IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

A Novel Generative AI-Based Approach for Robust Anomaly Identification in High-Dimensional Dataset

Siddhesh Amrale
Independent Researcher
amralesiddhesh@gmail.com

Abstract: *The number of security measures put in place is wide and is in response to the rising security threats. The growing complexity of cyberattacks and the complexity of network data analysis make the conventional intrusion detection systems insufficient to locate APTs and zero-day vulnerabilities. Anomaly detection in cybersecurity has obstacles such as class imbalance, high-dimensional data, and the inability to extrapolate to shifting attack patterns. This paper showcases an AI-based approach to accurately detecting anomalies using the UNSW-NB15 benchmark dataset, which contains both typical and unusual traffic. To guarantee stable feature contribution, the suggested solution employs a thorough preprocessing pipeline, which includes data cleaning, one-hot encoding, and feature scaling. The dimensionality reduction, feature extraction for discrimination, and redundancy reduction goals are achieved through the application of PCA. In order to reduce the class imbalance, the SMOTE manifests artificial samples of minority types of attack, making model training balanced. The Generative Adversarial Network (GAN) classifier is then trained so as to differentiate the malicious and benign traffic successfully. Experimental performance is better with high precision (PRE), accuracy (ACC), recall (REC) and F1-score (F1) of 99.82, 99.75, 99.89, and 99.88, respectively compared to baseline models, which included ANN (77.51%), Decision Tree (80.5%), and KNN (97.29%). The results justify the scalability, flexibility and robustness of the proposed GAN-based framework to identify anomalies in the contemporary cybersecurity environment on time.*

Keywords*:* Cybersecurity, Anomaly detection, UNSW-NB15 dataset, Generative Artificial Intelligence, Machine learning, GAN, SMOTE.

I. INTRODUCTION

Cybersecurity is an issue of high priority in the digital infrastructures and interconnected systems that are rapidly emerging globally [1]. The nature of cyber threats is getting advanced and they are targeting sensitive information and disabling key operations [2][3][4]. Intelligent and adaptable systems that can identify new threats in real-time are necessary since traditional security methods that rely on signatures or rules to detect attacks are not always successful [5]. Here, the data produced by network traffic, system logs, and IoT devices on a high-dimensional level are both opportunities and challenges to security analytics.

Data analysis, in particular anomaly detection is concerned with detecting unusual or uncommon events that are very different in comparison to the patterns previously determined. These anomalies may be a security violation, a fraud, equipment malfunctions, or any other vital occurrences, based on the area of application [6][7]. One technique that has become central to the issue of cybersecurity problems has been anomaly detection [8][9]. Using anomaly detection, new attacks and unusual behaviour can be found in data that conventional methods often fail to notice. This includes things like network traffic logs, sensor readings, and system telemetry. However, these methods often fail due to issues like feature redundancy, feature sparseness, and the curse of dimensionality [10][11][12]. Anomalies in high-dimensional data could be hard to detect if there are a lot of associated and duplicated features, which could damage the needs of traditional models. People call this "the curse of dimensionality." [13][14]. In addition, real-world data tends to be

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 4, Issue 2, October 2024 Impact Factor: 7.53

noisy, missing, and non-linear, and this makes detection of anomalies even more difficult. These difficulties highlight the need to create strong methods that have the potential to work in high-dimensional spaces and still be of high detection ACC.

Generative artificial intelligence (AI) is a promising concept to use in high-dimensional anomaly detection [15]. VAEs and GANs are generative models that can be trained to mimic the distribution of typical data patterns. In practice, they can accurately reconstruct these patterns and spot abnormalities when they deviate from the norm [16][17]. By utilizing deep learning architectures, generative AI-based models have become a go-to for cybersecurity jobs that need the detection of abnormalities that would otherwise be difficult to spot. This is because these models are trained to learn and capture complicated, non-linear interactions in high-dimensional space [18][19]. Large-scale experiments prove that the suggested framework is superior to traditional approaches in ACC, stability, and scalability and can be used as a valid solution to proactive detection of cybersecurity threats.

A. Motivation with Contribution

The fast development of interconnected systems and IoT networks has broadened the cyber threat landscape, revealing the weaknesses of conventional tests to detect anomalies in identifying the development of attacks and zero-day attacks. The traditional machine-learning models cannot deal with high-dimensional data, redundancy of features, and extreme imbalance of classes that result in biased and unreliable detection. To overcome these issues, this study suggests an AI-driven solution to strong anomaly detection where generative learning, feature reduction, and synthetic data generation are used to improve the adaptation, scalability, and resilience to the emergent cyber threats. This discovery has significant implications for cybersecurity and anomaly detection:

- Comprehensive preprocessing pipeline integrating data cleaning, one-hot encoding, and feature scaling tailored for the UNSW-NB15 dataset, ensuring reproducibility and consistency in network traffic analysis.
- Dimensionality reduction Intelligent dimensionality reduction based on the PCA summary of the most informative features, improved computation efficiency, and classification ACC.
- Successful control of class imbalance by the use of SMOTE, which generate artificial minority attacks samples to enhance detection of minor and unobtrusive anomalies.
- New GAN based classification architecture that simultaneously learns generative and discriminative paradigms to find intrusion patterns that are complex in nature.
- Strong performance testing based on multi-metric evaluation (ACC, PRE, REC, and F1) to test the model holistically.
- A scalable and adaptable generative AI framework that shows how it may be used in real life for next-generation intrusion detection systems in businesses and critical infrastructure.

