AI Driven Anomaly Detection in Network Traffic Using Hybrid CNN-GAN

Vuda Sreenivasa Rao [1,*], R. Balakrishna [2], Yousef A. Baker El-Ebiary [3], Puneet Thapar [4], K. Aanandha Saravanan [5], and Sanjiv Rao Godla [6]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fileds, Vaddeswaram, India
[2] Department of Artificial Intelligence and Data Science, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Inida
[3] Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin – UniSZA University, Malaysia
[4] Computer Science and Engineering Department, Lovely Professional University, Punjab, India
[5] VelTech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India
[6] Department of Computer Science & Engineering, Aditya College of Engineering & Technology-Surampalem, Andhra Pradesh, India
Email: vsreenivasarao@kluniversity.in (V.S.R.); r.balakrishna1989@gmail.com (R.B.); yousefelebiary@unisza.edu.my (Y.A.B.E.-E.); puneet.thapar90@gmail.com (P.T.); 5anand23sarvan@gmail.com (K.A.S.); sanjiv_gsr@yahoo.com (S.R.G.)
*Corresponding author

***Abstract*—As the complexity and sophistication of cyber threats continue to evolve, traditional methods of network anomaly detection fail to identify novel and subtle attacks. In response to this challenge, authors propose a novel approach to network anomaly detection utilizing a Hybrid Convolutional Neural Network (CNN) and Generative Adversarial Network (GAN) architecture. The hybrid model leverages the strengths of both CNN and GAN to enhance the detection of network anomalies. The CNN component is designed to extract high-level features from network traffic data, allowing it to capture complex patterns and relationships within the data. Simultaneously, the GAN component acts as a generator and discriminator, learning to generate normal network traffic patterns and distinguishing anomalies from them. To train the hybrid model, employing a large dataset of labelled network traffic, encompassing both normal and anomalous behavior. During training, the GAN generates synthetic normal traffic, creating a diverse set of normal data to train the CNN and help it generalize better to variations in network traffic. In experiments, the hybrid CNN-GAN model demonstrates superior performance in detecting network anomalies compared to traditional methods. It exhibits a high detection rate while minimizing false positives, making it a promising tool for enhancing network security using MATLAB software. The proposed approach contributes to the ongoing efforts to safeguard critical network infrastructures against evolving cyber threats by harnessing the power of AI-driven anomaly detection.**

***Keywords*—Generative Adversarial Network (GAN), Convolutional Neural Network (CNN), anomaly detection, cyber threats, network traffic data**

I. Introduction

The complexity and effectiveness of cyber-attacks are constantly rising in today's digital environment, posing enormous difficulties for network security. With the introduction of new and nuanced threats, conventional techniques of network detection of anomalies frequently find it difficult to keep up [1]. They offer a novel method for network anomaly detection that leverages the strength of a Mixed Convolutional Neural Network (CNN) with a Generative Adversarial Network (GAN) design in answer to this urgent demand for improved threat identification. This method is built on the combination of two cutting-edge deep learning methods, CNNs and GANs. CNNs have demonstrated their skill as feature extractors by identifying complicated patterns and correlations in large amounts of data [2]. They have found that being able to collect high-level features is quite useful for network traffic analysis. The GAN part of the model functions as a generator and discriminator, complementing the CNN part. It develops its capacity to recognize anomalies from these synthesized norms while concurrently learning to construct representations of typical network traffic patterns [3].

The hybrid model's training procedure is based on a huge and varied dataset that includes tagged network traffic. This dataset covers a wide range of network behavior, from standard, everyday behavior to the specifics of aberrant activities. By using such a large dataset, this model improves at spotting the minute variations that define network anomalies [4]. The constant growth of cyber threats challenges the established paradigm of network detection of anomalies in the never-ending cat-and-mouse game of cybersecurity. They offer

Manuscript received November 28, 2023; revised January 22, 2024; accepted January 24, 2024; published July 29, 2024.

a ground-breaking method that combines the strengths of a Mixed CNN and GAN design in response to this never-ending arms race, completely altering the network security environment [5].

The use of GANs throughout the training process is one of the pillars of the novel methodology. The GAN performs a dual function in this system, serving as both a generator and a discriminator. Its main responsibility is to produce synthetic copies of typical network traffic, which results in a large and varied collection of typical data. By enhancing the training dataset with this synthetic data, the CNN can gain knowledge from a wider range of network traffic changes [6]. The GAN-enhanced CNN displays better generalisation capabilities by offering a more thorough and nuanced perspective of typical network function. The hybrid CNN-GAN model demonstrates its excellent performance in the area of network anomaly identification through a number of thorough experiments. The model exhibits a remarkable capacity to accurately identify network anomalies while minimising false positives when compared to traditional approaches. This approach is positioned as a prospective instrument for raising network security to entirely novel heights because of this revolutionary capability [7]. The dedication to the continued fight against cyber dangers is demonstrated by the proposed merger of CNN and GAN technology. They want to strengthen crucial network infrastructures by utilising AI-driven anomaly detection to better protect them from the constantly evolving and highly skilled cyber adversaries that threaten the digital world. The collaboration between CNNs and GANs to improve the identification of network anomalies is highlighted in this research as they offer a novel method to network anomaly identification. They hope to herald in the next phase of network security with the merging of these two potent deep learning paradigms, one that is better prepared to combat the changing and more nefarious cyber threats that put the digital ecosystem at risk [8].

