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

Scalable AI Framework for Real-Time Anomaly Detection and Authentication Threat Management in Digital Networks

J. Naresh[1*], Venu Kumar Garshakurthy[2], Nagaluti Revanth Kumar[2], Supriya Boga[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering (AI&ML),
[1,2]Kommuri Pratap Reddy Institute of Technology, Ghanpur, Ghatkesar, 501301, Telangana, India.

*Correspondence: J. Naresh

ABSTRACT

Real-time digital infrastructures including enterprise networks, cloud platforms, Internet of Things (IoT) ecosystems, and online service environments generate massive volumes of traffic in the form of packet data, authentication logs, and system performance metrics. These continuous data streams require instant security monitoring and intelligent threat assessment. Traditional security approaches rely on manual log inspection, rule-based Intrusion Detection Systems (IDS), and static threshold mechanisms, where administrators analyze predefined signatures to detect anomalies. However, such methods are slow, labor-intensive, and unable to adapt to evolving cyberattack patterns, leading to delayed threat response, high false positive rates, poor scalability, and increased risk of undetected intrusions. To address these challenges, this work proposes a robust, automated, and scalable Artificial Intelligence (AI)-powered security framework for real-time anomaly detection and authentication threat management. The system initially employs machine learning algorithms such as K-Nearest Neighbor (KNN) and Support Vector Classifier (SVC) to learn behavioral patterns and establish decision boundaries between normal and malicious activities. Despite their effectiveness, these models face limitations such as high computational cost, sensitivity to feature scaling, large memory requirements, and inefficiency in handling probabilistic uncertainty. To overcome these issues, a Naive Bayes Classifier (NBC) is introduced as the core probabilistic inference engine. NBC leverages Bayesian decision theory to estimate posterior probabilities, enabling faster training, lightweight computation, and better scalability for high-dimensional data. The framework integrates data preprocessing, class balancing, multi-model training, and Flask-based web deployment for real-time inference. Performance evaluation using accuracy, precision, recall, and F1-score demonstrates reliable and efficient anomaly detection, confirming the framework's effectiveness in modern network security.

Keywords: Real-time security monitoring, anomaly detection, authentication threats, network traffic analysis, cybersecurity, intrusion detection, probabilistic inference, data preprocessing.

1. INTRODUCTION

In the rapidly evolving technological landscape, sensors are integral components that provide critical data for decision-making processes across various applications. Ensuring the reliability and accuracy of sensor data is critical, as any discrepancies can lead to significant errors and system failures [1]. As shown in fig. 1 the importance of this issue is magnified in the context of embedded systems and the Internet of Things (IoT), where sensors operate in diverse and often harsh environments. The challenge of ensuring sensor data integrity is amplified in embedded systems and IoT networks, where sensors are often exposed to harsh and variable conditions [2]. Traditional methodologies for anomaly detection, such as signature-based Intrusion Detection Systems (IDS), have proven effective against known threats but struggle with novel and sophisticated attacks. As cyber threats and system vulnerabilities evolve, there is a pressing

need for advanced detection techniques that can adapt to emerging risks and safeguard system integrity [3].

