INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

Enhancing Detection of Zero-Day Attacks in Cloud Infrastructure using Ensemble RBFNN with GAN-based Data Augmentation

Sukant Kumar Sahoo[1]*, Smitaprava Mishra[1], Biswaranjan Jena[1]

1 Department of Computer Science and Engineering (ITER), SOA (Deemed to be University) Bhubaneswar, Odisha. India

OPEN ACCESS

Received: 20/07/2025

Accepted: 25/08/2025

Published: 07/10/2025

Citation: Sahoo SK, Mishra S, Jena B (2025) Enhancing Detection of Zero-Day Attacks in Cloud Infrastructure using Ensemble RBFNN with GAN-based Data Augmentation. Indian Journal of Science and Technology 18(36): 2953-2963. https://doi.org/10.17485/IJST/v18i36.1268

* **Corresponding author**.

sukant0203@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The main objective of this study was to develop a novel and intelligent framework by integrating the Generative Adversarial Network (GAN) based data augmentation technique with ensembled Radial Basis Functions Networks (RBFNNs). The goal was to address the challenges of scarcity of training data and false positive cases and efficiently detect zero-day intrusion attacks in real-time with higher precision and accuracy. **Methods:** This study has proposed a novel framework for developing an IDS model, which was designed by integrating an ensemble of Radial Basis Function Neural Networks (RBFNNs) with Generative Adversarial Network (GAN) based data augmentation. This model was trained and tested with popular benchmark real-world datasets, augmented with GAN-based synthetic data, and outperformed traditional classification models. **Findings:** The proposed model achieved an accuracy of 98.7% and under 1.2% false positive rate (FPR) for zero-day attack detection, and demonstrated superior performance, as compared to standalone classifiers like Random Forest, SVM, CNN, and standard RBFNN. **Novelty:** The results suggested that ensembled learning along with generative data augmentation can help in building adaptable, intelligent and resilient IDS systems.

Keywords: Zero-day attack; Cloud Security; Resilient IDS; Ensemble Learning; GAN Data Augmentation

1 Introduction

Cloud computing has been most relevant solution for many enterprises due to its flexibility, scalability, out of the box security features, and cost-effectiveness. The use of virtual machines, serverless services, globally available and distributed databases, generate huge amount of network traffics in the cloud system. This transformation often challenges traditional security models, due to misconfigurations, dynamic workloads, and evolving threat vectors in cloud networks. Attackers exploit the dynamic and flexible features of cloud services to introduce attack vectors using various intrusion

techniques. Zero-day attacks are specifically dangerous as they are difficult to detect and most of the times remain undetected until they cause a significant damage. Traditional signature-based IDS[1] often fail to detect these attacks, as the signature of these new attacks are not available in the attack-signature databases.

Use of Machine Learning (ML) and Deep Learning (DL) techniques[2] have played significant roles in detecting anomalies that differ from normal behaviors to detect network intrusions in cloud computing environments. Their ability to process and analyze, complex and huge volume of data, with their models trained on wide varieties of datasets, help in building efficient and robust IDS systems. RBFNNs have been popular candidates for their simple structure, lightweight and ability to quickly learn complex datasets. The use of GAN models[3] helps in generating synthetic real-world data which can be augmented with existing datasets to enhance the representation of data samples meant for training purpose.

In this research work we have proposed to use an ensemble of RBFNNs which will be individually trained and produce an aggregated output to improve the detection accuracy. A conditional GAN (cGAN) module was used to enhance the training dataset to balance the data representation with realistic and rare synthetic data, that would help in building more intelligent and adaptable IDS for zero-day attack detection. The overall system was designed to improve the detection performance accuracy with low FPRs. Following is the summary of this research work:

- A novel hybrid framework combining ensemble RBFNN and GAN-based data augmentation for robust and accurate zero-day attack detection.
- A generative augmentation strategy that addresses the class imbalance problem by synthesizing realistic zero-day attack samples.
- An ensemble learning design that enhances generalization and mitigates overfitting in high-dimensional cloud network traffic data.
- Experimental validation on real-world datasets, that demonstrated superior performance compared to existing methods.

Zero-day attacks have been a challenging concern in the modern application systems deployed in cloud computing networks. Traditional IDS most of the time fail to detect these kinds of attacks due to their unpredictability natures in dynamic and flexible cloud infrastructures. Also, the scarcity of training data to train the systems to be adaptable to such kind of threats have become major concerns. In this section we have done a comprehensive review of related works already done by researchers in the past.

1.1 Traditional Intrusion Detection Systems (IDS)

Traditional IDSs are broadly classified as signature-based, and anomaly-based systems. Signature-based IDSs[4] are developed using a database of know and established attack signatures. While these IDSs effectively help in detecting the established attacks, they often fail to detect zero-day attacks with emerging and new threat types. Anomaly-based IDSs on the other hand are based on a baseline normal behavioral pattern. They are implemented as statistical model, rule-based, or threshold-based behavioral matching systems. Any deviation from normal baseline behavior is detected as potential threat. Singh, K. P. et al.[5], have conducted a performance assessment of open-source based IDSs for small and medium enterprises, and evaluated the performance against established benchmark standards, followed by evaluation of commercially available products. An anomaly-based intrusion system was proposed by Kishore, C. R. et al.[6], to detect and prevent attacks in IoT type environments. Using feature engineering approach based on trust factors, they have tried to improve accuracy and FPR. of their proposed model. Many such work have been carried out on anomaly-based IDS[7],[8], which focused on improving accuracy and low false positives.