They put forth a cutting-edge strategy that makes use of the advantages of both the CNN and GAN designs to solve this urgent demand for improved network security. The extraordinary feature extraction capabilities of Convolutional Neural Networks (CNNs) have attracted wide recognition. These networks are excellent at identifying intricate patterns and connections in data, which makes them an ideal choice for traffic on networks analysis. But even CNNs aren't perfect, especially when it involves accurately generalising across differences in network data [9]. As part of the ground-breaking methodology, providing a hybrid CNN-GAN framework that mixes the powerful features extraction capabilities of CNNs with the generating and discriminative power of GANs. The hybrid model's CNN component is built to extract high-level characteristics from internet traffic data, enabling it to recognise complex and subtle patterns. The GAN element of the architecture simultaneously assumes a dual function, acting as a generator and a discriminator. Its main job is to pick up on the tiny nuances of typical network traffic so that it can distinguish it from abnormal conduct. They use a large and varied dataset of tagged network traffic to efficiently train the hybrid model. This dataset includes a broad range of network behavior, from common and good-natured patterns of traffic to the subtleties of aberrant actions [10]. This extensive training dataset not just enables the model to recognize recognised anomalies but also places it in a very accurate position to detect newly unseen risks. Traditional approaches for detecting network anomalies include authorization, statistical, rules-based, traffic analysis, and port scanning, but they are confined to recognized threats, have difficulty adapting, and may yield false positives or miss subtle assaults. These approaches frequently lack an understanding of context and rely on past data, rendering them ineffective in developing unique assault patterns. Advanced approaches like machine learning and behavioral analytics are increasingly being used to circumvent these constraints by reacting to changing threats and comprehending real-time network environments.

The use of the GAN throughout the training process is one of the main novelties of the methodology. The GAN adds a variety of realistic data to the training data as it creates synthetic representations of typical network traffic. This enhancement improves the CNN component's flexibility to real-world circumstances by allowing it to generalize more successfully across changes in network traffic [11]. The hybrid CNN-GAN system has proven to perform better than conventional anomaly detection techniques in a number of rigorous studies. It demonstrates a remarkable capacity to accurately and efficiently identify network problems while minimizing false positives. This method is positioned as a promising tool for boosting network security in real-world applications due to the balance between precision as well as false positive reduction [12]. In order to usher in an entirely novel phase of network detection of anomalies that is flexible, precise, and robust in the midst of rising cyber threats, the ground-breaking Hybrid CNN-GAN approach is prepared to play a crucial part in this quest. The design and operation of the Hybrid CNN-GAN model will be covered in detail in the parts that follows, along with data on how it is trained, evaluated, and used in the real world. Seeking to demonstrate the revolutionary potential of this cutting-edge approach in network detection of anomalies by a thorough examination of the approach and related experimental findings.

The following are the main contributions of the suggested Hybrid CNN-GAN technique for network anomaly detection:

- In this hybrid architecture, CNNs and GANs are combined for thoroughly analysing data on network traffic by producing typical patterns of traffic and retrieving high-level features.
- The CNN component's architecture makes it easier to spot complex patterns and changing cyber threats in network traffic information, improving detection beyond what is possible with conventional techniques.
- In order to increase dataset variety and the ability of CNN to generalize across different traffic

variances, the GAN creates synthetic typical network activity patterns during training. This eventually improves detection accuracy.

- According to experimental findings, the combined CNN-GAN model has a high rate of detection for network abnormalities, which is crucial for quick detection of hostile activity and enhancing network security.
- The proposed approach is more useful and practical in actual network security scenarios since it minimizes false positives, which lessens the effort on security staff.

The rest of this study is shown as follows: Section II describes similar efforts based on network anomaly detection, and so on, to explain the remaining portions of the paper. Section III provides an explanation of the issues raised in the associated works. The general methodology of the suggested hybrid CNN-GAN network-based anomaly detection is described in Section IV of the proposal. In Section V, the outcomes of the hybrid CNN-GAN-based anomaly detection are explained. Finally, Sections VI and VII explain the overall analysis and conclusion.

II. Related Works

Network anomaly detection is essential because it offers a powerful tool for stopping or blocking intrusions. A variety of Auto Encoder (AE) driven deep learning algorithms for network anomaly detection have been developed recently with the advent of Artificial Intelligence (AI) in an effort to strengthen the stance towards network security. Without providing a comprehensive approach to comprehend the significant implications of the core set of crucial performance metrics of AE algorithms and the detection accuracy, the performance of current state-of-the-art AE models utilized for networks anomaly detection differs. Xu *et al.* [13] propose a brand-new 5-layer Automatic Encoder (AE) model is better suited for applications involving network anomaly detection. The suggestion is based on the findings of a thorough and meticulous examination of a number of performance indicators utilized in an AE model. In order to mitigate model bias brought on by disparities in information across different kinds of data in the feature set, employ a novel data pre-processing mechanism in the suggested model that transforms and eliminates the most detrimental misfits from the input samples. For the model to determine if a sample of network traffic is normal or abnormal, the suggested model makes use of the most efficient reconstruction error function. The model is more suited for feature learning and reducing dimension thanks to these sets of cutting-edge techniques and the ideal model architecture, which improves detection accuracy and F1-Score. On the NSL-KDD dataset, tested the suggested model, which performed better than other comparable approaches by reaching the greatest accuracy and F1-Score of 90.61% and 92.26% in detection, respectively. One disadvantage is the requirement to evaluate the model's applicability and generalizability using a variety of intrusion attacks and dataset samples, along with potential difficulties in expanding it to classifications with multiple classes.