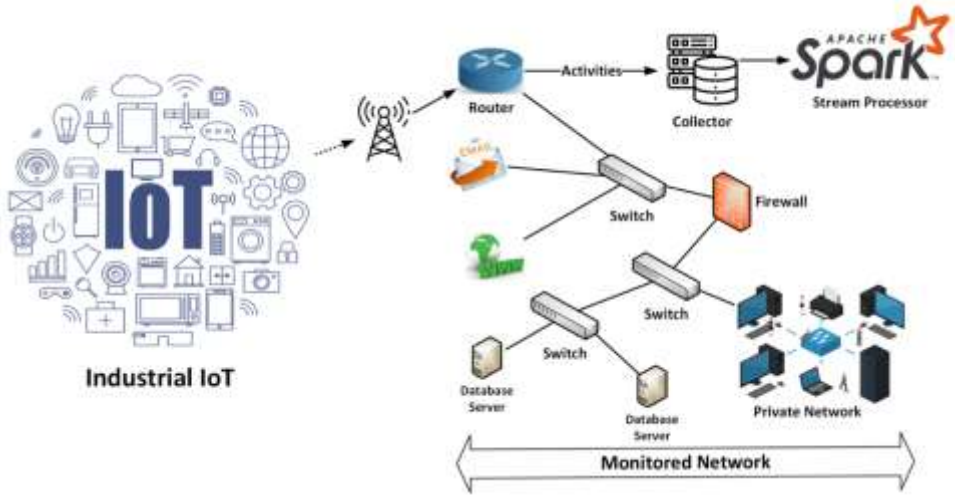

Fig. 1: Monitoring of IoT-based network traffic flows

This research addresses this critical gap by proposing an innovative approach that leverages discrete wavelet transforms (DWT) embedded within microcontrollers for real-time anomaly detection and fault isolation [4]. Wavelet transforms, particularly DWT, have emerged as powerful tools in signal processing. They allow signals to be decomposed into different frequency components and analyze localized features. The Haar wavelet from the DWT family was chosen for anomaly detection due to its simplicity and efficiency in decomposing non-stationary signals, allowing the detection of both transient and persistent faults in sensor data. Haar wavelets provide clear time and frequency localization, crucial for identifying anomalies in embedded systems. Their computational simplicity makes them ideal for real-time applications on resource-constrained devices like microcontrollers [5]. Euclidean distance was used together with DWT to quantify deviations between transformed data and a reference model, offering a straightforward and efficient way to detect faults.

2. LITERATURE SURVEY

Yang, et al. [6] Super-resolution (SR) is significant for hyperspectral image (HSI) applications. In single-frame HSI SR, how to reconstruct detailed image structures in high resolution (HR) HSI is challenging since there is no auxiliary image (e.g., HR multispectral image) providing structural information. An embedding subnet and a predicting subnet constitute the MW-3D-CNN, the embedding subnet extracts deep spatial-spectral features from the low resolution (LR) HSI and represents the LR HSI as a set of feature cubes. The feature cubes are then fed to the predicting subnet. There are multiple output branches in the predicting subnet, each of which corresponds to one wavelet sub-band and predicts the wavelet coefficients of HR HSI. The HR HSI can be obtained by applying inverse wavelet transform to the predicted wavelet coefficients. In the training stage, they proposed to train the MW-3D-CNN with L1 norm loss, which is more suitable than the conventional L2 norm loss for penalizing the errors in different wavelet sub-bands. Experiments on both simulated and real spaceborne HSI demonstrate that the proposed algorithm is competitive with other state-of-the-art HSI SR methods.

Wang, et al. [7]. experimented on old datasets, so they could not reflect the latest attack information. In addition, multi-classification experiments were conducted to sort traffic into benign traffic and six

categories of malicious attacks: BruteForce, Denial-of-service (DoS), Web Attacks, Infiltration, Botnet, and Distributed denial-of-service (DDoS). Each model showed a high accuracy in various experiments, and their multi-class classification accuracy were above 98%. Compared with the IDS of other papers, the proposed model effectively improves the detection performance. Moreover, the inference time for the combinations of CNN + RNN and CNN + LSTM is longer than that of the individual DNN, RNN and CNN. Therefore, the DNN, RNN and CNN are better than CNN + RNN and CNN + LSTM for considering the implementation of the algorithm in the IDS device.

Kim, et al. [8] Multipath errors are significantly challenging in radio navigation systems. Multipath errors in outdoor environments, such as in global navigation satellite system (GNSS) signal applications, have been widely studied for precise positioning. Multipath mitigation methods using a shallow neural network and a transfer learning-based deep neural network were respectively considered to overcome the complexity caused by the reflected signals in indoor environments. These methods classified each measurement according to whether the measurement exhibits a severe multipath error. Carrier-phase measurements broadcasted from the transmitter were used for the wavelet transform, and the magnitude values after the transform were used for neural network-based learning. Shallow and deep networks attain approximately 87.1% and 85.6% detection accuracies, respectively, and the positioning error can be reduced by 10.4% and 9.4%, respectively, after multipath mitigation.

