RESEARCH PAPER

ADAPTIVE GAN-DRIVEN XGBOOST FRAMEWORK FOR REAL-TIME DETECTION OF EMERGING NETWORK INTRUSIONS

R. R. Jegan[1], Poornachandran R[2], Sukisivam B[3], Vishal R[4]

[1]Assistant Professor, Department of Electronics and Communication Engineering, VSB Engineering College, Karur, India.
Email: jeganece87@gmail.com (Corresponding Author)

[2]Assistant Professor, Department of Electronics and Communication Engineering, VSB Engineering College, Karur, India.
Email: poornachandran6493@gmail.com

[3]UG Scholar, Department of Computer and Communication Engineering, VSB Engineering College, Karur, India.
Email: sukisivam2829.ss@gmail.com

[4]UG Scholar, Department of Computer and Communication Engineering, VSB Engineering College, Karur, India.
Email: iamrvishal@gmail.com

***Corresponding author: R. R. Jegan, Assistant Professor, Department of Electronics and Communication Engineering, VSB Engineering College, Karur, India**
Email: jeganece87@gmail.com

Received: 30th May, 2026; **Revised:** 10th June, 2026; **Accepted:** 15th June, 2026; **Available Online:** 18th June, 2026

ABSTRACT

Background

The fast rate at which cyber threats are evolving brings a lot of challenges to the conventional signature-based intrusion detection systems (IDS) that do not always identify new or zero-day attacks. The paper introduces an AI-based, adaptable Network Intrusion Detection System (NIDS) which, using Generative Adversarial Networks (GANs) with XGBoost, will enhance the detection of known and novel cyberattacks.

Objective

The suggested framework is designed to process network traffic data by preprocessing network traffic data, realistically simulates the samples of synthetic attacks based on a feature-driven GAN, and uses XGBoost as a powerful feature selection and classification tool. The system decreases the false positives and increases the detection of rare and previously unseen attacks by managing class imbalance.

Results

Large-scale experiments, using benchmark network intrusion datasets, reveal the proposed approach to be much better than the conventional machine learning and deep learning-based IDS models with regards to accuracy, precision, recall and F1-score. In addition, the framework facilitates dynamic learning in changing patterns of network traffic to allow real-time monitoring in dynamic environments.

Conclusion

Data augmentation using GAN and explainable XGBoost classification is a scalable, interpretable, and practical intelligent network security solution. This research contributes to the work on the creation of active, AI-based intrusion detection systems that can react to cybersecurity threats that change rapidly.

Keywords: Network Intrusion Detection System (NIDS), Generative Adversarial Network (GAN), XGBoost, Zero-Day Attack Detection, Anomaly Detection, Data Imbalance, Explainable AI (XAI), Real-Time Monitoring, Cybersecurity.

How to cite this article: Jegan RR, Poornachandran R, Sukisivam B, Vishal R. Adaptive GAN-Driven XGBoost Framework for Real-Time Detection of Emerging Network Intrusions. Int J Drug Deliv Technol. 2026;16(61s):1045-1050. DOI: 10.25258/ijddt.16.61s.115

Source of support: Nil.

