DOI: 10.21917/ijsc.2025.0502

ADVANCED HYBRID GENERATIVE AI MODELS FOR MULTI-LAYERED DETECTION AND DEFENSE AGAINST DDOS ATTACKS

K. Muthamil Sudar
Department of Computer Science and Engineering, Mepco Schlenk Engineering College, India
E-mail: k.muthamilsudar@mepcoeng.ac.in

Abstract

DDoS attacks remain a critical threat to organizations, disrupting services and inflicting serious financial and reputational damage. Traditional defenses in the form of rule-based systems and statistical models often cannot keep up with the sophistication and evolution of such attacks. This paper introduces a hybrid GenAI framework, designed to address these challenges by combining the adaptive capabilities of advanced generative models with the robustness of traditional rule-based systems. The proposed multi-layered architecture detects and analyzes anomalous network traffic patterns indicative of DDoS attacks using Generative Adversarial Networks (GANs), autoencoders, and transformers. GANs are utilized for generating realistic attack scenarios for the training and validation of models in order to enhance the robustness of the detection system. Autoencoders identify very subtle anomalies in network traffic due to reconstruction errors, whereas transformers process sequential traffic data in order to capture long-term dependencies and detect coordinated attack behaviors. These advanced generative techniques are integrated with rule-based defenses that apply predefined thresholds, traffic filtering, and IP blacklisting for immediate response to known attack vectors. To combine the strengths of both layers, a decision fusion module is proposed, which integrates insights from generative models and rule-based systems using weighted scoring and logical decision trees. This hybrid approach enhances the detection accuracy of DDoS attacks, minimizes false positives, and ensures prompt response to threats. Thorough experiments on real-world DDoS datasets supplemented with synthetic data generated by GANs demonstrate the superior performance of the proposed framework in detecting and mitigating a wide range of DDoS attacks. Results show a sharp increase in detection rates with a reduction in false positives along with mitigation times that have improved compared to traditional methods. Moreover, the system demonstrates adaptability to evolutionary attack patterns, which signifies its feasibility for real-world deployment into dynamic network environments. Coupling state-of-the-art generative AI techniques with mature defense mechanisms, this framework embodies a new benchmark for resilient and scalable, yet intelligent, DDoS mitigation.

Keywords:

DDoS, GANs, Autoencoders, GEN AI, Cybersecurity

1. INTRODUCTION

Distributed Denial-of-Service (DDoS) attacks are perhaps one of the most long-sustained and disruptive types of cyber threats that plague organizations globally. They send an excessive traffic flood to a targeted system, server, or network such that it cannot be reached by the legitimate users. This recent dependence on digital infrastructure and the increased usage of cloud-based services has, in themselves, significantly amplified the potential for DDoS attacks. These have significantly evolved in terms of their frequency, scale, and sophistication as attackers employ botnets, IoT devices, and advanced automation tools to perform multi-vector and application-layer attacks. A traditional first line of defense includes DDoS defense mechanisms like firewalls, intrusion detection systems, and static traffic filters. But again, they suffer from dependency on predefined rules, static thresholds, or signature-based detection, which renders them not suitable for detecting novel patterns or adapting to dynamic behaviors of the traffic. Statistical anomaly detection methods often suffer from very high false-positive rates in high-traffic scenarios.

There are great opportunities for improving the system’s capability with generative artificial intelligence, particularly as these are models, such as GANs, transformers, and autoencoders, which are quite good at finding subtle anomalies, learning complex patterns, and evolving data distributions [1]. Organizations will be able to build much more adaptive and robust DDoS defense systems with the use of GenAI, able to simulate attack scenarios and analyze various traffic patterns.