Fu, et al. [9] addressed the issue of low detection accuracy, proposes a model for traffic anomaly detection named a deep learning model for network intrusion detection. In intrusion detection public data sets, there are serious imbalance data generally. To address data imbalance issues, this paper employs the method of adaptive synthetic sampling (ADASYN) for sample expansion of minority class samples, to eventually form a relatively symmetric dataset, and uses a modified stacked autoencoder for data dimensionality reduction with the objective of enhancing information fusion. DLNID is an end-to-end model, so it does not need to undergo the process of manual feature extraction. After being tested on the public benchmark dataset on network intrusion detection NSL-KDD, experimental results show that the accuracy and F1 score of this model are better than those of other comparison methods, reaching 90.73% and 89.65%, respectively.

Zhang, et al. [10] proposed a novel algorithm based on both wavelet leader multifractal analysis (WLM) and machine learning (ML) principles. In earlier research on unmanned aerial systems (UAS), intrusion detection systems (IDS) based on multifractal (MF) spectral analysis have been used to provide accurate MF spectrum estimations of network traffic. Such an estimation is then used to detect and characterize flooding anomalies that can be observed in an unmanned aerial vehicle (UAV) network. However, the previous contributions have lacked the consideration of other types of network intrusions commonly observed in UAS networks, such as the man in the middle attack (MITM). In this work, this promising methodology has been accommodated to detect a spoofing attack within a UAS.

Ali, et, al. [11] implemented various deep learning models, including multilayer perceptron (MLP), convolutional neural network (CNN), and long short-term memory (LSTM), alongside traditional machine learning algorithms such as logistic regression, naive Bayes, random forest, K-nearest neighbors, and decision trees. Mao, et, al. [12] employed a dynamic routing mechanism to map sample feature vectors into robust class vector representations, achieving superior generalization when detecting unseen attack types. Compared to existing FCN–Transformer models, MFEI-IDS incorporates inductive learning to handle data imbalance and small-sample scenarios. Experiments on ISCX 2012 and CIC-IDS 2017

datasets show that MFEI-IDS outperforms mainstream IDS methods in accuracy, precision, recall, and F1-score, excelling in cross-dataset validation and demonstrating strong generalization capabilities.

Mari, et al. [13] demonstrated a way to create adversarial instances of network traffic that can be used to evade detection by a machine learning-based IDS. Moreover, this traffic can be used for training in order to improve performance in the case of new attacks. Thus, a generative adversarial network (GAN) i.e., an architecture based on a deep-learning algorithm capable of creating generative models was implemented. Cao, et al. [14] presented a novel model, called Wavelet Transform-based Dual-Stream Backbone Network (WTDBNet), which effectively integrates three key strengths: the ability of the Transformer to model long-range dependencies for global context, the capability of convolutional neural networks to extract detailed local features, and the efficiency of wavelet transform in frequency-domain decomposition for enhancing edges and texture details. These components are fused via channel and spatial attention mechanisms, thereby improving the model's ability to extract discriminative features. The effectiveness of WTDBNet is validated on two widely used benchmarks for fine-grained oriented ship detection, as well as on a self-constructed dataset designed to represent complex scenarios.

Sun, et al. [15] proposed a framework that combines CNN and Transformer, employs the wavelet transform and inverse wavelet transform for encoding and decoding, and progressively embeds the edge information on the raw image in the encoding processNext, the residual structure Swin Transformer group is used to extract global features. Then, the resulting feature map and the encoder's hybrid feature map are used for high-resolution feature map reconstruction by the decoder. The experimental results show that the proposed method can achieve an excellent effect in edge information protection and visual reconstruction of images. In addition, the effectiveness of each component of the proposed model is verified by ablation experiments.

3. PROPOSED SYSTEM

The proposed system architecture operates by transforming raw network traffic into highly discriminative, multi-scale features using wavelet decomposition and advanced preprocessing, followed by intelligent classification layers that detect anomalies and authentication failures with high accuracy. The entire pipeline is designed to capture long-range attack patterns, subtle deviations in login behaviors, and complex packet-level variations that traditional systems fail to interpret. By combining Multi-Scale Wavelet Processing with powerful machine-learning decision layers, the system enhances sensitivity, reduces false alarms, and ensures robust, real-time intrusion detection suitable for enterprise and defense network environments as shown in fig. 2.