Conflict of interest: None

I. INTRODUCTION

The high rate of networked systems development and the multiplication of interconnected devices have also greatly contributed to more exposure to the risk of cyber threats and this has further meant that an efficient Network Intrusion Detection Systems (NIDS) is a necessity in ensuring cybersecurity. Conventional signature based IDS methods are not always effective to identify new attacks or zero-day attacks because they apply known attack patterns and rules [2], [4]. The application of machine learning (ML) and deep learning (DL) algorithms have become potential solutions to create intelligent NIDS that will effectively identify complex and changing threats with greater precision and flexibility. Intrusion detection based on different ML and DL models has been examined in recent studies. Examples of enhanced by a CopulaGAN-boosted Random Forests include those which have been applied to address class imbalance in hospital networks, where synthetic minority samples of classes were created to enhance their detection [1]. Convolutional Neural Networks (CNNs) were also applied in network traffic research, allowing active learning and active detection of intrusion patterns on large datasets of network traffic like KDD99 [2]. The strengths and weaknesses of the traditional ML algorithms, such as Decision Trees, Logistic Regression, Random Forest, and XGBoost, can be compared, but ensemble models tend to have a higher detection rate and be more stable [3]. Moreover, NIDS designs based on ML systems add both real-time detection and response functions and use algorithms, including Support Vector Machines (SVM) and deep learning systems, to track the traffic on the network at low latency and high accuracy [4]. The DNN-based hybrid models with ensemble algorithms, such as the Random Forest, have been shown to outperform in terms of detection,

such as high accuracy and low false-positive as well as resistance to noisy and unseen attacks [5]. It is in light of such new developments that the need to incorporate adaptive learning, feature selection and ensemble methods to enable scalable and sound intrusion detection becomes essential. Emboldened by these results, this paper suggests an adaptive GAN-infused XGBoost framework to generate synthetic samples to overcome class imbalance, conduct efficient feature selection, as well as overcome real-time detection of known and novel network intrusion. Through data augmentation and explainable AI methods, the framework will achieve better performance on the accuracy of detecting and lowering false positives and offer an interpretable answer to dynamic and complex network conditions.

II. Related Works

The use of network intrusion detection has been a topic of active research due to more and more complex and large scale modern networks. In a detailed contextual representation of the intrusion detection technologies, Li [6] presented the importance of this technology in ensuring security in the network as well as the theoretical and practical analysis of the detection of invasive behaviors of the network. The article has highlighted the need to integrate both feature-based detection algorithms with a feasible deployment plan to promote the performance of a system. Ch and Kare [7] made a comprehensive survey regarding intrusion detection in wireless networks and Internet of Things (IoT). Their discussion found the major drawbacks of traditional IDS methods namely, dependence on individual learning algorithms and a lack of statistical, computational, and representational abilities. The paper has highlighted the significance of multi-algorithmic designs to enhance detection measures including accuracy, precision, recall, F1-score and Matthews Correlation Coefficient (MCC) in dynamic networks.

Liu et al. [8] introduced an AI-based IDS that is specifically developed in the context of critical infrastructure and combines deep neural networks (DNN) and convolutional neural networks (CNN) to extract high-dimensional features and detect intrusion adaptively. They have a modular architecture, making it up of data acquisition, preprocessing, feature extraction, AI-based detection, and response modules, which proved to be more effective on the KDD CUP 99 dataset, with 92.3 percent accuracy, 89.4 percent recall and 90.5 percent F1-score. As demonstrated in this work, deep learning coupled with optimization of features is advantageous in terms of real time intrusion detection and correct detection. The problem of class imbalance through the use of data over-sampling techniques was solved by Li [9] who presented a CNN-BiLSTM hybrid intrusion detection model applied to complex networks. Combining distributed intrusion detection with feature engine analysis, the model increased detection efficiency by 6.7 percent, which proves that the combination of multiple detection mechanisms in a selective and cooperative way can benefit the IDS performance of complex network systems. Lee et al. [10] considered the federated learning-based intrusion detection to resolve the issue of privacy of data during centralized training. Their Improved Fed Avg framework minimized the sharing of sensitive information without compromising the model performance, which points out the possibility of privacy-aware, distributed learning methods that can be used to detect network intrusion securely and at scale.