Recently hybrid approaches[9] using combination of signature-based and anomaly-based IDSs are also explored to improve detection performance. Priya, L. et al.[10] have proposed a hybrid IDS system to detect and prevent vulnerabilities in software-defined-network-based system. However, lack of intelligence required to adopt the evolving nature of emerging threats like zero-day attacks remain as major concerns.

This research work proposes a model to be intelligent enough to detect zero-day attack threats, beyond signature-based and rule-set-based approaches.

1.2 Machine Learning-Based Intrusion Detection

Machine Learning (ML) based intrusion detection systems have been regarded as enhanced versions for static IDS methods. They can learn complex traffic patterns and adopt well to detect threats with model training and tuning. Pujari, M. et al.[11] have studied various classification algorithms on contemporary datasets which included modern day network attack scenarios under adversarial settings. A quantum-inspired least-squared SVM (LS-SVM) classifier-based network intrusion system was proposed with an exclusive feature selection algorithm to improve detection accuracy[12]. Farnaaz, N. et al.[13] have worked

on a Random Forest classifier-based intrusion detection model and have presented results showing low false alarm with high detection accuracy. A K-Nearest Neighbor (KNN) classifier-based intrusion detection model[14] was used to effectively detect anomalies in the system call frequencies that were used to describe behavior of the program. However, traditional ML-based IDSs while useful, still struggle with zero-day attack patterns due to introduction of new and unknown vulnerabilities and network behaviors.

1.3 Neural Networks and RBFNN in Security

Deep Learning (DL) techniques have shown greater promises in building intrusion detection systems, because of their ability to process and handle complex and high volume of data. DL models like Convolutional Neural Networks (CNNs) and Recurrence Neural Networks (RNNs) are very useful for detecting spatial and temporal patterns in network traffic data. However, they are computationally intensive and not suitable for a light-weight system to detect attacks in real-time. RBFNN are seen as alternatives, because of their lightweight, fast converging, and good approximation properties. Many research works using RBFNN have been done[15],[16],[17] to develop IDSs with improved accuracy and low false positive rates. RBFNN-based models usually degrade in performance when trained with imbalanced and incomplete data and fail to detect zero-day attacks.

1.4 Generative Adversarial Networks (GANs) for Data Augmentation

Generative Adversarial Networks (GANs)[18] have revolutionized data augmentation for domains with scarce labelled data. It uses two neural networks to facilitate high quality data generation. The generator module helps in generating realistic synthetic data to improve the representation of data, while the discriminator distinguishes between real and fake data samples. Conditional GAN (cGAN)[19] are developed by introducing additional conditional layers to control the generation of data to improve the data quality. Al-Ajlan M et al.[20] have reviewed the application of GAN for various signature-based, anomaly-based and hybrid IDSs for their robustness, and found significant improvement in addressing class imbalance issues. The framework proposed in this research work uses GAN based data augmentation to address data imbalance in training data, by generating synthetic but realistic unseen attack vector samples.

1.5 Ensemble Learning for Intrusion Detection

Ensemble learning[21],[22],[23] technique combines multiple models, in order to improve the prediction accuracy and robustness. Techniques such as bagging, boosting, and stacking have been widely adopted in IDS research. Random Forests are a classic example of ensemble bagging, while AdaBoost represents boosting strategies. These methods reduce model variance and enhance generalization.

In the context of deep learning, ensembles of neural networks have also been explored. Thockchom, N. et al.[24] have introduced an ensemble learning-based IDS model that blends lightweight classifiers with a stochastic gradient descent meta-classifier, enhancing detection accuracy across both binary and multiclass scenarios. Evaluated on multiple benchmark datasets, their method incorporates Chi-square-based feature selection and demonstrates strong resilience to imbalanced data - a key step towards more reliable threat mitigation.

Ensemble learning with RBFNN is less explored, particularly in cyber security. Some researchers have proposed modular neural network ensembles to detect distributed denial-of-service (DDoS) attacks[25], where different RBFNNs specialize in specific traffic patterns. The combination improves detection accuracy and fault tolerance.

Our proposed framework builds upon this idea by training an ensemble of RBFNNs on different random subspaces of the augmented dataset. This design enhances model diversity and reduces overfitting, enabling more accurate zero-day attack detection.

1.6 Summary and Research Gap

Existing IDS solutions based on traditional rule-based or statistical methods are insufficient for detecting zero-day attacks, due to lack of real-world zero-day data to train the models. While ML and DL models provide improved detection capabilities, they require rich and balanced datasets to be effective. RBFNNs, despite their advantages, have not been extensively studied in ensemble settings or combined with generative data augmentation.

Prior works often relied on static attack filters and missed contextual security insights related to governance in cloud networks. Also, anomaly-based IDSs experience comparatively higher false positives. Moreover, while GANs have shown promise in synthetic data generation for cybersecurity, their application is often limited to improving minority class detection

without integration into a complete detection framework. There remains a gap in leveraging GAN-augmented datasets to train robust ensemble models like RBFNNs specifically for the zero-day detection problem in cloud networks.

Our research addressed the above-mentioned gap by proposing a hybrid framework that integrates GAN-based augmentation with ensemble RBFNNs, offering a scalable, real-time, and highly accurate solution for zero-day attack detection.