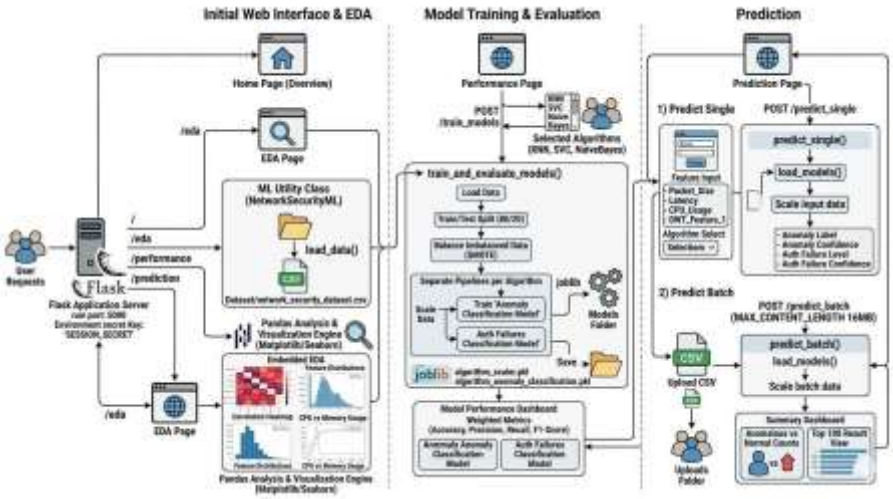

Fig. 2: Proposed system architecture

Raw Network Data Acquisition: The operational flow begins with the continuous acquisition of raw network traffic from distributed security endpoints such as routers, gateways, authentication servers, and firewall logs. This stage is crucial because long-range intrusion patterns require diverse multi-source data to identify deviations and subtle attack footprints. The system collects packet headers, connection metadata, frequency of requests, session durations, and access logs that capture both successful and failed authentication attempts. These inputs serve as the foundational evidence for detecting anomalies and unusual traffic bursts that may not be visible when using single-source monitoring systems.

Data Preprocessing and Cleaning: Once data enters the pipeline, the preprocessing layer transforms it into a standardized and noise-free structure suitable for advanced analytics. This step removes corrupted packets, duplicate entries, and incomplete authentication logs, ensuring that only meaningful and validated data flows into further processing. Normalization techniques are applied to maintain uniform scaling across diverse numerical attributes such as packet size, request count, and login intervals. Temporal alignment is also performed so that long-range dependencies such as slow attacks or progressive intrusion attempts—can be captured more accurately across chronological event sequences.

Multi-Scale Wavelet Decomposition: The next stage introduces the core innovation of the proposed system: multi-scale wavelet decomposition. Unlike traditional filters or time-domain transformations, wavelets analyze network signals at multiple resolutions simultaneously, allowing the system to detect both sudden anomalies (burst attacks) and long-term deviations (slow-paced intrusions). During this process, the raw data is decomposed into approximate (low-frequency) and detailed (high-frequency) components, revealing hidden fluctuations that attackers often exploit to bypass classic IDS models. This multi-resolution representation significantly enhances the system's ability to sense micro-level variations in packet flow and macro-level authentication irregularities.

Feature Engineering and Selection: After wavelet transformation, the system begins engineering features that capture the intelligence embedded within the decomposed signals. This step extracts statistical indicators such as entropy, variance, spike density, packet symmetry ratios, and login deviation scores, which represent refined patterns of normal and abnormal user behavior. High-dimensional features are then filtered using selection techniques to remove redundant or weak predictors, ensuring that the final

dataset contains only the most relevant attributes. This optimization enhances computational efficiency and prevents model overfitting, especially when analyzing large-scale enterprise network traffic.

