initiate machine learning based analysis tasks. The dashboard acts as the entry point where users can begin dataset exploration, train machine learning models, and perform prediction analysis.

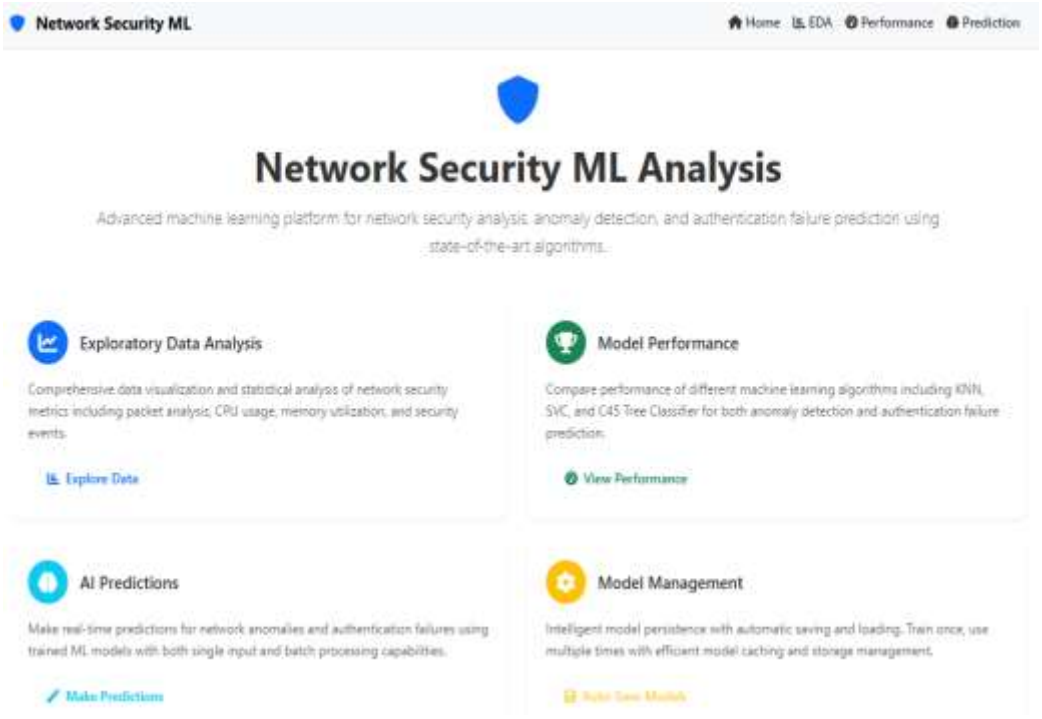

Fig. 4. Frontend Dashboard of Network Security ML Analysis Application.

Fig. 5 illustrates the model performance comparison interface used to train and evaluate machine learning algorithms within the system. The interface allows users to select algorithms such as KNN, SVC, and NBC for training and evaluation. Through this component, users can initiate the model training process and compare the effectiveness of different classification techniques. The interface supports experimentation with multiple algorithms for anomaly detection and authentication failure classification.

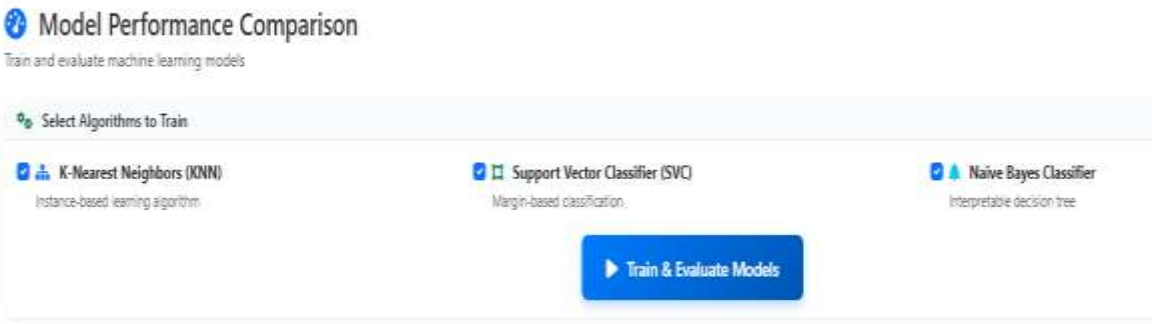

Fig. 5. Model Performance Comparison Interface for Training and Evaluation.