The quality of service for subscribers is significantly impacted by escalating cell failures and congestion, which are considered as abnormalities and cost the cellular carriers a significant revenue loss. Current research uses feed-forwards deep neural networks at the Core Network (CN) to detect the aforementioned issues in a single cell; however, the technique is unworkable because it will overwhelm the CN, which continuously monitors hundreds of cells. They divided the network into numerous 100-cell sections, each being watched by an edge server, in order to benefit from advances in Convolutional Neural Networks (CNNs) with deep layers and mobile edge computing. Hussain *et al.* [14] propose a system for pre-processing unprocessed call detail data with user behaviors into an image-like volume that is then supplied to a CNN model. A multileveled vector indicating the abnormal cell or cells is produced by the framework. The findings imply that the technology, which is adaptable and extendable for a manufacturing Internet of Things context, can identify anomalies with as much as 96% accuracy. The computational cost of manually tweaking hyperparameters or utilizing grid search is a downside, and it raises the possibility that future studies will use a more effective random search algorithm.

Some of the newest technological developments is artificial intelligence which allows machines to emulate human conduct. The most important tool used to spot cyberattacks or other unwanted activity is a system for Intrusion Detection (IDS). Artificial intelligence is frequently viewed as the superior technique for altering and developing IDS and is essential in identifying intrusions. Modern problems can be resolved using modern artificial intelligence techniques called neural network methods. Kanimozhi *et al.* [15] A sort of botnet assault that poses a major risk to financial and banking organizations is to be identified by the suggested system. The proposed technique is created utilizing artificial intelligence used on the largest and most current IDS Dataset of the Canadian Institute for Cybersecurity (CIC) via Amazon Web Services, also known as the CSE-CIC-IDS2018, which represents a real cyber defense dataset. With a precision score of 99.97%, an average surface area of the Receiver Operator's Characteristics (ROC) curves of 0.999, and a mean rate of false positives of just 0.03 the recommended smart neural network system works brilliantly. The proposed artificial intelligence-based intrusion detection system for botnet attack classification is robust, accurate, and exact. The newly suggested system can be utilized for traditional traffic analysis of networks, cyber-physical system traffic analysis, and real-time data on network traffic analysis. Scalability and performance concerns may arise when dealing with large datasets and additional attack classes, necessitating the usage of GPU-based optimizations and parallel processing structures, which may increase complexity.

Bibi *et al.* [16] explain Road surface imperfections are a serious problem for safe and effective traffic flow. As a result of inadequate building materials, high traffic

volumes, excessive traffic, and climate change, anomalies in road surfaces are rapidly getting worse. These defects need to be located and addressed to protect drivers, passengers, and vehicles from mechanical issues. Autonomous cars, which run without a driver's input and with the help of in-vehicle sensors, have been a study focus since the creation of Deep Neural Network (DNN) algorithms. Based on the integration of AI into vehicles, a combination of sensors and DNN techniques can assist autonomous vehicles assess their environment to identify tracks and barriers for straightforward movement. One of the biggest problems for autonomous vehicles is avoiding dangerous situations on the road caused by serious road defects. The concept of a vehicular network, also known as a Vehicular Ad Hoc Network (VANET), was developed by the Intelligent Transportation System (ITS) to guarantee security and safety in the flow of traffic, to handle concerns with accidents, and to communicate emergency data. A new method is proposed for the automatic detection of road imperfections by autonomous automobiles and the transmission of road data to vehicles approaching on the foundation of edge computing and VANET. The use of a vehicle cameras to take pictures of the road and the use of trained individuals for road anomaly identification could reduce the number of collisions and the risk of hazards on poor roads. Methods like Residual Convolutional Neural Network (ResNet-18) and the use of Visual Geometry Group (VGG-11) are utilized to consequently recognize and classify easy roads without deviations as well as paths with deviations like potholes, imperfections, and cracks using data from various internet sources. The results show that the models used outperformed competing techniques for locating road imperfections. There is a chance of greater complexity and challenges in the management of autonomous vehicles when combining different traffic abnormalities and preventive measures with less advanced models based on deep learning.

Cyberattacks and network intrusions have targeted modern IoT applications. The present technologies for identifying and avoiding invasions are unable to accurately identify any type of attack or abnormality in network activity due to a variety of constraints. Numerous machine learning-based strategies have also been provided by researchers, although they are ineffective for multi-class categorizing or classification accuracy. Xu *et al.* [17] Present an algorithm-based data-driven approach for anomaly and detection of intrusion that filters and analyses the data. The quality of the training dataset is improved by using mutual data as well as the Synthetic Minority Oversampling Technique (SMOTE) method. Additionally, automated intelligence is used to identify the technique that uses the best possible set of the hyper-parameter to categorize the data. This approach not only provides an excellent method without needing human computations for fine-tuning hyper-parameters but also lowers the cost of computation at running to verify the data. The resulting method solves the categorization with multiple class issues with 99.7% accuracy, outperforming the existing methods by a significant margin. The intricate nature and challenges of developing an intelligent algorithm that uses both transfer learning and reinforcement learning techniques to adjust to and classify new types of attacks could be detrimental. This can call for significant research and development activities.