B. Justification and Novelty

This research is essentially a response to the declining effectiveness of the traditional intrusion detection methods in handling high-dimensional, dynamic, and imbalanced cybersecurity data of a nature that has been increasing. The creation of authentic synthetic samples for minority attack classes is difficult because current algorithms often fail to generalize over changing attack patterns. The uniqueness of this paper lies in the combination of GANs with a full preprocessing pipeline, which comprises feature scaling, PCA-based dimensionality reduction, and SMOTE-based data balancing while utilizing the UNSW-NB15 dataset. Such a single AI-powered framework allows for the dynamic understanding of intricate attack behaviors, the detection ACC getting better, and the provision of a scalable, adaptable, real-time anomaly detection solution for contemporary network environments.

C. Structure of Paper

This is the general structure of the paper: This section II provides a survey of the research on anomaly identification using ML methods. Descriptions in depth of the method that has been suggested are offered in Section III which explains the design of the framework each feature. Section IV: Evaluate the results of the proposed models, draw

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

comparisons, have a discussion, and finally Section V summarizes this paper and enumerates the possible research fields for the coming time.

II. LITERATURE REVIEW

This section presents a literature review of generative AI and machine learning algorithms aimed at achieving efficient and accurate anomaly detection in cybersecurity settings. Subsequent literature reviews are summarized in Table I:

A et al. (2023) Generative AI anomaly detection systems were the main target of adversarial manipulations and adversarial attacks. Generative AI systems are clearly better at fending off quantum-based adversarial attacks than their more traditional counterparts, which rely on static models that lack the flexibility to swiftly adjust their defensive strategies to new threats. The findings of the experiments back up this claim. Finally, the challenge of safeguarding generative AI anomaly detection systems from quantum adversarial threats has arisen, which is both novel and exciting [20].

Raturi et al. (2023) Anomaly detection is a technique that is utilized to locate data anomalies. It is through generative adversarial networks (GANs) that complicated patterns can be learned and synthetic data can be created. A single outlier in timeseries data might be the reason for the training of a GAN. Using synthetic data improves the model's performance. High dimensionality, difficulties in capturing temporal correlations, and difficulties in discovering uncommon occurrences with skewed class distributions make it difficult for traditional ML models to handle the complexity of time-series anomaly identification. tried out a number of ML techniques for detecting outliers in time series data using the Yahoo! Webscope S5 dataset. With REC at 0.925, F1 at 0.912, ACC at 0.999, and a 0.976 area under the curve [21].

Esmaeili et al. (2023) The autoencoder-based prediction models were trained to automatically detect anomalous data using the three electrochemical aptasensors. Different concentrations, analytes, and bioreceptors cause the signal duration of each sensor to vary. To estimate the criteria for anomaly detection, forecasting models were employed that made use of autoencoder networks and the KDE technique. Additionally, the prediction models' training autoencoders, ULSTM autoencoders, and BLSTM autoencoders. Anomaly prediction models' ACC as a performance indicator revealed that vanilla and integrated models performed similarly, LSTM-based autoencoder models performed poorly, and the dataset with longer signals achieved an ACC of about 80% [22].

Hooshmand and Hosahalli (2022) One step in cyber-security's network anomaly detection process is sorting data from network traffic into three groups: TCP, UDP, and whatever else. After that, we'll take a look at each grouping independently. The model is built around a convolutional neural network (CNN) with one dimension. Using the Chi-square technique for feature selection and the synthetic minority over-sampling strategy to fix a class imbalance problem, the weighted average f-score for the TCP, UDP, OTHER, and ALL categories are 0.85, 0.97, and 0.86, respectively. One must run this before training the model. To evaluate the model, the UNSW-NB15 dataset is employed [23].

Abdelkhalek, Ravikumar and Govindarasu (2022) An ADS that use ML may detect various covert IT and OT threats based on physics- and pattern-based DER communication traffic thresholds. Using a model-based technique, the five DER-specific anomaly detection ML-algorithms were trained on the proposed ADS system's HIL testbed. The system measured 98.4% ACC, had a detection delay of 5 µs, and had a false-positive rate of 0.28% and a false-negative rate of 1.32% in consideration of accuracy [24].

Oprea et al. (2021) Research large datasets that include smart meter readings from an Irish trial study. Apply a hybrid approach and an unsupervised ML technique to detect potentially suspicious time series with out-of-the-ordinary values. The next step is to set a limit on the proportion of readings that are significantly out of the ordinary compared to the total readings. Finally, mark each time series as potentially problematic. Get a Spectral Residual-Convolutional Neural Network (SR-CNN) ready to sift through unlabeled data for outliers and a time-series anomaly training model based on martingales. The dataset is then processed using Fisher Linear Discriminant Analysis and Two-Class Boosted DT. The necessary capabilities for recognizing questionable consumers were obtained during model training: 0.894 F1, 90% ACC, and 0.875 PRE [25].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