2 Methodology

2.1 Proposed Model

The proposed IDS model was designed to integrate generative adversarial network (GAN) based data augmentation and an ensemble of RBFNNs. Figure 1, shows the architecture diagram of the proposed IDS model.

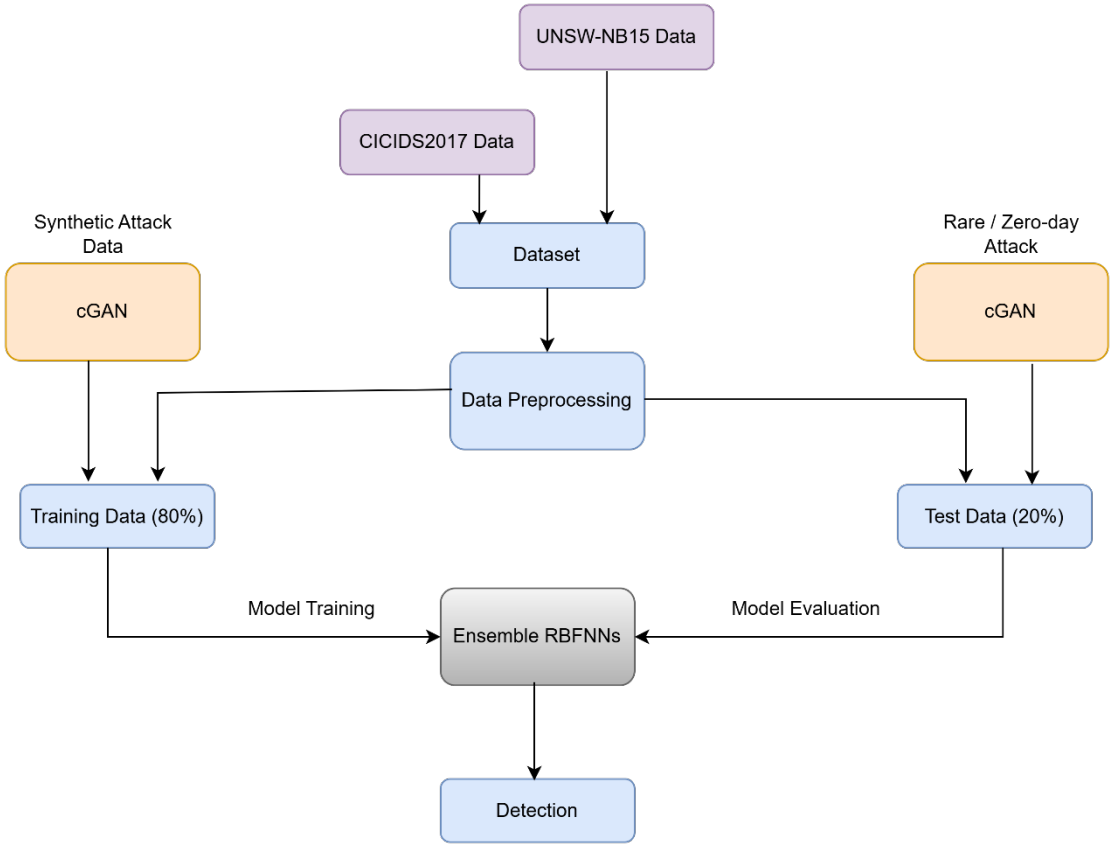

Fig 1. Proposed IDS Model for Zero-Day Attack

The overall pipeline is composed of six key stages: data preprocessing, feature selection, synthetic data generation, ensemble model construction, training and testing, and performance evaluation.

2.1.1. Data Collection and Preprocessing

To simulate real-world cloud network conditions, we utilized a benchmark dataset such as Canadian Institute for Cyber security data (CICIDS2017), and UNSW-NB15 dataset created in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS) for network intrusion, which included a mix of known and simulated zero-day attack types. Data preprocessing involved:

- ***Cleaning*:** Removing null or duplicate records and fixing malformed entries.
- ***Normalization*:** Applying Z-score normalization to bring numerical features into a common scale.
- ***Encoding*:** Using one-hot encoding for categorical fields such as protocol types, services etc.

This ensured consistent input for both the GAN and RBFNN models and helped mitigate bias due to scale differences.

2.1.2. Feature Selection

We have applied Recursive Feature Elimination (RFE) and Mutual Information Gain to identify the most significant features influencing attack classification. Reducing the dimensionality not only improved model interpretability but also decreased training time and enhanced generalization. The final selected features were those that maximized discriminative power between normal, known attacks, and potential zero-day behaviors.

2.1.3. Generative Adversarial Data Augmentation

To address the class imbalance and scarcity of zero-day attack samples, we introduced a Conditional Generative Adversarial Network (cGAN) trained on minority class samples (i.e., zero-day and rare attacks). The generator created realistic synthetic attack samples conditioned on class labels, while the discriminator ensured authenticity. Figure 2, shows the application of cGAN to generate synthetic data for zero-day-attack data or rare attack data.