Existing network anomaly detection approaches lack an integrated approach and a unified evaluation of essential performance metrics, which impedes complete knowledge and effective detection. In mobile network anomaly detection, feed-forward deep neural networks have the potential to overwhelm core networks, demanding more practical methods. While AI-based intrusion detection systems are quite accurate, scaling issues occur with huge datasets, necessitating more effective optimization methodologies. In traffic anomaly detection for self-driving vehicles, incorporating varied anomalies exposes a research gap in attaining effective control with simpler deep learning models. Current intrusion detection systems struggle with precision in the IoT setting, highlighting the need for better multi-class classification algorithms. These shortcomings underscore the need for novel technologies to boost network anomaly detection and improve network security against growing cyber threats.

III. Problem Statement

Addressing multiple issues in the fields of network safety and anomaly detection throughout several domains is the focus of the problem statement. First, there is a need for more efficient network anomaly detection techniques in the field of network security, especially using Auto Encoder (AE)-based deep learning methods, with an emphasis on comprehending and optimizing key performance indicators for increased detection precision and F1-Score. Secondly, the difficulty of detecting cell outages and overcrowding as anomalies in cell phone networks without overwhelming the core network needs a scalable strategy combining server edges and deep Convolutional Neural Networks (CNNs) for cell activity anomaly identification [18]. Thirdly, the goal of Intrusion Detection Systems (IDS) is to use artificial intelligence, especially neural network methods, for correctly identifying botnet attacks, but this must take into consideration scalability and performance constraints when handling massive data sets and extra attack classes. Last but not least, the issue in the field of roadway security is to automatically detect flaws in the road surface utilizing AI algorithms in autonomous vehicles, possibly via vehicle network ad hoc, while taking into account the complexity of managing various road abnormalities and preventive actions [19]. The combined need for novel AI-driven solutions to improve safety, reliability, and detection of anomalies across many domains is highlighted by the above statements. Malware, phishing, DoS attacks, threats from insiders, breaches of data, MitM attacks, zero-day vulnerabilities, advanced persistent threats, social engineering, and IoT-based threats are examples of cyber dangers. Antivirus software, email filtration, user awareness training, encryption, access restrictions, network security measures, regular upgrades, and sophisticated threat detection are all used to provide

protection. To manage risks, organizations utilize a defense-in-depth approach that includes preventative, investigative, and remedial measures as well as user training. Effective cybersecurity requires periodic risk assessments and the flexibility to respond to emerging threats.

IV. Proposed Hybrid CNN-GAN Method

In order to detect anomalies, the approach includes developing a combination of models which utilizes Convolutional Neural Networks (CNNs) over feature extraction from network activity information with Generative Adversarial Networks (GANs) for producing typical traffic patterns. Fig. 1 explains the overall conceptual Diagram.

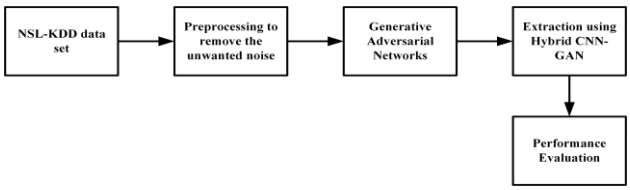

Fig. 1. Overall block diagram.

A. Dataset Collection

The most recent NSL-KDD data collection from 2009 was used in this study. The NSL-KDD information set has been presented as a solution to some of the problems associated with the KDD Cup'99 dataset (also present in DARPA'98) for IDS testing. NSL-KDD provides a more difficult attack distribution while resolving issues with the test data's massive amount of duplicate information and record duplication. The IDS scientific community has already embraced the NSL-KDD data collection. The 41 features of NSL-KDD, like their predecessors, are divided into three categories: basic features derived from TCP/IP communications; traffic features pertaining to a single host or service; as well as content characteristics based on information from packet contents [20]. Two distinct sets of the NSL-KDD information set are made available: trained (125,973 samples) as well as test (22,544 samples). The data is divided in a way that presents the greatest challenge to classifiers. The attack distributions of probabilities in both the test and train data sets are different, and 16 of the 38 classified dangers only appear in the evaluation data set. Additionally, just 2 or 3 samples across the entire database show the presence of various attacks.

B. Pre-Processing

Collecting data and doing exploratory data analysis are necessary for any machine learning inquiry. The dataset needed to be transformed into a classification feed as the first step in the process. Handling up the lost data became the first action as a result. The transmission anomaly has resulted in empty values in the "Accessed Node Type" and "Value" areas of the data set. The "Accessed Node Type" attributes, involving categorical data whereas the "Value" traits have continuous values, distinguish these two features [21].

There are additionally several approaches of matrix the data using classifications. It is common practice to use combined single hot coding and labels encoding. In order to transform the data into feature vectors, the labels encode technique was utilized in the present research. Although the majority of the attributes in the data collection possess nominal categorization values, they additionally include a large number of individual values. The total amount of characteristics could have substantially grown and the final data set might have contained multiple dimensions if these characteristics had been given a single hot encoding. However, the number of features stayed the same when label encoding was applied. This had no effect upon any dimension in the dataset. A hot encoding value would also need a lot of computation and have thinner qualities, which makes it harder to include into machine learning techniques. For labelling and encoding, the dataset is thus presented.