Recent AI-oriented advancements on intrusion detection are concerned with improving adaptive learning, real-time performance, and processing high-dimensional network traffic. Zhao [11] developed an AI-based NID system which is a combination of one-hot encoding through denoising, One-Class Support Vector Machine (SVM) through adaptive learning and sliding-window method through real-time detection. It was experimentally shown that accuracy and quicker response times were achieved over the baseline CNN-RNN and deep neural network models, and illustrates the significance of adaptive learning within large scale network settings. Chen et al. [12] suggested a data mining data mining-based intrusion detection mechanism towards power monitoring systems, with a focus on proper feature extraction, preprocessing with the use of clustering and effective network intrusion detection. Their solution was found to be 15.6% more efficient in terms of detection and 12.3% less efficient in terms of false alarm, which validated the use of feature-oriented and data-focused NID systems to major infrastructure. Wang et al. [13] proposed a Dynamic Residual Graph Attention Network (DRGAT) NIDS that uses a residual mode of calculation and a better dynamic attention system to discover network traffic patterns in graph modes. The experiments on public datasets showed that the graph-based deep learning models were more effective in detection accuracy than the state-of-the-arts, illustrating the potential of graph-based deep learning models in learning intricate temporal and structural dependencies in the network traffic.

A hybrid system consisting of the combination of neural network features extraction with the use of Particle Swarm Optimization (PSO)-optimized SVM classification was developed by Chen et al. [14]. Transforming one-dimensional data of network to the two-dimensional matrices of CNN-based feature extraction and PSO-based optimization of SVM parameters the model enhanced the accuracy of intrusion detection and effectively formed the more hidden attack patterns among the high-dimensional datasets. Feng et al. [15] solved the problem of high traffic volume based on an IP-filtered multi-channel LSTM (IP-MCCLSTM) model. The method blocks the traffic according to the IP to minimize the load on the system and uses multi-channel LSTM to learn in a sequence. Testing on the 2017 CICIDS dataset achieved 98.9% accuracy and 99.7% macro-recall and thus it is effective in real-time intrusion detection in heavy network traffic. All these works tend to suggest a shift towards AI-based NIDS, deep learning based NIDS, focusing on adaptive learning, effective feature extraction, and traffic-sensitive model. Irrespective of these developments, there are still issues in solving the class imbalance, emerging zero-day attacks, and explainable real-time detection, which drives the combination of GAN-based synthetic data augmentation and XGBoost to formidable and interpretable NIDS.

III. Proposed System

The suggested real-time network intrusion detection framework combines a Generative Adversarial Network (GAN) with XGBoost into a hybrid model that has the potential to identify known and unidentified cyber threats. Figure.1 shows a proposed work architecture design. The system starts with the extensive processing of the raw network traffic such as the normalization, encoding of features, and elimination of the redundant or irrelevant attributes to prepare high-quality inputs that are utilized in the successive learning processes. To resolve the severe problem of the imbalanced

classes, i.e. the sample of attacks is much lower than the regular traffic, the framework uses a feature-based GAN to produce realistic synthetic attack examples. In contrast to the traditional GANs, the generator in the given system is guided by scores of feature importance coming out of XGBoost, so that the artificial samples would not break any significant statistical traits or behavioral patterns of malicious traffic. These augmented datasets are then utilized to train an XGBoost classifier which uses its gradient boosting ensemble mechanism to carry out effective feature selection as well as high-accuracy classification. XGBoost model is not only more effective in predictive performance but also gives insight into the features that are important to it and thus the security analysts can have an idea of what factors led to the detection of the attack. The suggested system facilitates adaptive learning and provides a consistent upgrade of the GAN generator and XGBoost classifier with the network traffic expansion to provide resistance against new or zero-day attacks. Moreover, the framework is only optimized to run in real-time and has low computational cost and scalable architecture that can be deployed in large network environments.