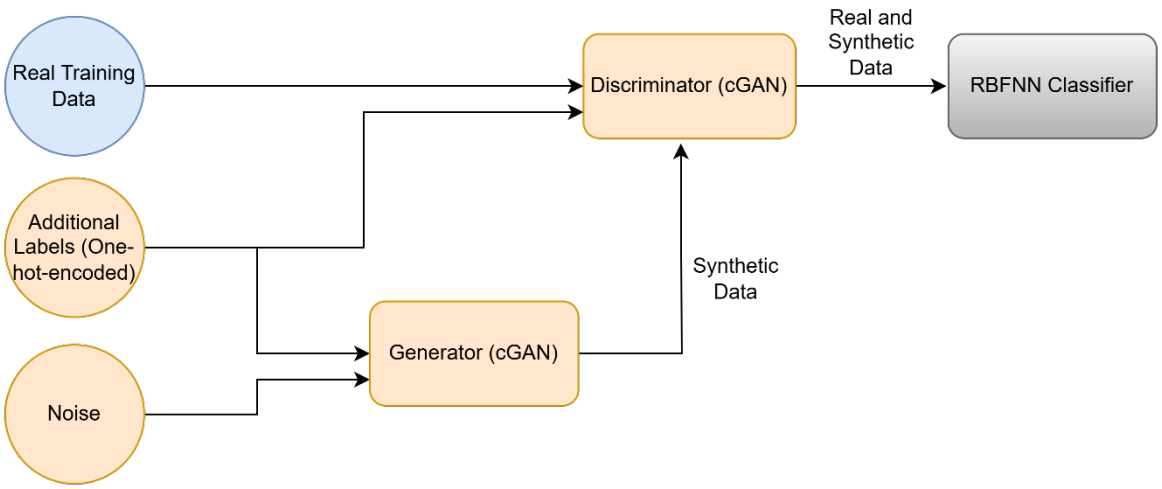

Fig 2. Synthetic Data Augmentation with cGAN

This step effectively augmented the training set with high-quality, diverse attack patterns that may not have appeared during data collection, enabling better generalization for the RBFNN ensemble.

2.1.4. Ensemble RBFNN Construction

The core detection engine is built using an Ensemble of RBFNNs, where each base RBFNN is trained on a bootstrapped subset of the augmented dataset. Key aspects include:

- ***Random Subspace Training*:** Each RBFNN was trained on a unique subset of features to promote model diversity.
- ***Local Gaussian Kernels*:** Hidden layers used radial basis functions on training data clusters, allowing sensitive response to anomalies.
- ***Voting Mechanism*:** The ensemble used a majority-voting scheme based on confidence scores for final predictions.

This ensemble strategy enhanced robustness and reduced overfitting, especially critical for unseen attack detection. Following figure 3, shows the ensemble RBFNN architecture for zero-day attack detection.

2.1.5. Model Training and Testing

During the experiment, we have used 80% of available datasets to train the model. The training dataset were augmented with realistic synthetic data to improve the data representation with unknown and rare samples. Each base RBFNN model was individually trained with a different subset of training data and were integrated into an ensemble. The aggregated output of ensemble was analyzed with remaining 20% of test data to evaluate the trained ensemble RBFNNs model for its detection performance accuracy.

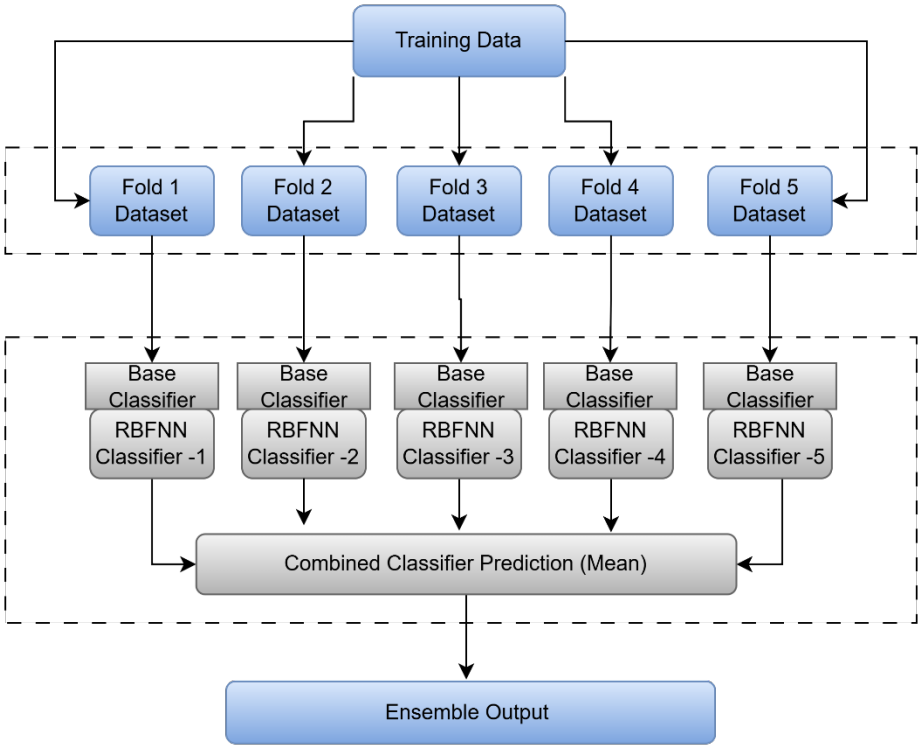

Fig 3. Ensemble RBFNN Architecture for Zero-Day attack detection

2.1.6. Performance Evaluation

Evaluation parameters such as, accuracy, precision, recall, F1-score, and AUC etc. were used to measure the performance of the proposed model. Additionally false positive rate (FPR) and detection rate (DR) were used to understand the zero-day attack detection performance. Comparisons were made between the proposed model and the standard traditional classifier models, such as SVN, Random Forest (RF), CNN, and standalone RBFNN to validate the efficiency in detecting the zero-day attacks.