C. Hybrid CNN-GAN

The GAN uses a game-theoretic approach, in which a network tries to learn how to generate data from an initial distribution via a game with two players in which two adversaries or sub networks, namely a producer G (.) and a system for discrimination D (.), are locked in an unending fight. The engine learns to produce precise representations that are identical to those in the set used for training, whereas the discriminating machine learns to distinguish between real images and manufactured ones. A popular deep learning network design called GAN leverages CNN and is based on generative modelling. The network learns to calculate the latent space of the data distribution associated with its training set before creating output samples based on this distribution. Although GAN has proven to be a successful method for creating data, in practise GAN is challenging to train because two separate networks can be trained from a single the backpropagation with a combination of generate and discriminator loss. As a consequence, neural networks produce inaccurate output images. To reduce training instabilities and produce more accurate final images, Deep Convolutional GANs (DCGAN) apply architectural limitations across the generator and discriminator networks. The structure of GAN is shown in Fig. 2.

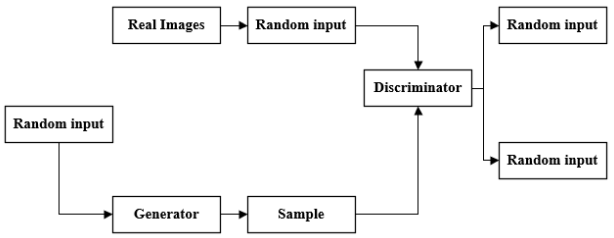

Fig. 2. GAN structure.

D. GAN for Anomaly Detection

GANs are exclusively developed with typical pictures when used for anomaly detection. Utilizing ordinary pictures to train a GAN, the discriminator learns to discriminate among genuine and recreated samples while

the generator understands a variety of original images and can reproduce normal images. There are no anomalous examples utilized during the training of the GAN network for anomaly identification. Whenever an anomalous picture is supplied to this train generator during testing, the image will continue to be rebuilt using the variety of normal data. The residual among the input anomalous query image and the one that was rebuilt, upon the other hand, will act as the anomaly. The training procedure is unsupervised since the GAN framework is not provided any guidance about how to recognize irregularities.

The discriminators assess how well the rebuilt picture is compared to the input image, and the generator produces a rebuilt normal image as well as a variety of normal images that it has learnt. During testing, a haemorrhage picture is fed into the network as its input, and the network outputs a reconstructed haemorrhage image based on the learnt manifolds by the generator, along a residual image which symbolizes the anomaly, as well as the discrepancy among the input and output haemorrhage images.

The generator and discriminator sub-networks make up the deep learning network design, that's comparable to the earlier work, Four successive deconvolution blocks constitute the generator in this design, which takes samples and maps low-dimensional latent vector *z* to high-dimensional pictures *x*. Fractionally stride deconvolution, batch normalization, and ReLU activations are all included in each of the first three blocks, while the final one is made up of Tanh (hyperbolic tangent) activation function. Using the 1D latent source noise vector *z*, that has a size of 100, the generator creates a vector of *pG* across what is actually seen *x* into a 2D manifolds with the same dimensions of the actual image. The discriminator *D*(.) is composed of four conventional convolution blocks that are activated with Leaky ReLU activations, and this down samples the generated images into a flattening layer before smoothing into its scalar output. Whether the outcome of *G*(*z*) is a "actual" or "fake" image, it is determined by the sigmoid activation function.

The discriminator *D* is taught during the training process to reduce the likelihood that produced pictures will be labelled as "fake" and the real training images will be classified as "real." Thus reducing $V_0(\mathrm{G}) = \log(1–D(G(z))$, the generator *G* is simultaneously educated to deceive the discriminator. The discriminator becomes better at successfully differentiating between genuine and created pictures while the generator gets better at producing realistic images during the adversarial training phase. While playing a min-max game to maximize the function *V*(*G*, *D*), the network is trained, and the goal function may be represented as in Eq. (1),

$$\min_G \max_D V_0(G,D) = E_x\left[\log\left(D(x)\right)\right] + E_z\left[\log\left(1 - D(G(z))\right)\right] \quad (1)$$

E. Extraction Using CNN

Convolutional Neural Network are the best deep learning implementation for dealing with multidimensional inputs like images, which are challenging for traditional neural networks to handle. CNN has a distinct layer in terms of the architecture. Following are the different levels of a standard CNN network:

1) Input layer: The input layers transfer the inputs that might include several dimensions, to the following layer.

2) Convolution layer: Convolution is applied to the data obtained from the layer of input using filters of a specific size that are present in this layer. Each convolution filter searches the input data, and the results of this process are applied to all information according to the filtering and step sizes.

3) Pooling layer: This layer completes its duties after the layers of convolution by compiling the information that the filters have gathered. The maximum pooling operations, which selects the highest number in the chosen screens, is frequently used to do these summarising operations.

4) Fully connected layer: This layers compressed input so that every input is connected to each perceptron. It is typically seen at the end of CNN. The existence of this level, along with perceptrons, can increase the accuracy of classification.

The map of features is the result of each layer of convolution on CNN combined with the pooling operation; the dimensions of the input data and filters have an important effect on the resulting feature map. The feature map may be created using a particular formula. The output may be determined using the following function in Eq. (2), for instance, if the input has a two-dimensional I_0(m, n) and the filters size are $F_0(a, b)$:

$$O_0 = \sum_a \sum_b I_0(m + a, n + b) F_0(a, b) \quad (2)$$

The results from the convolution component will be sent for the pooling layers in order to provide an additional abstract representation of the features map. Maximum pooling is frequently used as a viable method to carry out pooling procedures. A second filter of a specific size will be utilised during max-pooling. Stride regulates the distance that the filter goes when processing the input in addition to the filter size. After convolution and pooling, the output be transmitted to the layer that is completely linked to provides a flat representation of a feature map. A feed-forward neural network also that already exists is frequently connected to the flat view in order to improve the model's accuracy. Additionally to the inputs and filter sizes, several other aspects must be kept in account for CNN to perform successfully [22]. An example of among these elements is padding. Padding is the procedure of adding zeroes to the input's boundaries; this technique can help with filter scanning by making sure that everyone value is scanned only once as well as there shouldn't be any reputation problems due to the filter size. The Architecture of hubrid CNN-GAN is shown in Fig. 3.