Fig. 6. presents the evaluation results obtained after training the selected machine learning models. For anomaly detection classification, NBC achieved an accuracy of 95.40 percent, precision of 95.89 percent, recall of 95.40 percent, and F1 score of 95.49 percent. The KNN model achieved an accuracy of 82.40 percent with an F1 score of 83.23 percent, while the SVC model achieved an accuracy of 72.30 percent with an F1 score of 73.82 percent. In authentication failure classification, Naive Bayes achieved 100 percent accuracy, precision, recall, and F1 score.

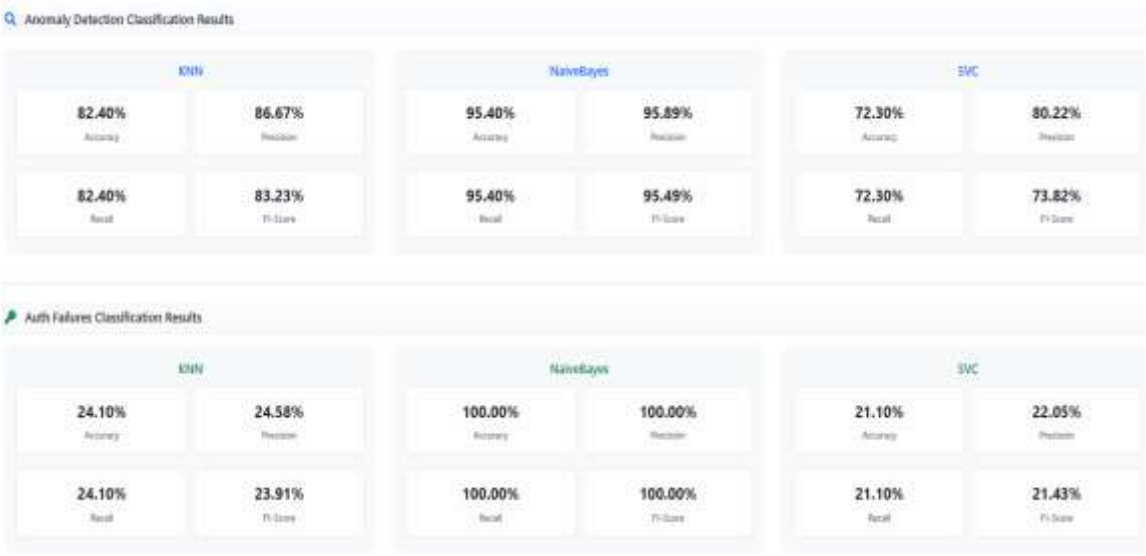

Fig. 6. Model Performance Evaluation Interface after Training the models.

Fig. 7 illustrates the prediction interface used for performing single input analysis in the network security application. The interface allows users to provide network traffic parameters including packet size, transmission rate, latency, protocol type, active connections, CPU usage, memory usage, bandwidth utilization, request response time, authentication failures, access violations, firewall blocks, IDS alerts,

and DWT feature values. These input parameters are processed by the trained machine learning model to determine the security status of the network activity. The interface supports real time prediction of anomalous network behavior and authentication failure levels.