Recent studies have widely expanded the scope of AI (artificial intelligence) applications to include AI-driven methods for achieving robust anomaly detection. As a result, they demonstrate significant progress in the ACC and automation of security and reliability mechanisms across various domains. LR, KNN, SVM, NB, DT, and RF are still widely used, but ensemble-based frameworks have made these systems more resilient to high-dimensional and noisy data. To successfully capture complex spatial and temporal dependencies within data streams, advanced DL techniques have been developed, such as autoencoders, CNNs, GANs, and hybrid architectures combining CNN-LSTM or Transformer models. Recent studies have used data augmentation techniques like SMOTE, feature selection, and dimensionality reduction (PCA) to enhance model generalization and solve problems with class imbalance. There are still obstacles to overcome in terms of real-time adaptation, computational efficiency, and resilience against adversarial and quantum-based attack vectors, even with current developments. The next step in research is to create lightweight, adaptive, and explainable AI systems that enhance the transparency, interpretability, and robustness of anomaly detection systems that need to operate in changing and dynamic threat environments

Table 1: Comparative Analysis of Recent Studies on Generative Artificial Intelligence-Based Anomaly Detection.

Author(s) & Year	Anomaly Type	Methodology / Approach	Key Findings	Challenges	Limitations / Future Work
A et al. (2023)	Adversarial & Quantum-based attacks on AI anomaly detection systems	Advanced Generative AI techniques for dynamic adaptation against evolving quantum adversarial strategies	Enhanced resistance to adversarial attacks based on quantum mechanics; enhanced variability	Static models aren't flexible enough to fend off sophisticated attacks.	Extend protection strategies for quantum-era AI systems; improve real-time adaptability
Raturi et al. (2023)	Time-series anomalies	Anomaly detection model based on GAN; assessed using ML metrics (F1, REC, PRE, AUC-ROC)	F1=0.912, PRE=0.899, REC=0.925, and AUC-ROC=0.976 indicate high performance.	Handling high-dimensionality, temporal dependencies, and skewed class distributions	Explore real-time adaptation and cross-domain generalization for time-series anomaly detection
Esmaeili et al. (2023)	Sensor data anomalies	Autoencoder, ULSTM, and BLSTM models, with KDE thresholding for anomaly detection	ACC ≈ 80%; LSTM-based autoencoders showed the least ACC	Varying signal lengths, bioreceptor variability	Improve signal normalization, integrate hybrid feature selection and ensemble architectures
Hooshmand & Hosahalli (2022)	Network traffic anomalies	1D CNN with Chi-square feature selection and SMOTE oversampling to handle imbalance; evaluated by protocol type	Weighted F-scores: TCP (0.85), UDP (0.97), OTHER (0.86), ALL (0.78)	Class imbalance and feature redundancy in network data	Extend to real-time intrusion systems; evaluate on cross-dataset generalization
Abdelkhalek, Ravikumar & Govindara	IT & OT anomalies in DER communications	Model-based ML approach using five DER-specific algorithms with physics and pattern-	Detection ACC 98.4%, Latency 5 µs, FP 0.28%, FN 1.32%	High complexity of mixed IT/OT environments	Optimize for scalability; integrate AI explainability in DER anomaly detection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

su (2022)		based thresholds			
Oprea et al. (2021)	Power consumption anomalies	Hybrid unsupervised ML: SR-CNN, martingale-based models + Two-Class Boosted Decision Tree & Fisher LDA	ACC 90%, PRE 0.875, F1 0.894	Lack of labeled data and noisy readings	Extend to larger smart grid datasets; improve interpretability of hybrid models

III. METHODOLOGY

The suggested machine learning tool that would use GANs to protect networks and identify intrusions is depicted in Figure 1. The UNSW-NB15 dataset served as the basis for the investigation. The methodology is founded on a multi-stage pipeline that starts with data pretreatment. Data cleaning, one-hot encoding of categorical variables, and feature scaling to ensure homogenous feature contributions are all part of this process. PCA is a tool for improving computational performance by reducing dimensionality, retrieving features, and reducing redundancy. The SMOTE is one approach to the problem of class imbalance. This technique helps learning models to be balanced by providing fictional samples of the underrepresented attack classes. Before being trained in a GAN-based classifier, the clean dataset is split into testing and training subsets. This is where the discriminator and generator acquire the ability to identify patterns that distinguish between benign and malicious traffic. These four metrics—ACC, PRE, REC, and F1—are used to assess the model's proficiency. These metrics demonstrate the framework's soundness and efficiency in anomaly and IDS.