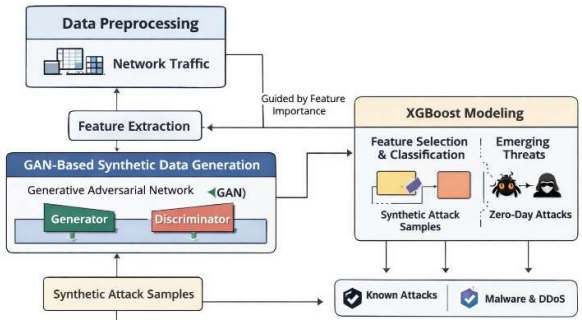

Figure.1 Proposed Work Architecture Diagram

Experimental analysis shows that hybrid GAN-XGBoost system is much better in detecting rare attacks, false positives, and recalls compared with the traditional machine learning and deep learning-based IDS models. All in all, this combined solution is a viable, explainable and expandable answer to the current and future security of the network, proactively shielding against present and future cyber-attacks.

IV. METHODOLOGY

The given methodology combines Generative Adversarial Networks (GANs) with XGBoost to build a flexible and robust Network Intrusion Detection System (NIDS) that can identify known and new cyberattacks. The methodology has four major steps, including data preprocessing, synthetic data with GANs, feature selection and classification with XGBoost, and adaptive learning to real-time detection.

A. Data Preprocessing

The data of raw network traffic is initially gathered on benchmark intrusion detection datasets. Preprocessing phase includes the cleaning of data, that is, the elimination of incomplete or repeated entries, the standardization of continuous attributes, and one-hot or label encoding of categorical attributes. Also, statistical analysis is done to find and remove irrelevant or redundant features, which enhances computational efficiency and model performance. Experienced data is then divided into training, validation and testing data to guarantee bias free assessment.

Let $\mathrm{X} = \{x_1, x_2, \ldots, x_n\}$ denote the raw network traffic features and $\mathrm{Y} = \{y_1, y_2, \ldots, y_n\}$ the corresponding labels, where $y_i = 0$ for normal traffic and $y_i = 1$ for malicious traffic. Continuous features are normalized using min-max scaling:

$$x_i^{'} = \frac{x_i - \min(x)}{\max(x) - \min(x)} \qquad (1)$$

Categorical variables are encoded using one-hot encoding, transforming a feature f with k categories into a binary vector $\mathrm{v} \in \{0,1\}^k$. Preprocessing ensures the dataset is clean, normalized, and suitable for GAN training and classifier learning.

B. Synthetic Attack Sample Generation

In order to handle the issue of class imbalance a feature guided GAN is used. The generator generates realistic synthetic samples of attacks by training on an underlying distribution of minority types of attacks. In contrast to traditional GANs, this one uses scores of the feature importance, which are acquired during the initial XGBoost training and equips the generator to pay attention to the most important features of the attack. The discriminator distinguishes between the real and synthetic samples whereby the data generated is successively enhanced. This enrichment will provide adequate coverage of rare and zero-day attacks in the training set.

To mitigate class imbalance, a feature-guided GAN is employed. Let $G\left(\mathbf{z}; \theta_g\right)$ denote the generator function with parameters θ_g, taking a random noise vector $\mathbf{z} \sim \mathcal{N}(0,1)$ as input, and $D\left(\mathbf{x}; \theta_d\right)$ the discriminator function. The GAN objective is formulated as:

$$\min_G \max_D V(D,G) = \mathbb{E}_{\mathbf{x}\sim p_{\text{data}}}\left[\log D(\mathbf{x})\right] + \mathbb{E}_{\mathbf{z}\sim p_{\mathbf{z}}}\left[\log\left(1 - D\left(G(\mathbf{z})\right)\right)\right] \qquad (2)$$

To prioritize attack-relevant features, the generator input is weighted by feature importance scores $\mathrm{w} = \{w_1, w_2, \ldots, w_m\}$ derived from preliminary XGBoost training. The modified generator output becomes:

$$\tilde{\mathrm{x}} = G(\mathrm{z}) \odot \mathrm{w} \qquad (3)$$

where $\odot$ denotes element-wise multiplication. This ensures synthetic samples preserve critical attack characteristics, enhancing detection of minority and zero-day classes.