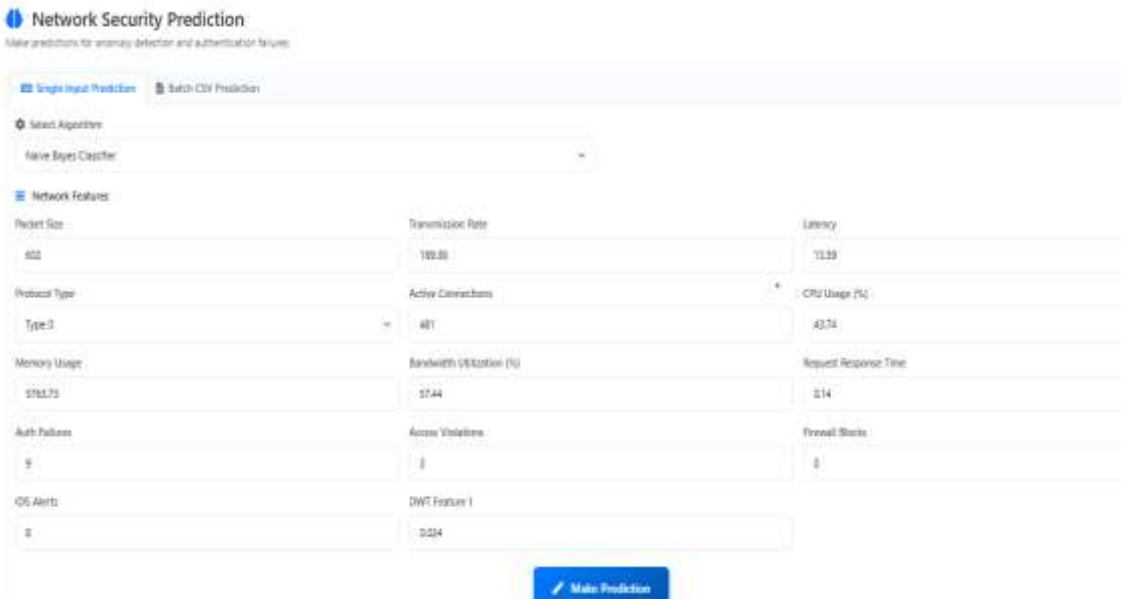

Fig. 7. Network Security Prediction Interface for Single Input Analysis.

Fig. 8. Output of the Test Data.

Fig. 8 shows the prediction results generated by the system after processing the provided network traffic data. The anomaly detection module predicts the network activity as normal with a confidence level of approximately 97.72 percent. In addition, the authentication failure classification module predicts level 9 with 100.00 percent confidence. These prediction results demonstrate the ability of the trained machine learning model to analyse network features and provide security related insights.

5. CONCLUSION

The research presents a robust Flask-based web application that seamlessly integrates machine learning for intelligent network security analysis. The system leverages a network dataset enriched with wavelet-derived attributes, particularly DWT_Feature_1, to strengthen anomaly detection and authentication failure classification. Multiple classifiers, including KNN, SVC, and NBC, are evaluated, with NBC achieving superior performance such as 95.40% accuracy, precision, recall, and F1-score for anomaly detection, and a perfect 100% across all metrics for authentication failure classification. In contrast, KNN

and SVC demonstrate comparatively lower performance, achieving 82.40% and 72.30% anomaly detection accuracy, and only 24.10% and 21.10% accuracy for authentication failure prediction. Performance optimization strategies include SMOTE-based class balancing to address dataset skew (1,354 anomalous vs. 3,646 normal samples), StandardScaler-driven feature normalization for stable learning, and joblib-based model persistence for efficient deployment. These enhancements collectively improve predictive reliability, computational efficiency, and real-time operational readiness of the intrusion detection framework.

REFERENCES

[1]. Li, D.; Wang, Y.; Wang, J.; Wang, C.; Duan, Y. Recent Advances in Sensor Fault Diagnosis: A Review. Sens. Actuators A Phys. 2020, 309, 111990.

[2]. Fatima, N.; Riaz, S.; Ali, S.; Khan, R.; Ullah, M.; Kwak, D. Sensors Faults Classification and Faulty Signals Reconstruction Using Deep Learning. IEEE Access 2024, 12, 100544–100558.

[3]. Yang, J.W.; Lee, Y.D.; Koo, I.S. Convolutional Autoencoder-Based Sensor Fault Classification. Int. Conf. Ubiquitous Future Netw. 2018, 2018, 865–867

[4]. Jiang, X.; Zhang, X.; Zhang, Y. Establishment and Optimization of Sensor Fault Identification Model Based on Classification and Regression Tree and Particle Swarm Optimization. Mater. Res. Express 2021, 8, 085703.

[5]. Jiang, C.Y.; Li, L.C.; Ye, C.L.; Yu, S.Y. Research on Sensor Fault Identification Based on Improved 1-v-r SVM Classification Method. Int. J. Adv. Media Commun. 2016, 6, 235–245.