Algorithm 1: Algorithm for Hybrid CNN-GAN

Step 1: Preparing Data and Pre-processing, Separate the dataset's normal and abnormal samples;

Step 2: Train the GAN to produce regular data. Setup the generator and discriminator networks in the GAN paradigm;

Step 3: Create artificial normal data. Make a lot of synthetic normal data samples;
Step 4: Train a CNN classifier. Convolutional and fully linked layers should be used to start the CNN model;
Step 5: Finding anomalies;
Step 6: Review and present the findings. Calculate and report performance indicators, such as the F1-Score, recall, and accuracy;
Step 7: Improving network designs and hyper parameters for improved outcomes.

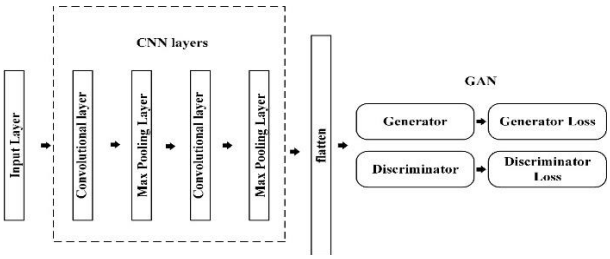

Fig. 3. Hybrid CNN-GAN architecture.

V. Results

A. Evaluation Metrics

In order to conduct the tests, the algorithm is trained exclusively on benign traffic; nevertheless, the test situation will include three cases: input information of only harmless, innocuous and nefarious and pure illicit traffic. Additionally, since this strategy attempts to significantly reduce processing time, choose to identify a new flow as malicious or not rather than carefully study the specifics of its attack type. In reality, if the suggested system finds a harmful flow, it will alert the user, send the data packets to a few off-line computational costly traffic classification methods for additional analysis, and stop the malicious flow all at once [23]. In order to evaluate performance on the basis of a binary classifier, numerous typical metrics are utilised in the sections that follow.

- True Positive (TP)—how many attack flows are actually classified as attacks.
- False Positive (FP)—quantity of harmless flows that are mistakenly categorised as attacks.
- True Negative (TN)—How many benign flows are appropriately categorised as normal?
- False Negative (FN)—the quantity of assault flows that are mistakenly categorised as normal.

The percentage of the overall amount of correctly classified items is measured by accuracy. The definitions of the terms precision, recall, and F1-measure are given. The final one is an overall correlation between precision and recall, and the first two show the percentage of accurate classifications that are affected by incorrect ones.

1) Accuracy: The level of precision with which the quantity being taken into account is compared to a standard or known value. Test results for a particular item that are close to a recognised value but very different from one another point to a lack of precision in the measurement. The formula for accuracy is Eq. (3).

$$Accuracy = \frac{TP+TN}{TP++TN+FP+FN} \quad (3)$$

2) Precision: Being exact entails having accuracy. It defines two or more measurements are to each other, irrespective of whether the measurements are exact or not. The formula in Eq. (4) provides the precision computation.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

3) Recall: Precision and recall are typically used together as a basic performance indicator. While accuracy evaluates quality, recall indicates quantity. Eq. (5) determines recall.

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

4) F1-Score: The accuracy and recall are expanded upon using the F1-Score that can be thought of as a harmonics average of accuracy and memory. It might serve as a useful gauge of performance for datasets with imbalances [24]. F1-Score is determined by Eq. (6).

$$F1 = \frac{2TP}{2TP} + FP + FN \; = 2 \times Precision \times \frac{Recall}{Precision+Recall} \quad (6)$$

B. Training and Testing Accuracy and Loss

Accuracy and loss during training and testing are crucial parameters for assessing the accuracy of machine learning networks. The model's efficacy on the training information during the training phase is reflected in the accuracy of the training data and loss. A good fit between the predictions and the training data is indicated by significant training correctness and low training loss. Testing accuracy and loss, on the other hand, gauges how effectively the framework generalizes to new data.

Fig. 4. Graph of training and testing loss.

Good testing accuracy along with low testing loss are ideal since they show that the model is capable of making precise forecasts on brand-new, untainted data. The model may have memorized the training information rather than discovering meaningful patterns if there is a significant difference between the testing and training measures. This is known as overfitting. Fig. 4 shows the training and testing loss of this model, when a machine learning or deep learning algorithm is being trained, the provided data shows the development and validation loss values over a number of epochs.

The trained loss and the testing loss show a continuous trend of lower numbers as the training moves across the epochs through 1 to 5. This decrease in loss indicates that the learning process is likely going well because the algorithm is gradually becoming better at fitting the data used for training and generalizing to new data. The tight alignment of the goal values and converging of the test and training loss rates indicate that the algorithm is learning and optimising its settings, and that it is getting better at making accurate forecasts as the number of epochs rises.