Model Training Using Proposed Machine Learning Algorithms: The processed dataset is then fed into a multi-model learning environment where algorithms like NBC, KNN, and SVC are rigorously trained. Each model is exposed to thousands of labeled samples representing normal behavior, anomalies, and authentication outcomes categorized as positive, negative, or neutral. Cross-validation ensures that the model generalizes well to unseen traffic patterns, while hyperparameter tuning enhances decision boundaries, probabilistic estimations, and nearest-neighbor distances. This training phase equips the proposed system to differentiate between benign fluctuations and genuine attacks with improved precision and reduced false alarms.

Real-Time Prediction and Intrusion Detection: During live deployment, the system performs high-speed inference by transforming incoming traffic into wavelet-based features and applying the trained models to classify each event. Every network request is rapidly evaluated to determine whether it represents normal behavior, suspicious activity, or an authentication failure category. Real-time alerts are triggered for anomalies such as brute-force attacks, session hijacking attempts, excessive login failures, or unusual traffic bursts originating from unknown sources. By processing data instantly and intelligently, the system ensures robust early detection of intrusions before they escalate into major security breaches.

Continuous Learning and Adaptive Feedback Loop: The final stage introduces adaptive intelligence by feeding system outputs back into the learning layer. Detected anomalies, new attack signatures, and evolving traffic behaviors are stored to update the model's knowledge base over time. This feedback loop ensures resilience against emerging threats, supporting continuous retraining and self-improvement without requiring manual reconfiguration. As attack patterns evolve—whether through AI-based evasion or long-range stealth techniques—the system dynamically adjusts thresholds, improves classification boundaries, and maintains high detection performance in complex defense-network environments.

4. RESULTS ANALYSIS

The results section presents the key findings of a study in a clear and organized manner. It focuses on displaying the data collected through experiments, surveys, or analysis without interpretation. Typically, results are shown using tables, graphs, or charts to make patterns and trends easy to understand. This section highlights important outcomes, comparisons, and any significant relationships observed in the data. It avoids personal opinions and sticks strictly to factual information. The results section provides the foundation for discussion and conclusions in the research.

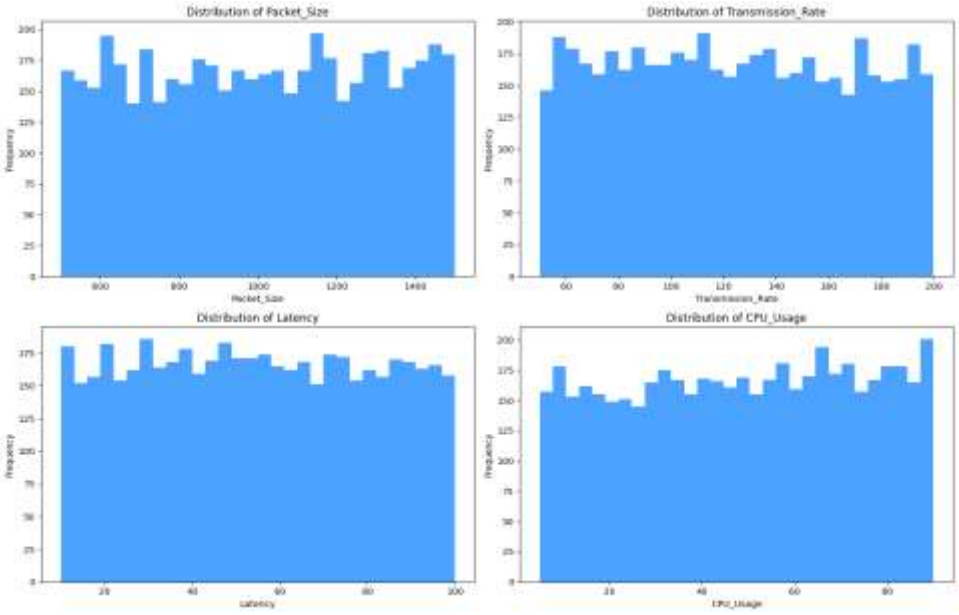

Fig. 4: Visualizing Key Feature Distributions using Histogram.