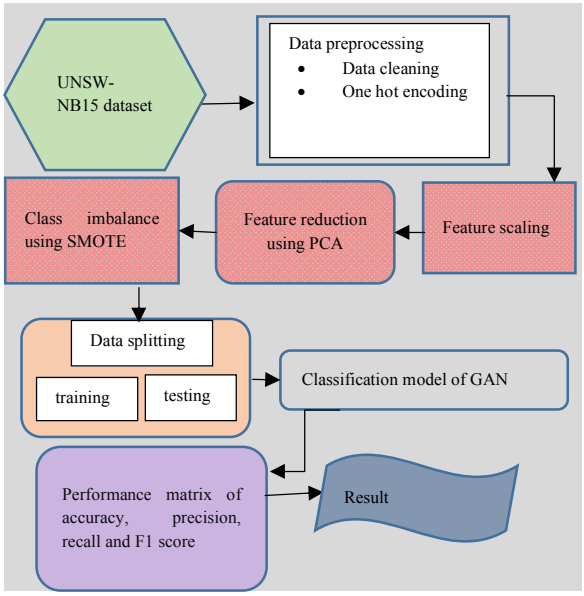

Fig. 1. Flowchart for Anomaly detection using machine learning models

A. Data Collection

The UNSW Cyber Range Lab developed the UNSW-NB15 dataset with the help of the IXIA Perfect Storm tool. This dataset is considered a state-of-the-art benchmark for network IDS. With 49 features spanning flow, content, and time characteristics, it includes both benign and malicious traffic. Anomaly detection and intrusion detection models in high-dimensional networks can be tested on this dataset, which has over 2.5 million records spanning several attack types like DoS, Exploits, and Reconnaissance. some of the visualizations are given below:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

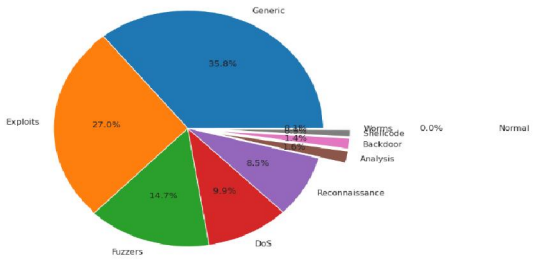

Fig. 2. Attack Type Distribution for Anomaly Detection

Figure 2 shows the distribution of several cybersecurity threat categories in this pie chart. Generic threats dominate at 35.4%, followed by Exploits at 27.0%, Fuzzers at 14.3%, and DoS attacks at 9.4%. Reconnaissance accounts for 8.5%, while smaller segments include Analysis, Backdoor, Shellcode, Worms, and Normal traffic at 0.0%. The visualization effectively categorizes network traffic patterns for anomaly detection systems.

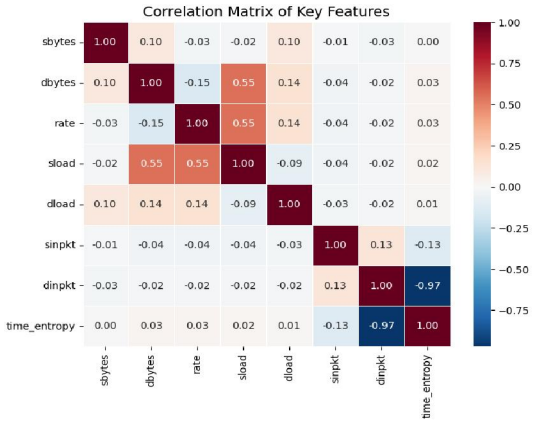

Fig. 3. Correlated heatmap of network traffic feature

This correlation matrix heatmap visualizes the statistical relationships between critical network traffic features in cybersecurity in Figure 3. The color gradient reveals the most significant correlation patterns, for instance, the strong positive correlations between bytes and packets as well as the strong negative correlations between dsinpkt and temporal entropy (-0.97). Dark blue (negative correlation, -1.00) and dark red (positive correlation, +1.00) are the hues that make up the gradient. These correlation patterns signal to us the feature dependencies, multicollinearity problems, and redundant variables. The examination of such data is indispensable when deciding on features, reducing the number of features, and creating stable models of ML that can detect anomalies efficiently.

B. Data Preprocessing

Data pre-processing refers to the operations of making raw data suitable for data mining analytics by changing it to properly structured datasets. Often, raw data is incomplete or has the wrong format. Major steps of data preprocessing are:

- **Data cleaning:** Duplicate record removal, missing value handling, and consistent data type and column name checking are all parts of data cleaning. Besides that, it is also about dropping the irrelevant or constant features to remove the noise and get the dataset ready for model training that can be trusted.
- **One hot encoding:** One-Hot Encoding. The data is a method where the features, which are usually given as categories, are changed into columns that are represented numerically by either 0 or 1. Features like protocol, service, and status are included in this. In the case of categorical data, it signifies that machine learning models do not have to infer a connection between the categories.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

C. Feature Scaling

The learning process of the model is ensured when numerical attributes, such as packet size, duration, and byte count, are normalized. Here, the term "feature scaling" applies. Standard data normalization involves setting each feature to a mean of 0 and a standard deviation of 1 to prevent outlying features from being overshadowed by outlying ones. Various methods, including StandardScaler, are used to achieve this goal.

D. Feature Reduction Using PCA

PCA is a dimensionality reduction technique that simplifies data sets by reducing their interrelated features to a smaller number of independent variables. As a result of this technique, which is used to reduce computing complexity, the maximum variance is captured in fewer dimensions, thus preserving the essential information for the purpose of intrusion detection. Predictive component analysis (PCA) makes a model more efficient and less difficult to understand when it is used to project the data into these main components [26]. This facilitates the visualization of class separation (normal vs. attack) and the reduction of redundant noise.

E. Class Imbalance Using SMOTE

The distribution of classes can be so extremely unequal that the number of attack cases is very much greater than that of normal traffic, which may cause machine learning models to be biased towards the dominant class. The problem with SMOTE, which attempts to build a more balanced dataset by creating synthetic examples for minority classes, is thus fixed. After applying SMOTE, the previously underrepresented attack classes are augmented, resulting in a more uniform class distribution that improves model training and anomaly detection performance.