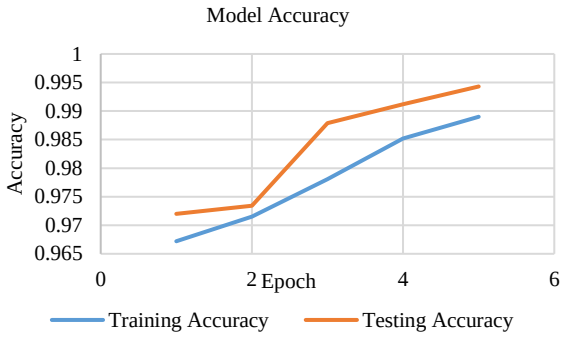

Fig. 5. Training and testing accuracy.

Throughout the training phase of a machine learning or deep learning model shown in Fig. 5, the provided data captures the training and testing accuracy values over a number of epochs. The training accuracy and testing accuracy both increase steadily from epoch 1 to epoch 5. The model's accuracy is growing on both the initial training and unknown testing datasets, which is reflected in an upward trajectory. The convergence of the testing and training accuracy scores indicates that the model performs well on the information it was trained on as well as generalizing successfully to fresh, illuminating its capacity to generate precise predictions. The model is growing and becoming better, as evidenced by this development over epochs.

C. ROC Curve

A graphical depiction used to assess the effectiveness of binary classification models is called a ROC curve. At different categorization criteria, it shows the compromise between TPR and FPR. In most cases, the curve begins at (0, 0), which represents the point that everything is identified as negative, then progressively slopes upward towards (1, 1) as the limit gets higher, signifying flawless classification. A framework is thought to be more effective at differentiating between both good and bad cases if its area underneath the ROC Curve (AUC) is higher.

Fig. 6 shows the binary classifications model's ROC curve. At various threshold settings, the FPR and TPR are displayed. The FPR begins at 0 and gradually rises as the threshold moves from 0 to 1, showing that additional false positives have been identified as positive. The percentage of true positives that are correctly classified, or TPR, rises concurrently as the threshold is tightened, eventually reaching 1 to indicate perfect classification. As the categorization threshold changes, this curve shows the compromise of correctly categorizing positive occurrences as positive (TPR) and mistakenly classifying negative examples as positive (FPR).

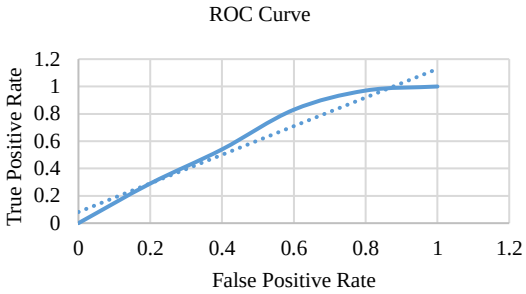

Fig. 6. ROC curve.

The suggested model's comparative performance metrics are presented in Table I. It shows the comparison of performance metrics of the existing and proposed model. The SVM classifier displays an acceptable accuracy of 80.22% combined with an excellent precision of 95.85% in the evaluation of various classifiers for a particular assignment, demonstrating its great capacity to accurately identify positive cases while minimizing false positives. With a recall rate of only 68.21%, it falls short and may overlook some important situations. The hybrid CNN-GAN approach combines CNN for feature extraction with GAN to generate synthetic normal data, which improves anomaly detection. When compared with SVM and DNN, it is more adaptable to complicated data distributions and has the capacity to detect minor anomalies, leading to cutting-edge network security performance.

TABLE I. COMPARISON OF DIFFERENT EXISTING METHODS WITH PROPOSED HYBRID CNN-GAN

Methods	Accuracy (%)	F1-Score (%)	Precision (%)	Recall (%)
SVM	80.22	79.72	95.85	68.21
DNN	72.28	69.97	91.26	56.73
CNN-GAN	99.43	85.23	97.35	83.64

The DNN classifier encounters issues with recall at 56.73%, suggesting possible trouble in catching all positive cases, but obtaining a success rate of 72.28% and an excellent precision of 91.26%. The CNN-GAN classifier, on the other hand, stands out with a remarkable accuracy of 99.43%, demonstrating its capacity to categorize examples accurately. It's balancing F1 rating of 85.23%, which reflects an equilibrium between recall (83.64%) and precision (97.35%), makes it a viable option for the assignment, especially when recall as well as precision are important factors to take into account.

D. Discussions

By combining a combination of CNN and GAN architecture, developed an innovative approach for detecting network anomalies in this research. When it comes to complex and newly evolving cyber threats, established methods of anomaly identification in network traffic frequently fall short. The hybrid model successfully overcomes this difficulty. In order to recognize intricate

connections and patterns within information, the CNN component shines in collecting high-level characteristics from network data. The GAN component, meanwhile, performs dual roles of generator and discriminator, gaining the capacity to generate typical network traffic trends while identifying anomalies. The GAN produces artificial normal traffic after being trained on a sizable dataset that includes labelled examples of both normal and unusual activity. This diversifies the dataset utilized for training the CNN and improves its capacity to respond to changes in network traffic. The hybrid CNN-GAN models outperform conventional approaches, obtaining a great detection rate while minimizing false positives, as shown by the experimental results. Through the effective instrument of AI-driven anomaly detection, this strategy represents a promising improvement in reinforcing network security operations and greatly contributes to protecting crucial network infrastructures from continuously changing cyber threats.