Fig. 4 depicts the distribution of important network traffic features using histogram-based visualizations. The figure includes histograms for packet size, transmission rate, latency, and CPU usage. Packet size values range approximately between 500 and 1500 units, while transmission rate values range between about 50 and 200 units. Latency values are distributed between roughly 10 and 100 units, and CPU usage ranges between approximately 5 and 90 percent. These distributions help researchers understand how network characteristics vary across the dataset. Such analysis is useful for identifying feature patterns and detecting potential outliers before model training.

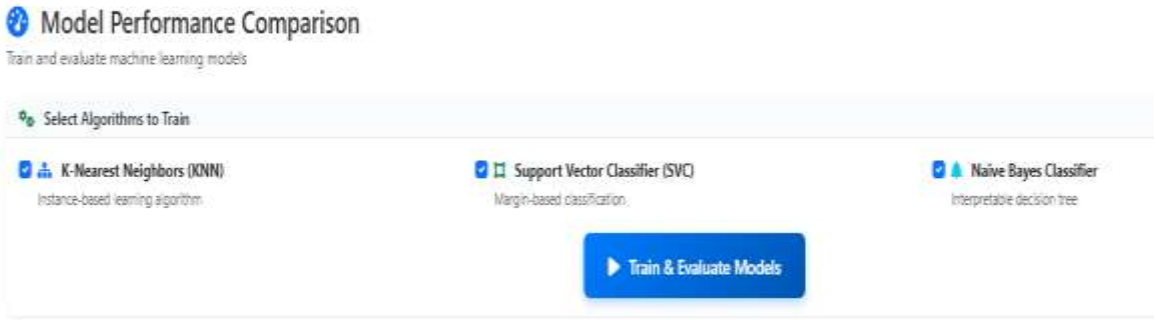

Fig. 5: Model Performance Comparison Interface for Training and Evaluation.

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 NB 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.

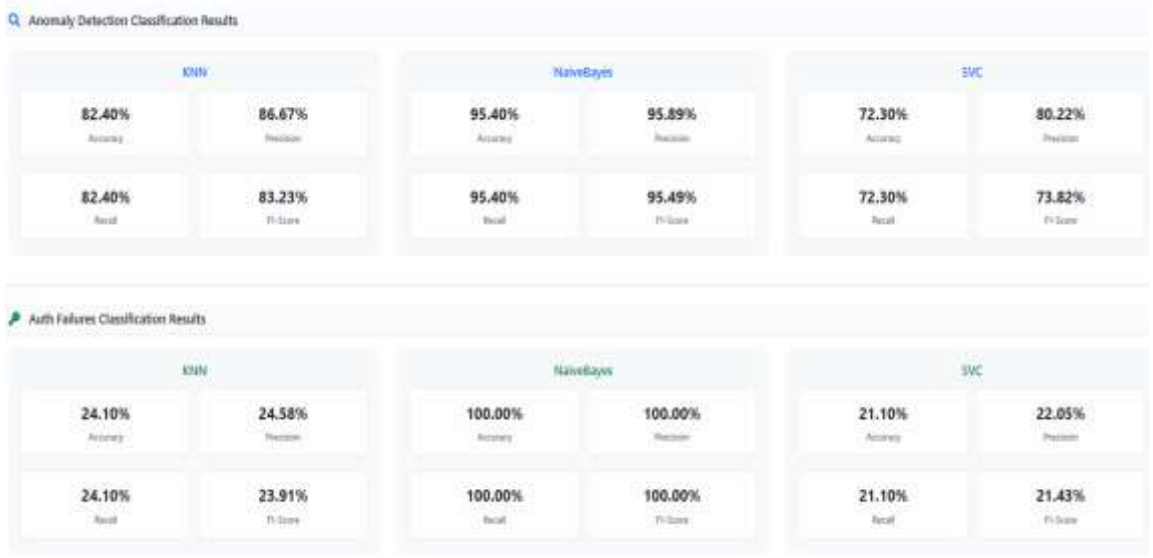

Fig. 6: Model Performance Evaluation Interface after Training the models.

Fig. 6 presents the evaluation results obtained after training the selected machine learning models. For anomaly detection classification, Naive Bayes 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. 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.