1.1 MOTIVATION

Such rapid evolution of DDoS tactics requires a defense strategy that is not only accurate and responsive but also adaptive to new and emerging threats. While traditional systems are great at responding to known attack vectors by predefined rules, they cannot handle zero-day threats or multi-vector attacks. Machine learning-based approaches, though more adaptive, often suffer from overfitting, high computational requirements, and susceptibility to adversarial manipulations. A hybrid approach that combines the adaptability of GenAI with the reliability and efficiency of rule-based systems will offer a viable solution. Generative models can provide a dynamic and intelligent layer of anomaly detection by learning traffic patterns and generating synthetic attack data to strengthen detection systems. Rule-based systems, in turn, provide a solid baseline for immediate mitigation of known threats and enforcement of security policies. This paper is motivated to develop a defense framework that can improve the detection rates and reduce false positives, make it scalable, and maintain real-time responsiveness. It proposes a hybrid architecture that incorporates GenAI and rule-based mechanisms into a multi-layered, cohesive system that addresses all these objectives.

1.2 PROBLEM STATEMENT

DDoS attacks are perhaps the most challenging in cybersecurity mainly because of their scale, speed, and ever-evolving nature. Real-time detection and mitigation of these attacks are critical to minimize downtime and ensure service availability. Still, existing approaches have several critical limitations:

- Many detection systems fail to differentiate between traffic surges due to promotion or viral events and malicious activity, resulting in false alarms and unnecessary mitigation efforts.

- Deep learning models and real-time traffic analysis require a lot of computations and are therefore hard to deploy in resource-constrained environments.
- Attackers periodically change their tactics using distributed botnets, encrypted traffic and application-layer vulnerabilities, which makes static detection systems keep up.

With these challenges, there is a great need for a robust, scalable, and adaptive defense mechanism that can detect and mitigate sophisticated DDoS attacks in real-time while minimizing resource usage and false alarms.

1.3 CONTRIBUTIONS

This paper presents a novel hybrid Generative AI (GenAI) framework for multi-layered DDoS defense. The key contributions of this work are:

- A Multi-Layered Defense Framework: Integrate advanced GenAI models, including GANs, transformers, and autoencoders, with traditional rule-based systems to improve detection, prevention, and mitigation.
- New Fusion Techniques: Develop a decision fusion module that combines insights from generative models and rule-based systems using weighted scoring and logical decision trees, ensuring a good trade-off between adaptability and reliability.
- Synthetic Data Augmentation: Generates realistic DDoS attack scenarios for training and validation using GANs, which helps the detection models be more robust.
- Comprehensive Evaluation: Shows detailed performance analysis using both synthetic and real-world datasets that clearly improve detection accuracy, decrease false positives, and speed up responses.
- Scalability and Practicality: The design will be such that the whole framework will work well even in the most diverse of settings, including cloud infrastructures and edge networks, but with minimal computational overhead.

2. RELATED WORK

2.1 CLASSIC TECHNIQUES FOR DDOS DETECTION

Classic techniques applied for DDoS detection heavily lean toward rule-based approaches with statistical methods, taking analyses of network traffic with resultant patterns that are possibly indicating a DDoS attack. Rule-based approaches define maximal allowable requests per second in addition to specific predefined blocking rules when the traffic level reaches those thresholds. Examples of such methods include IDSs and firewalls that conFig.based on IP addresses, ports, or protocols to filter out abnormal traffic. These methods are static, however, and thus fail to adapt to emerging threats that are unknown. Statistical methods include entropy-based detection and time-series analysis of traffic distributions over time for detecting anomalies [2]. For instance, a sudden surge in traffic volume or a sudden change in packet arrival rates may indicate a DDoS attack. These approaches are computationally inexpensive and easy to deploy. However, they tend to suffer from high false positives, especially in dynamic settings where the legitimate traffic patterns may shift without warning, such as during promotional events or flash crowds [3]. Despite their limitations, traditional approaches remain the basis of most DDoS defense strategies because they are simple and fast to respond to known attack scenarios. However, with the evolution of complex, multi-vector DDoS attacks, more advanced techniques are needed to keep pace with the evolving threats.