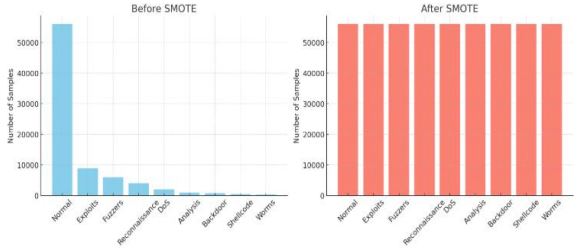

Fig. 4. Applying Before and after SMOTE

Figure 4 is a bar chart or histogram that shows the class frequencies before and after SMOTE. It clearly shows how the normal and attack samples are now more evenly distributed.

F. Data Splitting

A GAN model is trained using complicated network traffic patterns using the 80:20 split of the UNSW-NB15 dataset, and its detection performance is evaluated using a testing set with unknown data.

G. Proposed Models of Generative AI-based GAN model for Anomaly detection

An ML model called a GAN combines two different kinds of ML models: discriminator networks (D) and generator networks (G). Generator G, on the other hand, discovers a method to deceive the discriminator into accepting erroneous input by treating it as a noise signal obtained from a normal distribution $k(z)$ that follows $z \sim \mathcal{X}(0,1)$ [27]. After that, discriminator D works out a way to distinguish between the attacks found in the actual data X and the fraudulent data generated by G. The stability of G and D were also taught via gradient descent. Equation (1) represents the WGAN learning process with the symbols of GP and a min-max game between two entities, G and C.

$$L = E_{\hat{x}\sim p_g}[D(\hat{x})] - E_{\hat{x}\sim p_r}[D(\hat{x})] + E_{\hat{x}\sim p_g}[\lambda(\|\nabla_{\hat{x}} D(\hat{x})\|_2 - 1)^2] \quad (1)$$

The equation $p(\lambda) = [\lambda(\|\nabla_{\hat{x}} D(\hat{x})\|_2 - 1)^2]$ can be written differently. in the form of the gradient penalty and $\hat{x} = qx + (1-q)\,\hat{x}$, $q \sim U(0,1)$. This method replaces the state-action value $Q(s, a)$ with the distribution of the target traffic data X learned via WGAN-GP across all returns. The current sensed data states is given into the generator G, and, for each updated round, the networks are updated using a minibatch (s, a, r, s') mi=1 from X. The IDS uses the Bellman

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 4, Issue 2, October 2024 Impact Factor: 7.53

optimality operator T, as seen in Equation (2), to obtain distribution samples that are true to form.

$$x(t) = r(t) + \gamma^{b} minG\big(z(t), s(t+1)\big) \quad (2)$$

where the target generator network is *G*.

The loss functions of the critic *G* network and the generator C network are given by Equations (3) and (4), respectively:

$$L_c = E_{\hat{x}\sim p_g}[f\big(G^{g(t)}\big(z(t), s(t), \tau(t)\big)\big] - E_{\hat{x}\sim p_r}\big[f\big(x(t), \tau(t)\big)\big] + p(\lambda) \quad (3)$$

$$L_G = E_{\hat{x}\sim p_g}\big[fG^{g(t)}(z(t), s(t), \tau(t))\big] \quad (4)$$

H. Performance Matrix

The proposed GAN-based model is evaluated using standard metrics such as ACC, PRE, REC, and F1. Here are the definitions of the confusion matrix elements:

- **True positive (TP):** Accurately labelling harmful network traffic as harmful
- **False positive (FP):** Mistakenly labelling lawful network traffic as hostile
- **True negative (TN):** Accurately distinguishing between authorized and actual network traffic
- **False negative (FN):** Incorrectly classifying malicious network traffic as legitimate

Accuracy

The ACC checks how well the IDS predicts normal and abnormal data. ACC is comparable to Equation (5).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (5)$$

Precision

One way to express the ACC is as a percentage of all normal recordings divided by all recordings that the IDS has deemed normal. It is through Equation (6) that PRE is monetized:

$$Precision = \frac{TP}{TP+FR} \times 100 \quad (6)$$

Recall

The REC compares the amount of actual recordings with the inter-class correlation coefficient (ACC) of the IDS's predictions. The REC is computed using Equation (7):

$$Recall = \frac{TP}{TP+FN} \times 100 \quad (7)$$

F1 Score

F1 is the arithmetic mean of REC and PRE. In order to determine the F1, use Equation (8):

$$F1 - score = \frac{2\times recall\times precision}{recall+precision} \quad (8)$$

IV. RESULTS AND DISCUSSION

The results of the experimental investigation that was carried out to detect outliers in the UNSW-NB15 dataset are presented in this section. In order to differentiate between legitimate and malicious network traffic patterns, the dataset employs a solved binary classification problem. The experiments were run in Python and a Jupyter Notebook in Google Colab, and the model was trained with the help of Tensor libraries, including TensorFlow, Keras, pandas, NumPy, seaborn, and matplotlib. The processing of large-scale network traffic data would be fast and efficient on a setup comprising an NVIDIA RTX 3070 graphics card, 32 GB of RAM, and an Intel Xeon-class processor. In classification, a GAN was employed, which is selected as a result of the complex data distributions mastering nature of the method and the complex anomaly patterns learning capability through the adversarial training. The model performance was evaluated in terms of ACC, PRE, REC and F1, which provided a detailed account of the detection capability. The testing validates that the GAN-based approach can be a useful tool for cybersecurity applications involving real-time network intrusion detection, and the findings demonstrate that it has a very high predictive ACC.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