2.2 Methods

The framework for our proposed model used a conditional GAN (cGAN) to generate realistic synthetic data for advanced and controlled data augmentation, to improve the representation of data with unknown and rare attack samples. RBFNN-based ensemble learning was used to improve model performance with a better aggregated output. Each base RBFNN used Gaussian Kernel in its hidden layer and were independently trained with a subset of training data augmented with realistic synthetic data generated by cGAN module. The output of the ensemble used majority voting method to determine final predictions.

3 Results and Discussion

The environment of experimentation, datasets taken, and findings along with the comparative evaluation with prior state-of-the-art models are discussed as follows.

3.1 Experimental Settings

Our experiments were conducted by leveraging widely used cloud and network intrusion datasets, such as CICIDS2017 dataset, and UNSW-NB15 dataset.

All experiments were conducted on a system with an Intel Core i7 processor, with 32GB RAM, 2 Physical Core, 4 Logical Core, and using Python programming language libraries such as, Tensor Flow, Keras, Scikit-learn etc.

The datasets were divided into 80% training, 20% testing sets. Synthetic attack data were generated using Conditional GANs and included in the training phase to simulate rare and zero-day attack scenarios.

3.2 Dataset Description

- ***CICIDS2017*:** This dataset contained both benign and various attack types such as DDoS, Port Scan, and Web Attacks. For zero-day simulation, certain attack types were withheld during training and introduced only during testing.
- ***UNSW-NB15*:** This included a comprehensive collection of normal and malicious activities. Attack categories like Exploits, Analysis, and Shell code were used to simulate unknown threats during evaluation.