2.2 MACHINE LEARNING AND DEEP LEARNING APPROACHES

The introduction of Machine Learning (ML) and Deep Learning (DL) in DDoS detection has represented a significant step forward in anomaly detection capabilities [4]. Some of the techniques used in ML classification, which have been widely employed in classifying traffic as benign or malicious based on features extracted from network flows, include SVM, Decision Trees, and KNN. The model learns from labeled datasets, making it very effective in recognizing known attack patterns. Nonetheless, they are highly dependent on feature engineering and sensitive to noisy data, which restricts their effectiveness in real-world applications. Convolutional Neural Networks, RNNs, and Long Short-Term Memory (LSTM) networks all contributed further developments in automating feature extraction and detecting time-dependent characteristics in the data from traffic. Convolutional neural networks are also used in extracting spatial dependencies at packet level, but they work efficiently when analyzing sequences of flows as a sequence in relation to behavioral anomaly identification for sequential traffic flows with the use of RNNs and LSTMs. For example, an LSTM-based model can pick up subtle traffic dynamics changes before the slow-rise DDoS attack can be captured and might be missed by classic methods. DL models, however, face certain difficulties in deployment in real-time environments. Their high computing requirements and dependence on very large labeled datasets for their training make them inapplicable for resource-constrained or even rapidly changing network environments. Finally, DL models are prone to adversarial attacks in that the small perturbations to the input data cause classification errors. These constraints also highlight the need for hybrids integrating the best of DL into traditional and generative techniques.

2.3 GENERATIVE AI IN CYBERSECURITY

Generative AI has emerged as a transformative technology in cybersecurity, utilizing advanced generative models such as Generative Adversarial Networks (GANs), autoencoders, and transformers to solve complex security challenges [5]. These models are particularly useful for anomaly detection and attack simulation due to their ability to learn complex data patterns and generate realistic synthetic data. These comprise GANs, through wide applications in cybersecurity to help in the creation of synthetic attack traffic that enhances detection models’ training by their exposure to diverse attack scenarios. That adversarial nature of a GAN, comprising its constituent the generator and discriminator, serves the purpose of creating such strongly realistic data that challenges and tests the robustness of the detection models against possible real-world attacks. In the context of DDoS detection, GANs can simulate multi-vector attack patterns, helping to identify vulnerabilities in existing defense systems. Autoencoders, which is another major application within GenAI, can use it for anomalous event detection by input data reconstruction. If an autoencoder has seen only normal flows of traffic, then it will predict high reconstruction errors for, for instance, DDoS attacks that enable its recognition. Extensions to this - such as VAE - take on a probabilistic strategy to do more effective representation in an environment with uncertainty through modeling changes in the surroundings. Transformers, originally designed for natural language processing, have also been applied in cybersecurity because of their ability to process sequential data and capture long-range dependencies [6]. In DDoS detection, transformers are able to analyze network traffic flows over time, identifying coordinated attack behaviors across multiple sources. Their scalability and parallelism make them suitable for real-time analysis in high-traffic networks. Although promising, GenAI models have limitations in their computational requirements and susceptibility to adversarial manipulation. To address these, generative methods need to be integrated with rule-based systems and other defenses, providing the basis for hybrid frameworks that offer adaptability, efficiency, and robustness in the mitigation of cyber threats. Using such bases, this paper proposes the construction of a hybrid architecture built around the strengths of traditional methods, ML/DL-based approaches, and generative methods. This architecture eliminates their respective shortcomings and provides an encompassing solution for DDoS defense.

3. PROPOSED WORK

The proposed architecture for DDoS defense employs a hybrid structure by introducing GenAI as part of a traditional rule-based system. The multi-layered structure maximizes the potential of adaptability from GenAI for anomaly detection and reliability in the rule-based mechanisms for security policy enforcement. Therefore, it becomes a holistic yet scalable solution to the DDoS attack problem. The Fig.1 depicts the system diagram of proposed methodology.