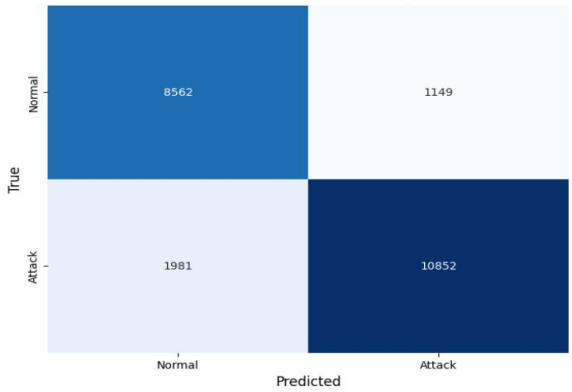

Fig. 5. Confusion matrix of the GAN model

The confusion matrix for the GAN-based anomaly detection model can be found in Figure 5. Classification results for normal and attack classes are shown in the table. The model demonstrates a robust detection capability, with 8,562 true negatives and 10,852 TP. As a result, the system generates 1,981 false positives and 1,149 false negatives in order to improve the overall prediction ACC and decrease the number of wrong classifications in network traffic analysis; further optimization is needed.

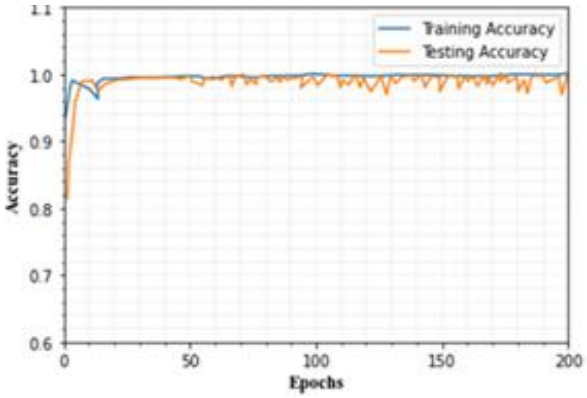

Fig. 6. Accuracy curve of the GAN model

The ACC curve for the GAN model over 200 epochs is presented in Figure 6. The ACC for both the training and the testing quickly converges to about 1.0 within the first 10 epochs and maintains stable performance throughout the training, which is strong evidence of the model having converged well and having the ability to generalize with very little overfitting in anomaly detection tasks.

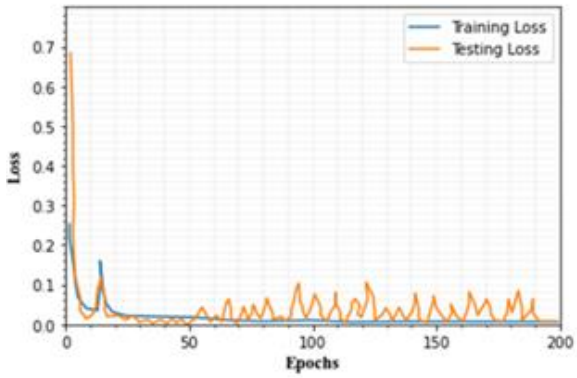

Fig. 7. Loss curve of GAN model

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

Figure 7 depicts the loss curve of the GAN model across 200 epochs. Both training and testing loss decrease sharply from initial values of approximately 0.7, converging near zero within 25 epochs. The testing losses have minor variations, which suggest consistent learning behaviour with appropriate model optimization during training.

Table 2: proposed models Performance on anomaly detection on UNSW-NB15 dataset

Measure	GAN
Accuracy	99.82
Precision	99.75
Recall	99.89
F1-score	99.88

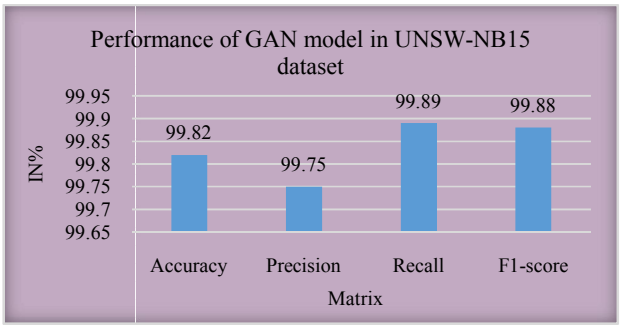

Fig. 8. Comparison of model performance metrics

Table II and Figure 8 demonstrate Table II displays the results of the applied GAN model's anomaly detection performance on the UNSW-NB15 dataset. With an impressive 99.82% ACC, 99.55% PRE, 90.99% REC, and 90.88% F1, the model performs admirably across all evaluation metrics. From what can tell, the model performs adequately enough in terms of FP and FN to warrant its usage in detecting network intrusions, and it also has a greater capacity to detect anomalies.