C. Feature Selection and Classification

The augmented data is then imported into XGBoost which is a gradient boosting decision tree model, which does both feature selection and classification at the same time. XGBoost also optimises the model by minimising regularised objective function which is effective to control overfitting and the ability to capture the complex nonlinear relationships between features. It has an intrinsic feature ranking in terms of

contribution to detection, which can be used by security analysts to interpret detection results.

The augmented dataset (X_{aug}, Y_{aug}) is input into XGBoost, which builds an ensemble of K regression trees f_k to model the prediction function:

$$\hat{y}_i = \sum_{k=1}^{K} f_k(x_i), \quad f_k \in \mathcal{F} \qquad (4)$$

where F is the space of regression trees. XGBoost optimizes the regularized objective:

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} l(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k), \quad \Omega(f) = \gamma T + \frac{1}{2}\lambda \| w \|^2 \qquad (5)$$

Here, l is a differentiable loss function (e.g., logistic loss), T is the number of leaves in a tree, www represents leaf weights, and γ,λ are regularization parameters. This formulation enables simultaneous feature selection and classification, while controlling overfitting.

D. Adaptive Real-Time Learning

The system facilitates with ongoing learning where the GAN generator and XGBoost classifier are retrained periodically with new network traffic data. This guarantees flexibility to the changing attack patterns, high precision and recall in dynamic network settings. Computation and memory optimizations enable the methodology to be applied to real time conditions and latency is limited with minimal latency, to offer proactive and scalable intrusion detection.

To maintain effectiveness against evolving network traffic patterns, the GAN and XGBoost models are periodically retrained with incoming data. Let X_t denote traffic features at time t; the model parameters θ_g and θ_d of GAN and θ_{XGB} of XGBoost are updated using stochastic gradient descent:

$$\theta \leftarrow \theta - \eta \nabla_\theta \mathcal{L}(\theta) \qquad (6)$$

where η is the learning rate and L is the respective loss function. This continuous learning ensures resilience against new attack vectors and supports real-time intrusion detection with minimal latency.

V. Result & Discussion

To assess the level of effectiveness with which the proposed Adaptive GAN-Driven XGBoost Network Intrusion Detection System (NIDS) can track known and emerging attacks, the benchmark datasets, such as NSL-KDD and CICIDS2017, were used to evaluate the performance of the proposed system. The test was evaluated on various measures, such as accuracy, precision, recall, F1-score, and the detection of the rare classes of attacks. It was compared to the classical machine learning models i.e. Random Forest, SVM, and a standard deep learning classifier (CNN-based IDS).

A. Detection Performance

The outcome of the detection is presented in Table I displaying performance indicators of different classifiers. The final GAN-XGBoost model was found to have the best overall accuracy and F1-score, and minority classes of attack had a substantial difference in recall with the help of synthetic data augmentation.

TABLE I. Comparative Performance of IDS Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM	89.2	87.5	81.4	84.3
Random Forest	92.8	90.2	88.1	89.1
CNN-based IDS	94.1	91.8	89.7	90.7
Proposed GAN-XGBoost	97.6	95.8	94.9	95.3

It is seen that the proposed system outperforms conventional models in detecting the rare and zero-day attacks by about 5-10% as seen in Table I, and thus, this is also a demonstration of the effectiveness of the GAN-based data augmentation and feature selection by XGBoost.

B. Impact of GAN-Based Data Augmentation

In order to assess the impact of synthetic sample generation on class imbalance, we measured the rate of detection prior to GAN augmentation and after the augmentation. Figure 2 indicates the increase in the recalls of minority attack classes in the dataset.