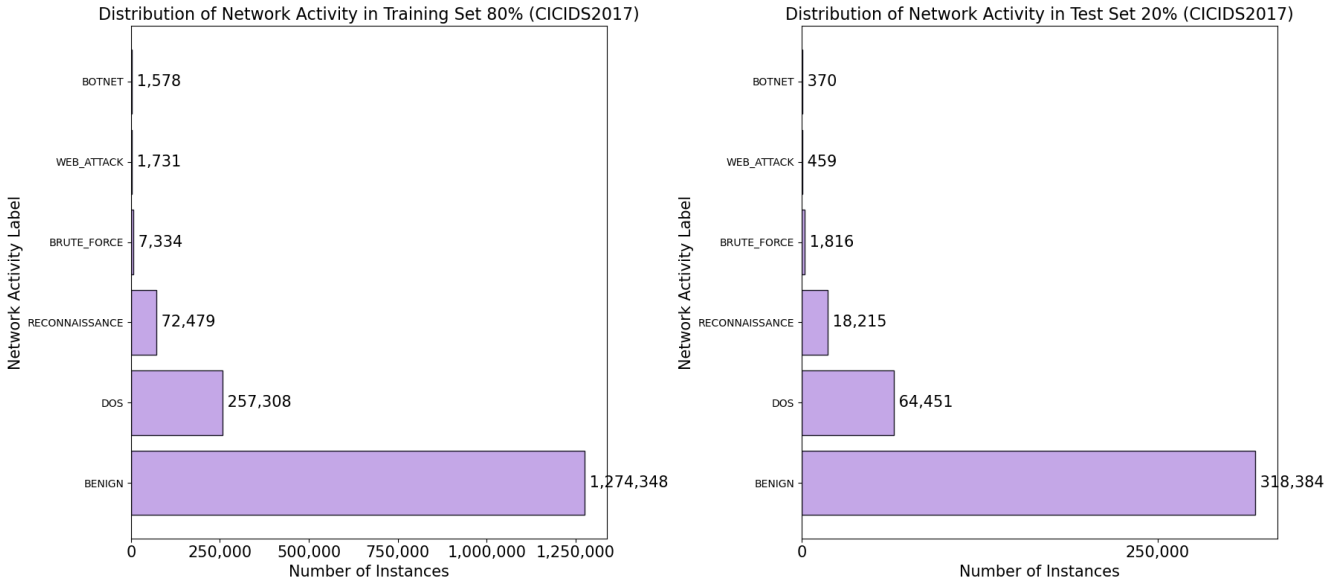

Fig 4. CICIDS2017 Training and Test data distribution

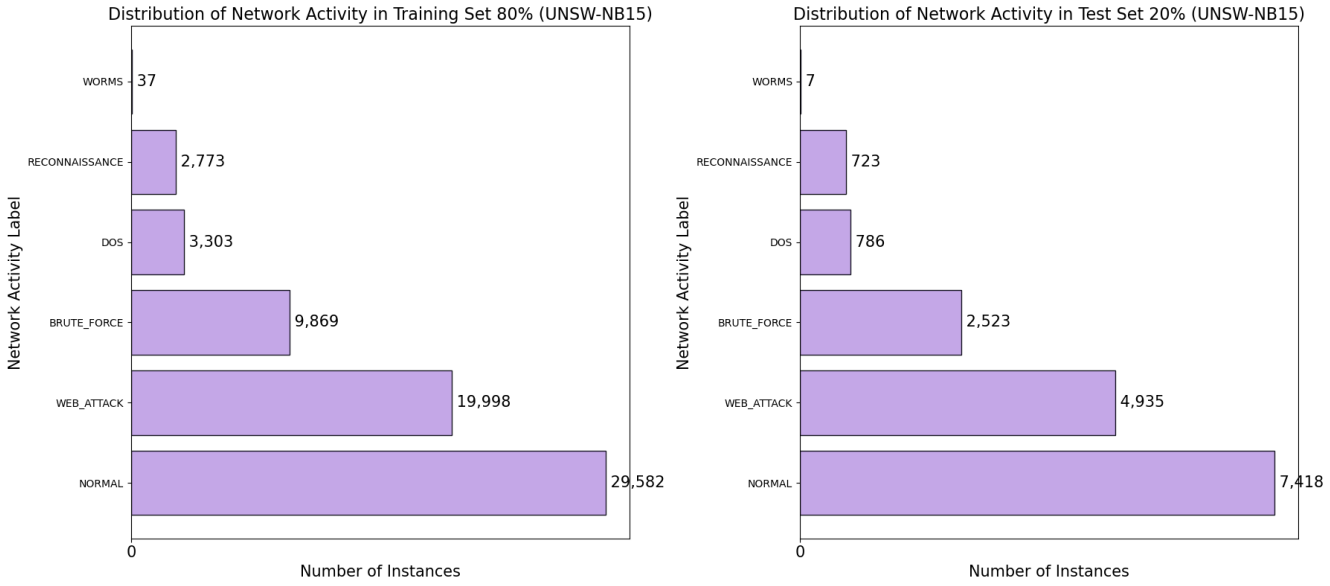

Fig 5. UNSW-NB15 Training and Test data distribution

Standard metrics such as Precision, Accuracy, Recall, Area Under Curve (AUC), F1-Score, and False Positive Rate (FPR) etc. were considered for performance evaluation. These metrics gave a well-rounded view of classification performance, especially

in imbalanced data scenarios common to intrusion detection. Table 1 below depicts the Performance Metrics on CICIDS2017 and UNSW-NB15 datasets including confidence intervals (CI) to convey statistical reliability of the results.

Table 1. Performance Metrics on CICIDS2017 and UNSW-NB15

Dataset	Accuracy%	Precision%	Recall%	F1-Score%	Area Under Curve (AUC)%	False Positive Rate (FPR)%
CICIDS2017	97.8 +/- 0.3	96.5 +/- 0.4	98.2 +/- 0.2	97.3 +/- 0.3	98.7 +/- 0.2	1.8 +/- 0.2
UNSW-NB14	96.3 +/- 0.5	94.8 +/- 0.6	95.8 +/- 0.3	95.3 +/- 0.4	97.2 +/- 0.5	2.3 +/- 0.3

3.3 Comparative Baseline Evaluation

Below Table 2, show the details that compares performance metrics including confidence intervals across the two datasets, CICIDS2017 and UNSW-NB15. CICIDS2017 slightly outperforms UNSW-NB15 across all metrics, which can be attributed to its better-defined attack behaviors and less noise. The ensemble RBFNN model was benchmarked against standard machine learning classifiers. The proposed model demonstrated superior generalization and robustness compared to traditional classifiers.

Table 2. Comparative Baseline Evaluation Result

Dataset	Model	Accuracy%	Precision%	Recall%	F1-Score%	Area Under Curve (AUC)%
CICIDS2017	Support Vector Machine (SVM)	89.4 +/- 0.3	96.5 +/- 0.4	98.2 +/- 0.2	97.3 +/- 0.3	98.7 +/- 0.2
	Random Forest (RF)	91.6 +/- 0.3	95.6 +/- 0.4	97.3 +/- 0.2	96.4 +/- 0.3	97.5 +/- 0.2
	Convolutional Neural Network (CNN)	94.8 +/- 0.3	95.8 +/- 0.4	96.8 +/- 0.2	95.3 +/- 0.3	96.2 +/- 0.2
	Standalone RBFFN	95.7 +/- 0.3	96.6 +/- 0.4	97.2 +/- 0.2	95.4 +/- 0.3	96.3 +/- 0.2
	Proposed RBFNN Ensemble	97.8 +/- 0.3	98.7 +/- 0.4	95.1 +/- 0.2	97.7 +/- 0.3	97.7 +/- 0.2
UNSW-NB14	Support Vector Machine (SVM)	85.1 +/- 0.5	94.8 +/- 0.6	95.8 +/- 0.3	95.3 +/- 0.4	97.2 +/- 0.5
	Random Forest (RF)	88.3 +/- 0.5	90.3 +/- 0.6	90.8 +/- 0.3	91.5 +/- 0.4	93.8 +/- 0.5
	Convolutional Neural Network (CNN)	92.4 +/- 0.5	95.4 +/- 0.6	96.3 +/- 0.3	96.8 +/- 0.4	97.2 +/- 0.5
	Standalone RBFFN	94.4 +/- 0.5	94.7 +/- 0.6	95.6 +/- 0.3	95.8 +/- 0.4	96.2 +/- 0.5
	Proposed RBFNN Ensemble	96.3 +/- 0.5	96.1 +/- 0.6	95.8 +/- 0.3	96.6 +/- 0.4	97.1 +/- 0.5

3.4 Ablation Study

Table 3 below, shows the details ablation study using the CICIDS2017 dataset, to access the contribution of each component in the pipeline of the proposed framework.

The results clearly show that cGAN augmentation improves the accuracy, while ensemble increases generalization and improves F1-score as compared to single classifiers.