The proposed method for improving network intrusion detection systems employs a GAN design. In order for the model to detect complicated patterns and distinguish between typical and unusual network traffic, it is trained using an adversarial GAN architecture, which combines a generator with a discriminator. The generator generates fake data samples, and the discriminator checks their authenticity, thus establishing a competitive learning process that builds feature extraction and anomaly detection capacities. that it is trained on the UNSW-NB15 dataset, which consists of various network traffic patterns with several attack forms as well as normal ones. By training adversarial, the discriminator is able to discriminate well between legitimate network actions and malicious intrusions, and the generator is able to better approximate the distribution of normal traffic. In this type of adversarial mechanism, the model is able to learn complex data representations and accurately identify subtle anomalies that conventional approaches may miss, and thus this makes it relevant to real-time network security use.

A. Discussion

Table III compares the ACC, PRE REC, and F1 of many ML models that are used for AD. With scores of 99.82% ACC, 99.75% PRE, 99.89% REC, and 99.88% F1, the suggested GAN model outperforms the baseline approaches across the board. With an F1 of 88.9 and an ACC of 94.1, the KNN model consistently ranks second, while the DT ranks third with an ACC of 80.5. The lowest performance is observed in the ANN with a 77.51% ACC, 79.50% PRE and 77.53% REC, along with 77.28% F1. These findings conclusively prove that the GAN is better at identifying network anomalies, as it confirms the usefulness of the GAN in use in intrusion detection systems compared to standard machine learning methods.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 4, Issue 2, October 2024
Impact Factor: 7.53

Table 3: Comparison Between the Proposed Model and Existing Models for Anomaly Detection in Cybersecurity Environment

Model	Accuracy	Precision	Recall	F1 score
GAN	99.82	99.75	99.89	99.88
ANN[28]	77.51	79.50	77.53	77.28
DT[29]	80.5	94.1	84.2	88.9
KNN[30]	97.29	97.32	97.29	97.29

Table III includes a comparison of the performance of various ML models used to detect anomalies based on ACC, PRE, REC, and the F1 measures. The proposed GAN model also shows the best results in all measures, scoring 99.82% ACC, 99.75% PRE, 99.89% REC, and 99.88% F1, which is much better than the base methods. KNN model has the second consistent high 97.29% performance, and the DT has an ACC of 80.5, with relatively high ACC of 94.1 and with F1 of 88.9. The lowest performance is observed in the Artificial Neural Network with a 77.51% ACC, 79.50% PRE and 77.53% REC, along with 77.28% F1. These findings conclusively prove that the GAN is better at identifying network anomalies, as it confirms the usefulness of the GAN in use in IDS compared to standard ML methods.

Conclusion and Future Work

The rapid expansion of multi-interconnected infrastructures and advanced cyber-attacks has increased the pressure on smart and responsive network security solutions. The major issue with anomaly detection is that the distribution of attacks is highly skewed, with malicious activity represented by a low portion of the network traffic, leading to biased detection models. The conventional signature-based intrusion detection systems are incapable of detecting zero-day attacks, as well as evolving ones; therefore, they require sophisticated AI-based solutions. Using the UNSW-NB15 dataset, which contains a wide range of attack types (e.g., exploits, DoS, reconnaissance, and backdoor attacks), the paper proposes an AI-based Generative Approach to Robust Anomaly Detection. The methodology consists of data cleaning, one-hot encoding, feature scaling, dimensionality reduction using PCA and class balancing using SMOTE. An adversarial Generative Network (GAN) is subsequently trained to learn sophisticated attack features and detect fine anomalies, which are more effective than ANN, Decision Tree, and KNN. These findings highlight the strength and effectiveness of generative adversarial networks in real-time IDS in which early and accurate threat detection is central to the security of organizations

Future research involves the use of improved generative architecture, Explainable AI (XAI) to interpret and federated learning with privacy-preserving distributed detection. The proposed framework forms a strong basis towards the next-generation, real-time, and adaptive anomaly detection in the current cybersecurity ecosystem.

REFERENCES

[1] A. N. M. B. Rashid, M. Ahmed, L. F. Sikos, and P. Haskell-Dowland, "Anomaly Detection in Cybersecurity Datasets via Cooperative Co-evolution-based Feature Selection," *ACM Trans. Manag. Inf. Syst.*, 2022, doi: 10.1145/3495165.

[2] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly Detection for Cybersecurity of the Substations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011, doi: 10.1109/TSG.2011.2159406.

[3] J. Hong, C. C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, Jul. 2014, doi: 10.1109/TSG.2013.2294473.

[4] C. Sánchez-Zas, X. Larriva-Novo, V. A. Villagrá, M. S. Rodrigo, and J. I. Moreno, "Design and Evaluation of Unsupervised Machine Learning Models for Anomaly Detection in Streaming Cybersecurity Logs," *Mathematics*, vol. 10, no. 21, Oct. 2022, doi: 10.3390/math10214043.

[5] J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[6] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 4, Issue 2, October 2024 Impact Factor: 7.53

[7] S. B. Wankhede, "Anomaly Detection using Machine Learning Techniques," in *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, IEEE, Mar. 2019, pp. 1–3. doi: 10.1109/I2CT45611.2019.9033532.

[8] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Comput. Networks*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007, doi: 10.1016/j.comnet.2007.02.001.