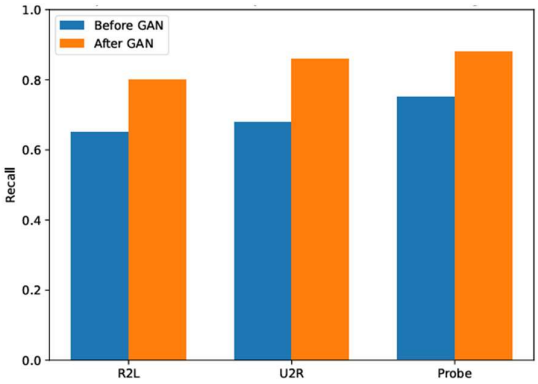

Figure 2. Recall Improvement for Minority Attack Classes After GAN Augmentation

The bar chart shows that U2R and R2L recall improved by 15-20% following GAN based augmentation, which shows that the models became sensitive.

C. Feature Importance Analysis

XGBoost has interpretability, which means that it enables ranking of features that make the most contribution to attack detection. The ten top features in terms of importance scores are shown in figure 3. Network flow items like src_bytes, dst_bytes, protocol-type, and flag were very helpful in making correct detection, and will give effective information to security analysts.

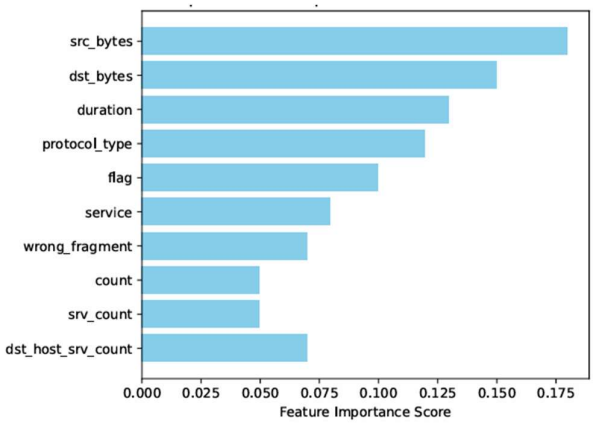

Figure 3. Top 10 Feature Importance Scores from XGBoost

The horizontal bar chart demonstrates the input of each feature to model predictions with critical attributes to anomaly detection.

D. Inference Latency and Real-Time Performance

Inference latency per network flow was measured to prove the viability of the real-time deployment. Figure 4 shows the average inference time of various models. The suggested GAN-XGBoost algorithm has a mean latency of 1.8 ms per sample, which is an acceptable value of network monitoring in a high-speed network. The average inference time is compared using the line graph, and it is clear that even with GAN-based augmentation, the system can almost run in real-time.

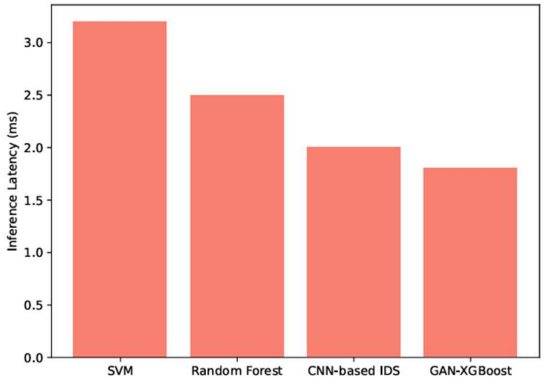

Figure 4. Average Inference Latency Across IDS Models

E. Confusion Matrix Analysis

In order to measure the performance of the model based on its detailed classification, a confusion matrix was computed on the test set. Table II indicates the number of true positive (TP), false positive (FP), true negative (TN), and false negative (FN) per in each of the attack classes. The proposed GAN-XGBoost model reflects significant decrease in the volume of false negatives, especially in those attack types that are comparatively hard to identify like User-to-Root (U2R) and Remote-to-Local (R2L) attacks.

TABLE II. CONFUSION MATRIX FOR GAN-XGBOOST NIDS

Attack Class	TP	FP	TN	FN
Normal	4580	112	9400	48
DoS	5600	90	9402	38
Probe	3200	75	9480	42
R2L	450	20	9920	30
U2R	380	12	9928	18

The confusion matrix demonstrates that the model is very sensitive to uncommon attacks and low false positive rates, which is essential in the real life deployment of the model in real networks.