Table 3. Performance Comparison

Model	Precision	Recall	F1-Score	Observations
Standalone baseline RBFFN (Single Classifier, No Augmentation)	94.22%	95.24%	95.16%	Suffers from minority class under representation, and lower detection of new or rare attack types
Baseline + Ensemble Learning (No Augmentation)	94.86%	95.30%	95.21%	Improves accuracy, but still limited by data imbalance
Baseline + cGAN Augmentation (Single RBFNN Classifier)	94.88%	96.43%	95.27%	Boosts rare-class recall, but some overfitting to synthetic samples
Proposed RBFNN Ensemble + cGAN (Full model)	**95.14%**	**97.71%**	**97.72%**	**Achieves overall better performance by combining diversity in data**

3.5 Zero-Day Attack Detection

When evaluated specifically on zero-day attacks (unseen during training) following were the results observed on both the datasets.

- ***CICIDS2017*:** Detection rate of 95.1%.
- ***UNSW-NB15*:** Detection rate of 93.4%.

This showcased the effectiveness of using GANs for synthetic attack generation, allowing the model to learn diverse threat behaviours and generalize well.

The novelty of the proposed model is a hybrid of GAN and ensemble RBFNN architecture, that incorporates the feature of synthetic but realistic attack sample generation to train the model. This model outperformed traditional ML classifiers in terms of precision, recall, accuracy, F1-score etc., in detecting previously unknow attack types in real-time.

3.6 Computational Cost

While the cGAN with ensembled RBFNNs approach provides significant improvement in detecting zero-day-attacks, at the same time the computation overhead needs to be carefully considered. The iterative adversarial optimization between the generator and the discriminator of the cGAN component incurs significant training cost. Trade-off needs to be made for real-time and resource constrained deployments. Lighter versions of GAN with reduced parameters and complexity without significantly sacrificing generation quality need to be explored. Transfer learning approach for models to adapt to new attack types may be considered to reduce cost. Combining cGAN with computationally cheaper augmentation methods and separating data generation from ensembled pipeline and running it on a distributed system could optimize cost.

3.7 Data Generation Quality Metrics

To ensure the quality of synthetic data generated by cGAN, data quality metrics such as distribution overlap, gain in precision, and gain in F1-score were used to establish the robustness of augmented dataset. Table 4 below outlines the objective metrics and their interpretations.

Table 4. Data Quality Metrics

Metric	Observed Value	Benchmark/ Baseline	Interpretation
Distribution Overlap	0.12	< 0.15	High distribution overlap between synthetic and real data.
Precision Gain (with cGAN augmentation)	+0.7%	Baseline model without cGAN	Synthetic data provides measurable improvement in classification accuracy.
F1-Score Gain (with cGAN augmentation)	+0.2%	Baseline model without cGAN	Enhanced discriminative ability in distinguishing attacks and normal traffic.

3.8 Security Considerations

It is important to note that GANs and deep learning models in general are not immune to adversarial threats. Malicious attacks could manipulate and influence training and inference data that can lead to misclassification and can compromise dataset. Preprocessing of datasets to detect and filter suspicious inputs before they reach the model, and applying privacy-preserving noise to limit data leakage would ensure conceptual robustness. Incorporating adversarial techniques during training would help in improving resiliency and reliability.

3.9 Scalability and Inference Latency

The training phase of cGAN augmented ensembled model is computationally intensive. Inference-time performance is critical for real-time monitoring. The integrated ensembled classifier was observed to process approximately 350 samples per second on a CPU only configuration, and average per sample classification latency was around 10.32 milliseconds. With additional processing units (CPUs), the model can scale linearly. Despite high training cost, the current implementation can be deployed as a viable, high-throughput, and real-time detection system in large-scale cloud environment.

4 Limitations of Proposed Solution

While the proposed ensemble RBFNN model with GAN-based data augmentation achieved high accuracy and generalization in detecting zero-day attacks, it presented certain limitations. First, the computational cost of GAN training, even when pre-processed offline, remained relatively high, especially in CPU-only environments. This can impact scalability for real-time applications in large-scale cloud deployments. Second, the quality of synthetic data generated by GANs may vary, potentially introducing noise or artifacts that affect model stability. Third, feature engineering was primarily manual, which may miss deeper temporal, or contextual patterns present in network traffic.

5 Conclusion and Future works

This research focused and contributed towards a resilient approach to design a zero-day-aware anomaly-based intrusion detection system. The model demonstrated the benefit of integrating an advanced data augmentation technique, cGAN with an ensemble of RBFNNs for a more intelligent, adoptive, and efficient IDS to detect zero-day attacks, beyond signature-based, and static rule-sets-based approaches. The proposed method achieved 97.8% accuracy and 2.30% FPR with CICIDS2017 dataset. One of the unique contributions of this study was conditional GAN-based threat synthesis for zero-day attack coverage. The model performance showed the results with significantly low FPR and high detection rate. While the training time of GANs remain computationally intensive, performance may be degraded, if the synthetic data is not close enough to real-world attack patterns. One of the open questions in this study is, how the model would respond when the GAN itself is under attack. The future work will focus on a lightweight, transformer-based architecture. Additionally federated learning will enable decentralized processing across multiple cloud nodes to improve the scalability. Adoptive loss functions will be explored to improve stability of GAN module.