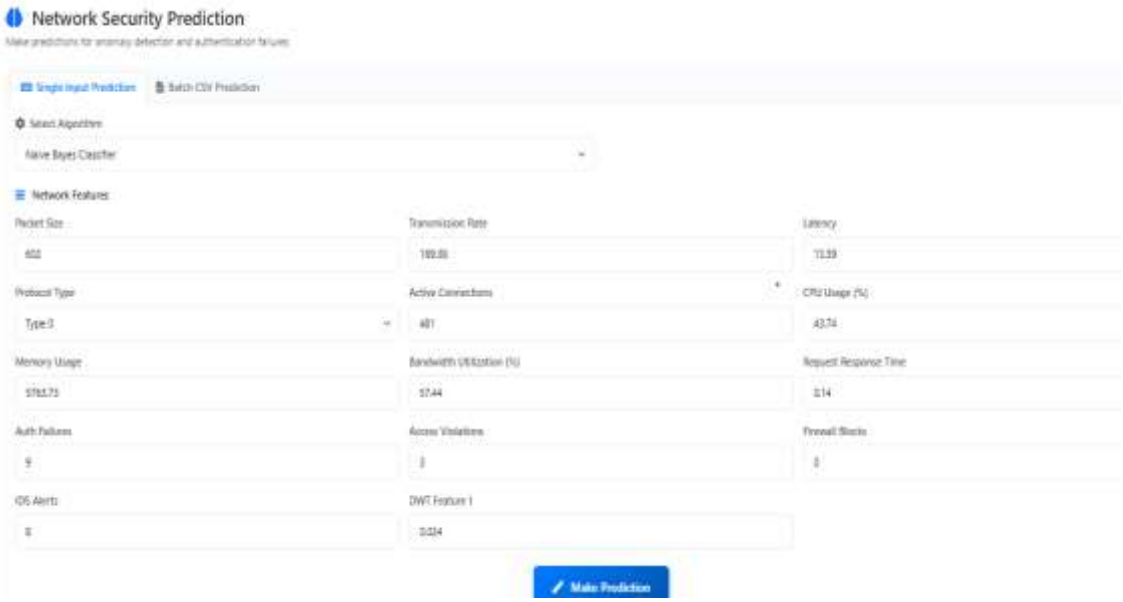

Fig. 7: Network Security Prediction Interface for Single Input Analysis.

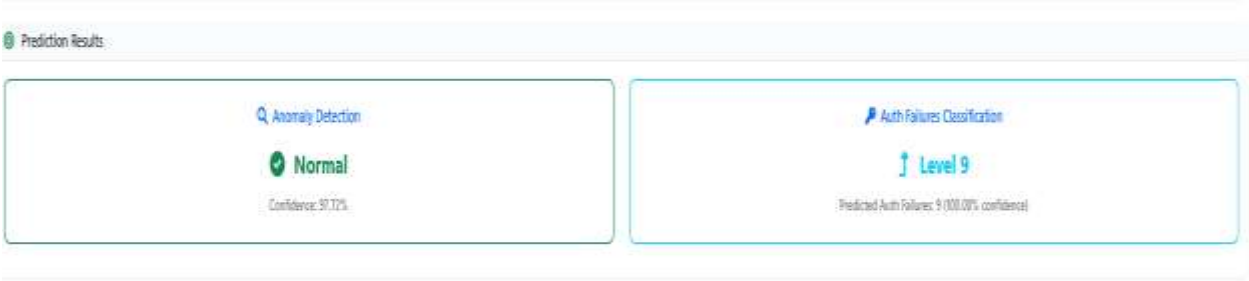

Fig. 8: Output of the Test Data.

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 analyze 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]. 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

[7]. Wang, Y.-C.; Houng, Y.-C.; Chen, H.-X.; Tseng, S.-M. Network Anomaly Intrusion Detection Based on Deep Learning Approach. Sensors 2023, 23, 2171. https://doi.org/10.3390/s23042171

[8]. 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

[9]. Fu, Y.; Du, Y.; Cao, Z.; Li, Q.; Xiang, W. A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. Electronics 2022, 11, 898. https://doi.org/10.3390/electronics11060898

[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]. 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

[15]. 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