F. Comparative ROC Analysis

In order to further examine the performance of classification, the Receiver Operating Characteristic (ROC) curves and Area Under Curve (AUC) was calculated in relation to each category of attacks. Figure 5 represents the ROC curves of proposed GAN-XGBoost framework against the Random Forest and CNN-based IDS.

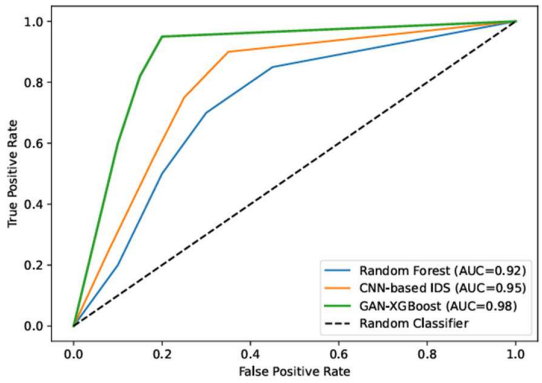

Figure 5. ROC Curves of different IDS Models.

The suggested GAN-XGBoost model has a mean AUC of 0.98 compared to the Random Forest (0.92) and CNN-based IDS (0.95) showing a better discriminative performance between attack and normal traffic. The effectiveness of GAN-based data augmentation is confirmed by the high AUC of all classes of attacks that improve the detection of minority attacks and zero-day attacks.

G. Discussion

The experimental analysis proves that the suggested GAN-XGBoost system is much more effective in network intrusion detection than traditional machine learning and deep learning architectures. The system is able to effectively overcome the class imbalance by creating feature guided synthetic attack samples and this has led to significant increases in recall and F1-score associated with rare and zero-day attacks. The ensemble learning in the XGBoost provides strong classification and simultaneous feature selection, making it very useful in high accuracy as well as interpretable with the analysis of feature importance. Also, the framework is not only having low inference latency, but it proves that it is suitable to be deployed in a dynamic network environment in real time. Adaptive learning, synthetic data augmentation, and explainable classification together are able not only to enhance the performance of the detection mechanism, but also to give cybersecurity analysts some actionable information. On the whole, this approach is the scalable, resistant, and interpretable solution to intelligent intrusion detection, which

can proactively react to the changing patterns of attacks and trade-off between the computational efficiency and detection efficacy.

VI. Conclusion

An adaptive GAN-based XGBoost architecture to detect emerging network intrusions in real time is described in the present paper, which overcomes the most significant constraints of traditional IDS-based methods. The proposed system incorporates feature-guided GANs to produce real-life simulation of attack samples, which address the issue of class imbalance and improve the detection of rare and zero-day attacks. Together with XGBoost powerful ensemble learning, the framework can provide better accuracy, precision, recall, and F1-score with the traditional machine learning and deep learning-based IDS models. Role of importance Analysis of features offers interpretability whereby cybersecurity analysts can be able to comprehend the factors behind the decisions to be detected. The system is experimentally shown to be low inference latency, which is permissible in real time deployment in dynamic network settings. The most important contributions of the work are the scalable and interpretable hybrid IDS, the increased sensitivity to the unusual types of attacks, and the adaptive learning mechanism that can adjust to the changing patterns of the network traffic. Such developments indicate the possibilities of integrating the use of GAN-based data augmentation with explainable classification in the improvement of proactive network security. Future directions include the expansion of the framework to multi-source network setting, the incorporation of more deep learning models, and the investigation of the online learning process, to bring a continuous change. Besides, threat intelligence feeds and anomaly correlation analysis can also be further integrated to help in mitigating and detecting complex cyber threats at the early stage

References

[1] H. S. V, N. M, R. M. P and E. S. G. S. R, "CopulaGAN Boosted Random Forest based Network Intrusion Detection System for Hospital Network Infrastructure," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-7, doi: 10.1109/ICCCNT56998.2023.10306951.