VI. Conclusion

As a result of combining the advantages of a Hybrid CNN and GAN architecture, the research has developed a ground-breaking solution to network anomaly detection. Traditional detection techniques have been shown to be ineffective in spotting new and subtle attacks in a time when cyber threats are becoming more complex. The hybrid model provides a reliable answer to this problem. They have created an adaptable and flexible anomaly detection system by combining the ability of CNN to extract high-level characteristics from network traffic information with the GAN's capacity to recreate typical traffic patterns while identifying anomalies. The hybrid CNN-GAN model has demonstrated improved performance through rigorous experimentation, attaining a remarkable detection rate while minimizing false positives. This advancement highlights the huge potential of AI-driven detection of anomalies in this field and makes a significant contribution to the ongoing effort to protect critical networks against the constantly changing landscape of cyber threats.

This strategy not only enables improved identification of anomalies but also lays the groundwork for ongoing development and adaptability as the field of cybersecurity changes. The hybrid approach can be improved in the future by incorporating the use of streams of real-time information and the creation of defenses against zero-day assaults. In order to ensure this technology's usability and scalability, efforts should also be made to install and integrate it into operational networks. In the end, research highlights the crucial role AI-driven solutions play in strengthening network security, providing a potential way to handle the ever-changing problems brought on by cyber-attacks in the digital age.

Conflict of Interest

The authors declare no conflicts of interest.

Author Contributions

V.S.R, R.B, B.T, and S.R.G collected, analyzed, and interpreted the data., K.A.S and Y.A.B.E.E supervised and contributed equally to the writing process. All authors had approved the final version.

References

[1] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, 100059, 2019.

[2] A. Aboah, "A vision-based system for traffic anomaly detection using deep learning and decision trees," in *Proc. the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 4207–4212.

[3] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2021.

[4] A. Yehezkel, E. Elyashiv, and O. Soffer, "Network anomaly detection using transfer learning based on auto-encoders loss normalization," in *Proc. the 14th ACM Workshop on Artificial Intelligence and Security*, 2021, pp. 61–71.

[5] J. Zhao, R. Masood, and S. Seneviratne, "A review of computer vision methods in network security," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1838–1878, 2021.

[6] K. M. Abuali, L. Nissirat, and A. Al-Samawi *et al.*, "Intrusion detection techniques in social media cloud: Review and future directions," *Wireless Communications and Mobile Computing*, 2023.

[7] D. K. Reddy, H. S. Behera, J. Nayak, P. Vijayakumar, B. Naik, and P. K. Singh, "Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 4121, 2021.

[8] Q. Xiao, J. Liu, Q. Wang, Z. Jiang, X. Wang, and Y. Yao, "Towards network anomaly detection using graph embedding," in *Proc. Computational Science–ICCS 2020: 20th International Conference*, Amsterdam, The Netherlands, June 3–5, 2020, pp. 156–169.

[9] J. Sinha and M. Manollas, "Efficient deep CNN-BiLSTM model for network intrusion detection," in *Proc. the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition*, 2020, pp. 223–231.

[10] W. Ullah, T. Hussain, Z. A. Khan, U. Haroon, and S. W. Baik, "Intelligent dual stream CNN and echo state network for anomaly detection," *Knowledge-Based Systems*, vol. 253, 109456, 2022.

[11] H.-J. Kim, J. Lee, C. Park, and J.-G. Park, "Network anomaly detection based on GAN with scaling properties," in *Proc. 2021 International Conference on Information and Communication Technology Convergence (ICTC)*, 2021, pp. 1244–1248.

[12] K.-T. Nguyen, D.-T. Dinh, M. N. Do, and M.-T. Tran, "Anomaly detection in traffic surveillance videos with gan-based future frame prediction," in *Proc. the 2020 International Conference on Multimedia Retrieval*, 2020, pp. 457–463.

[13] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, "Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset," *IEEE Access*, vol. 9, pp. 140136–140146, 2021.

[14] B. Hussain, Q. Du, A. Imran, and M. A. Imran, "Artificial intelligence-powered mobile edge computing-based anomaly detection in cellular networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 4986–4996, 2019.

[15] V. Kanimozhi and T. P. Jacob, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," in *Proc. 2019 International Conference on Communication and Signal Processing (ICCSP)*, 2019, pp. 0033–0036.

[16] R. Bibi, Y. Saeed, and A. Zeb, "Edge AI-based automated detection and classification of road anomalies in VANET using deep learning," *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–16, 2021.

[17] H. Xu, Z. Sun, Y. Cao, and H. Bilal, "A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things," *Soft Computing*, pp. 1–13, 2023.
[18] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: A systematic review," *IEEE Access*, vol. 9, pp. 78658–78700, 2021.
[19] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on Artificial Intelligence (AI) techniques for Vehicular Ad-Hoc Networks (VANETs)," *Vehicular Communications*, vol. 34, 100403, 2022.
[20] F. Iglesias and T. Zseby, "Analysis of network traffic features for anomaly detection," *Machine Learning*, vol. 101, pp. 59–84, 2015.
[21] M. Hasan, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, 2019.
[22] M. Alabadi and Y. Celik, "Anomaly detection for cyber-security based on convolution neural network: A survey," in *Proc. 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1–14.
[23] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and V.-L. Nguyen, "An unsupervised deep learning model for early network traffic anomaly detection," *IEEE Access*, vol. 8, pp. 30387–30399, 2020.
[24] Y. Guan. (2023). ACS-IoT: A CNN-BiLSTM model for anomaly classification in IoT networks. Project Paper. [Online]. Available: http://hdl.handle.net/10464/17884