[9] G. Narayan, "Intrusion Detection Based on Anamoly Using Artificial Neural Network," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 6, no. 6, pp. 11–14, Jun. 2018, doi: 10.22214/ijraset.2018.6003.

[10] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.

[11] R. Priyadarshini, K. Anuratha, N. Rajendran, and S. Sujeetha, "APMFT: Anamoly Prediction Model for Financial Transactions Using Learning Methods in Machine Learning and Deep Learning," in *Advances in Parallel Computing*, 2021. doi: 10.3233/APC210101.

[12] K. Nandhini, M. Pavithra, K. Revathi, and A. Rajiv, "Anamoly detection for safety monitoring," in *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, IEEE, Mar. 2017, pp. 1–6. doi: 10.1109/ICSCN.2017.8085682.

[13] K. Seetharaman, "Incorporating the Internet of Things (IoT) for Smart Cities: Applications, Challenges, and Emerging Trends," *Asian J. Comput. Sci. Eng.*, vol. 08, no. 01, pp. 8–14, Mar. 2023, doi: 10.22377/ajcse.v8i01.199.

[14] R. Patel, "Artificial Intelligence-Powered Optimization of Industrial IoT Networks Using Python-Based Machine Learning," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 138–148, 2023, doi: 10.56472/25832646/JETA-V3I8P116.

[15] S. K. Singh, M. H. Anisi, S. Clough, T. Blyth, and D. Jarchi, "CNN-BiLSTM based GAN for Anamoly Detection from Multivariate Time Series Data," in *2023 24th International Conference on Digital Signal Processing (DSP)*, IEEE, Jun. 2023, pp. 1–4. doi: 10.1109/DSP58604.2023.10167937.

[16] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1137–1151, Jun. 2021, doi: 10.1109/TNSM.2021.3078381.

[17] L. Akoglu, H. Tong, and D. Koutra, "Graph-based anomaly detection and description: A survey," *Data Min. Knowl. Discov.*, vol. 29, no. 3, pp. 626–688, May 2015, doi: 10.1007/s10618-014-0365-y.

[18] V. Shah, "Scalable data center networking: Evaluating VXLAN EVPN as a next-generation overlay solution," *Asian J. Comput. Sci. Eng.*, vol. 8, no. 3, pp. 1–7, 2023.

[19] H. P. Kapadia, "Generative AI for Real-Time Conversational Agents," *Int. J. Curr. Sci.*, vol. 13, no. 3, pp. 201–208, 2023.

[20] J. A, V. Ebenezer, A. J. Isaac, J. Marshell, P. Pradeepa, and V. Naveen, "Adversarial Attacks on Generative AI Anomaly Detection in the Quantum Era," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, IEEE, Nov. 2023, pp. 1833–1840. doi: 10.1109/ICECA58529.2023.10395092.

[21] R. Raturi, A. Kumar, N. Vyas, and V. Dutt, "A Novel Approach for Anomaly Detection in Time-Series Data using Generative Adversarial Networks," in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, IEEE, Jun. 2023, pp. 1352–1357. doi: 10.1109/ICSCSS57650.2023.10169365.

[22] F. Esmaeili, E. Cassie, H. P. T. Nguyen, N. O. V Plank, C. P. Unsworth, and A. Wang, "Anomaly Detection for Sensor Signals Utilizing Deep Learning Autoencoder-Based Neural Networks," *Bioengineering*, vol. 10, no. 4, Mar. 2023, doi: 10.3390/bioengineering10040405.

[23] M. K. Hooshmand and D. Hosahalli, "Network Anomaly Detection using Deep Learning Techniques," *CAAI Trans. Intell. Technol.*, vol. 7, no. 2, pp. 228–243, Jun. 2022, doi: 10.1049/cit2.12078.

[24] M. Abdelkhalek, G. Ravikumar, and M. Govindarasu, "ML-based Anomaly Detection System for DER

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 4, Issue 2, October 2024 Impact Factor: 7.53

Communication in Smart Grid," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/ISGT50606.2022.9817481.

[25] S.-V. Oprea, A. Bâra, F. C. Puican, and I. C. Radu, "Anomaly Detection with Machine Learning Algorithms and Big Data in Electricity Consumption," *Sustainability*, vol. 13, no. 19, Oct. 2021, doi: 10.3390/su131910963.

[26] U. A. Korat and A. Alimohammad, "A Reconfigurable Hardware Architecture for Principal Component Analysis," *Circuits, Syst. Signal Process.*, vol. 38, no. 5, pp. 2097–2113, May 2019, doi: 10.1007/s00034-018-0953-y.

[27] H. Benaddi, M. Jouhari, K. Ibrahimi, J. Ben Othman, and E. M. Amhoud, "Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks," *Sensors*, vol. 22, no. 21, Oct. 2022, doi: 10.3390/s22218085.

[28] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, vol. 7, no. 1, Dec. 2020, doi: 10.1186/s40537-020-00379-6.

[29] C. Park, J. Lee, Y. Kim, J. G. Park, H. Kim, and D. Hong, "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2330–2345, Feb. 2023, doi: 10.1109/JIOT.2022.3211346.

[30] S. Mokhtari, A. Abbaspour, K. K. Yen, and A. Sargolzaei, "A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data," *Electronics*, vol. 10, no. 4, Feb. 2021, doi: 10.3390/electronics10040407.