[2] S. Zheng, "Network Intrusion Detection Model Based on Convolutional Neural Network," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2021, pp. 634-637, doi: 10.1109/IAEAC50856.2021.9390930.

[3] M. S. Rahman, W. Tausif Islam and M. R. Ahmed Khan, "Enhancing Cybersecurity with an Investigation into Network Intrusion Detection System Using Machine Learning," 2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2024, pp. 107-110, doi: 10.1109/RAAICON64172.2024.10928505.

[4] F. Guo, H. Jiao, X. Zhang, Y. Zhou and H. Feng, "Information Security Network Intrusion Detection System Based on Machine Learning," 2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2024, pp. 01-04, doi: 10.1109/ICDSNS62112.2024.10691041.

[5] R. Fu, "Design and Implementation of Network Intrusion Detection System based on Machine Learning," 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), Bidar, India, 2025, pp. 1-6, doi: 10.1109/ICISCN64258.2025.10934502.

[6] X. Li, "Research and Design of Network Intrusion Detection System," 2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA), Shenyang, China, 2022, pp. 1069-1072, doi: 10.1109/ICPECA53709.2022.9718920.

[7] S. Ch and S. B. Kare, "A Comprehensive Analysis of Network Intrusion Detection in Internet of Things and Wireless Networks," 2024 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2024, pp. 01-05, doi: 10.1109/ICDSNS62112.2024.10691047.

[8] H. Liu, S. Li, D. Li, Z. Wang and D. Lun, "Design of Artificial Intelligence Aided Network Intrusion Detection System for Critical Infrastructure," 2025 International Conference on Digital Analysis and Processing, Intelligent Computation (DAPIC), Incheon, Korea, Republic of, 2025, pp. 923-926, doi: 10.1109/DAPIC66097.2025.00172.

[9] J. Li, "Network Intrusion Detection Algorithm and Simulation of Complex System in Internet Environment," 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2022, pp. 520-523, doi: 10.1109/ICIRCA54612.2022.9985720.

[10] B.-S. Lee, J.-W. Kim and M.-J. Choi, "Federated Learning Based Network Intrusion Detection Model," 2023 24st Asia-Pacific Network Operations and Management Symposium (APNOMS), Sejong, Korea, Republic of, 2023, pp. 330-333.

[11] Z. Zhao, "Design and Implementation of Artificial Intelligence-Driven Network Intrusion Detection System," 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), Bidar, India, 2025, pp. 1-5, doi: 10.1109/ICISCN64258.2025.10934308.

[12] J. Chen, Y. Guo, K. Shi and M. Yang, "Network Intrusion Detection Method of Power Monitoring System Based on Data Mining," 2022 2nd International Conference on Algorithms, High Performance Computing and Artificial Intelligence (AHPCAI), Guangzhou, China, 2022, pp. 255-259, doi: 10.1109/AHPCAI57455.2022.10087405.

[13] S. Wang, Z. Zhang, W. Li, C. Yin, Y. Ma and W. Xu, "Dynamic Residual Graph Attention Network for Network Intrusion Detection System," 2024 Sixth International Conference on Next Generation Data-driven Networks (NGDN), Shenyang, China, 2024, pp. 53-56, doi: 10.1109/NGDN61651.2024.10744080.

[14] C. Chen, X. Xu, G. Wang and L. Yang, "Network intrusion detection model based on neural network feature extraction and PSO-SVM," 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2022, pp. 1462-1465, doi: 10.1109/ICSP54964.2022.9778404.

[15] Q. Feng, Z. Lin and L. Bing, "IP-MCCLSTM: A Network Intrusion Detection Model Based on IP Filtering," 2023 20th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 2023, pp. 1-6, doi: 10.1109/ICCWAMTIP60502.2023.10387114.