[6]. Paracha, M.A.; Jamil, S.U.; Shahzad, K.; Khan, M.A.; Rasheed, A. Leveraging AI for Network Threat Detection—A Conceptual Overview. Electronics 2024, 13, 4611. https://doi.org/10.3390/electronics13234611

[7]. Chiriac, B.-N.; Anton, F.-D.; Ioniță, A.-D.; Vasilică, B.-V. A Modular AI-Driven Intrusion Detection System for Network Traffic Monitoring in Industry 4.0, Using Nvidia Morpheus and Generative Adversarial Networks. Sensors 2025, 25, 130. https://doi.org/10.3390/s25010130

[8]. Abuali, K.M.; Nissirat, L.; Al-Samawi, A. Advancing Network Security with AI: SVM-Based Deep Learning for Intrusion Detection. Sensors 2023, 23, 8959. https://doi.org/10.3390/s23218959

[9]. Toldinas, J.; Venčkauskas, A.; Damaševičius, R.; Grigaliūnas, Š.; Morkevičius, N.; Baranauskas, E. A Novel Approach for Network Intrusion Detection Using Multistage Deep Learning Image Recognition. Electronics 2021, 10, 1854. https://doi.org/10.3390/electronics10151854

[10]. Zhang, R.; Condomines, J.-P.; Lochin, E. A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System. Drones 2022, 6, 21. https://doi.org/10.3390/drones6010021

[11]. Ali, M.L.; Thakur, K.; Schmeelk, S.; Debello, J.; Dragos, D. Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study. Appl. Sci. 2025, 15, 1903. https://doi.org/10.3390/app15041903

[12]. Mao, J.; Yang, X.; Hu, B.; Lu, Y.; Yin, G. Intrusion Detection System Based on Multi-Level Feature Extraction and Inductive Network. Electronics 2025, 14, 189. https://doi.org/10.3390/electronics14010189

[13]. Mari, A.-G.; Zinca, D.; Dobrota, V. Development of a Machine-Learning Intrusion Detection System and Testing of Its Performance Using a Generative Adversarial Network. Sensors 2023, 23, 1315. https://doi.org/10.3390/s23031315

[14]. Thapa, N.; Liu, Z.; KC, D.B.; Gokaraju, B.; Roy, K. Comparison of Machine Learning and Deep Learning Models for Network Intrusion Detection Systems. Future Internet 2020, 12, 167. https://doi.org/10.3390/fi12100167

[15]. Mohammad, R.; Saeed, F.; Almazroi, A.A.; Alsubaei, F.S.; Almazroi, A.A. Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach. Systems 2024, 12, 79. https://doi.org/10.3390/systems12030079

[16]. Elmasry, R.M.; Abd El Ghany, M.A.; Salem, M.A.-M.; Fahmy, O.M. MultiWave-Net: An Optimized Spatiotemporal Network for Abnormal Action Recognition Using Wavelet-Based Channel Augmentation. AI 2024, 5, 259-289. https://doi.org/10.3390/ai5010014

[17]. Cao, W.; Zhao, X.; Wang, H.; Hu, Y. WTDBNet: A Wavelet Transform-Based Dual-Stream Backbone Network for Fine-Grained Ship Detection. Remote Sens. 2025, 17, 1570. https://doi.org/10.3390/rs17091570

[18]. Sun, K.; Meng, F.; Tian, Y. Multi-Level Wavelet-Based Network Embedded with Edge Enhancement Information for Underwater Image Enhancement. J. Mar. Sci. Eng. 2022, 10, 884. https://doi.org/10.3390/jmse10070884

[19]. Kim, O.-J.; Kee, C. Wavelet and Neural Network-Based Multipath Detection for Precise Positioning Systems. Mathematics 2023, 11, 1400. https://doi.org/10.3390/math11061400

[20]. Yang, J.; Zhao, Y.-Q.; Chan, J.C.-W.; Xiao, L. A Multi-Scale Wavelet 3D-CNN for Hyperspectral Image Super-Resolution. Remote Sens. 2019, 11, 1557. https://doi.org/10.3390/rs11131557