References

1) Asad H, Adhikari S, Gashi I. A perspective–retrospective analysis of diversity in signature-based open-source network intrusion detection systems. *International Journal of Information Security*. 2024;23:1331–1346. https://doi.org/10.1007/s10207-023-00794-9.
2) Pelekis S, Koutroubas T, Blika A. Adversarial machine learning: a review of methods, tools, and critical industry sectors. *Artificial Intelligence Review*. 2025;58:226. https://doi.org/10.1007/s10462-025-11147-4.
3) Sharma P, Kumar M, Sharma HK. Generative adversarial networks (GANs): Introduction, Taxonomy, Variants, Limitations, and Applications. *Multimedia Tools and Applications*. 2024;83:88811–88858. https://doi.org/10.1007/s11042-024-18767-y.
4) Waleed A, Jamali AF, Masood A. Which open-source IDS? Snort, Suricata or Zeek. *Computer Networks*. 2022;213. https://doi.org/10.1016/j.comnet.2022.109116.
5) Singh KP, Kesswani N. An anomaly-based intrusion detection system for IoT networks using trust factor. *SN Computer Science*. 2022;3:168. https://doi.org/10.1007/s42979-022-01053-9.
6) Kishore CR, Rao DC, Behera HS. Deep learning approach for anomaly detection in CAN bus network: An intelligent LSTM-based intrusion detection system;vol. 480. 2022. https://doi.org/10.1007/978-981-19-3089-8_51.
7) Veeramreddy J, Prasad K. Anomaly-based intrusion detection system. 2019. https://doi.org/10.5772/intechopen.82287.
8) Khaleel Y, Habeeb M, Albahri A, Al-Quraishi T, Albahri O, Alamoodi A. Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods. *Journal of Intelligent Systems*. 2024;33(1):20240153.
9) Shaikh A, Gupta P. Intelligent Communication Technologies and Virtual Mobile Networks: Advanced Signature-Based Intrusion Detection System. 2023. https://doi.org/10.1007/978-981-19-1844-5_24.

10) Priya L, Rajagopalan N. A Hybrid Intrusion Detection System for Mitigating Flow Table Buffer Saturation Attacks in Software-Defined Networking. *SN Computer Science*. 2025. https://doi.org/10.1007/s42979-025-04079-x.
11) Pujari M, Pacheco Y, Cherukuri B. A Comparative Study on the Impact of Adversarial Machine Learning Attacks on Contemporary Intrusion Detection Datasets. *SN Computer Science*. 2022. https://doi.org/10.1007/s42979-022-01321-8.
12) Waghmode P, Kanumuri M, El-Ocla H. Intrusion detection system based on machine learning using least square support vector machine. *Scientific Reports*. 2025. https://doi.org/10.1038/s41598-025-95621-7.
13) Farnaaz N, Jabbar MA. Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science*. 2016;89. https://doi.org/10.1016/j.procs.2016.06.047.
14) Yihua L, Rao V. Use of K-Nearest Neighbor classifier for intrusion detection. *Computers & Security*. 2002;21. https://doi.org/10.1016/S0167-4048(02)00514-X.
15) Attou H, Guezzaz A, Benkirane S. A New Secure Model for Cloud Environments Using RBFNN and AdaBoost. *SN Computer Science*. 2025. https://doi.org/10.1007/s42979-025-03691-1.
16) Wang Y. Deep Learning-Based Network Intrusion Detection Systems. *Applied and Computational Engineering*. 2024;109:179–188.
17) Muhammad N, Phulpoto A, Ahmed I, Abbass G. Radial Basis Function Neural Networks (RBFNN) for Secure Intrusion Detection in the Internet of Drones (IoD). *Proceedings of the Bulgarian Academy of Sciences*. 2024. https://doi.org/10.7546/CRABS.2024.08.09.
18) Dunmore A, Jang-Jaccard J, Sabrina F, Kwak J. A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection. *IEEE Access*. 2023. https://doi.org/10.1109/ACCESS.2023.3296707.
19) Yu F, Wang L, Fang X, Zhang Y. The Defense of Adversarial Example with Conditional Generative Adversarial Networks. *Security and Communication Networks*. 2020;p. 1–12. https://doi.org/10.1155/2020/3932584.
20) Al-Ajlan M, Ykhlef M. A Review of Generative Adversarial Networks for Intrusion Detection Systems: Advances, Challenges, and Future Directions. *Computers, Materials & Continua*. 2024;81(2):2053–2076.
21) Lucas T, Figueiredo I, Tojeiro C, Almeida A, Scherer R, Brega JR, et al. A Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks. *IEEE Access*. 2023. https://doi.org/10.1109/ACCESS.2023.3328535.
22) Babaey V, Faragardi HR. Detecting Zero-Day Web Attacks with an Ensemble of LSTM, GRU, and Stacked Autoencoders. *Computers*. 2025;14(6):205. https://doi.org/10.3390/computers14060205.
23) Harahsheh K. Enhancing IoT Security Using Lightweight Machine Learning Algorithms: A Comprehensive Approach Using Ensemble Learning, Feature Selection, and Federated Transfer Learning. *Doctor of Philosophy (PhD), Dissertation, Electrical & Computer Engineering, Old Dominion University*. 2025. Available from: https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1606&context=ece_etds.
24) Thockchom N, Singh MM, Nandi U. A novel ensemble learning-based model for network intrusion detection. *Complex & Intelligent Systems*. 2023;9:5693–5714. https://doi.org/10.1007/s40747-023-01013-7.
25) Gavrilis D, Dermatas E. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. *Computer Networks*. 2005;48(2):235–245. https://doi.org/10.1016/j.comnet.2004.08.014.