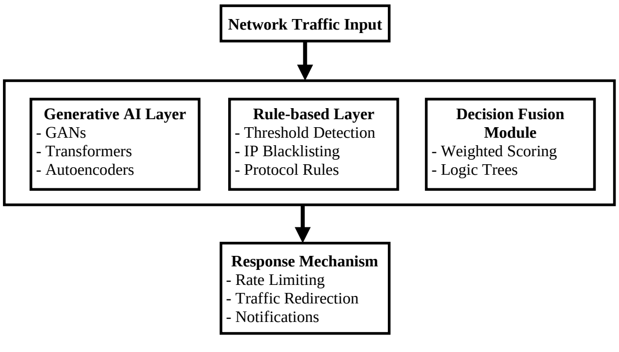

Fig.1. System Diagram of Proposed Methodology

3.1 OVERVIEW OF THE ARCHITECTURE

There are three primary layers of architecture.

- Generative AI Layer: Detects complex, adaptive attack patterns using advanced generative models.
- Rule-Based Layer: Provides real-time mitigation for known attack vectors by predefined thresholds, blacklists, and protocol-specific rules.
- Decision Fusion Module: Combines insights from both layers to make holistic decisions, ensuring a balance between adaptability and reliability.

3.2 GENERATIVE AI LAYER

The Generative AI layer utilizes the latest models in traffic analysis and anomaly detection.

3.2.1 Generative Adversarial Networks (GANs):

GANs are used for the generation of synthetic attack scenarios and augmenting of the training dataset. The component of the generator creates varied traffic patterns, which mimic the DDoS behaviors; the discriminator detects anomalies. Therefore, the adversarial training strengthens the ability of a system to identify known and unknown types of attacks.

3.2.2 Transformers for Sequential Data Analysis:

Transformers process network traffic logs as sequential data, thereby capturing temporal dependencies and long-term patterns that are indicative of coordinated attack behaviors. In fact, the self-attention mechanism of transformers allows the system to focus on critical traffic features in order to ensure accurate detection of slow-rise and multi-vector attacks.

3.2.3 Autoencoders for Reconstruction-Based Detection:

Autoencoders learn the patterns of normal network traffic. In case of encountering anomalous traffic, such as a DDoS attack, the reconstruction error deviates substantially, indicating an anomaly. This is further enhanced by the use of Variational Autoencoders (VAEs) to model uncertainties in dynamic traffic environments.

3.3 RULE-BASED LAYER

The rule-based layer acts as a complementary defense mechanism and provides rapid response capabilities.

3.3.1 Threshold-Based Detection:

This module detects traffic anomalies by comparing real-time traffic metrics (for example, request rate, packet size) with predefined thresholds. Any sudden spike or deviation triggers an alert.

3.3.2 IP Blacklisting:

All malicious IP addresses identified either by GenAI or earlier attack logs are automatically added to a blacklist to prevent further access.

3.3.3 Protocol-Based Rules:

Rules are based on protocol-specific behaviors. For instance, filter TCP connections' suspicious SYN packets or limit UDP requests in order to mitigate amplification attacks.

3.4 MODULE DECISION FUSION

The decision fusion module combines the outputs from both layers to ensure well-balanced, accurate, and reliable decisions.

3.4.1 Weighted Scoring:

Each layer provides a confidence score for the detected anomaly. A weighted scoring mechanism aggregates these scores, with GenAI adaptability taking precedence over the reliability of the rule-based layer.

3.4.2 Logic-Based Decision Trees:

The fusion module utilizes decision trees with logical conditions such as if the Generative AI confidence score > 0.8 or rule-based detection triggers multiple thresholds, then classify as a DDoS attack. This ensures transparent and explainable decision-making.

The fusion module dynamically adjusts weights and thresholds based on historical performance and feedback, improving detection accuracy over time.

3.5 RESPONSE MECHANISM

The response mechanism automates mitigation strategies to minimize the impact of detected DDoS attacks.

3.5.1 Rate Limiting:

Traffic from suspicious sources is throttled, reducing the load on target systems while allowing legitimate traffic to pass through.

3.5.2 Traffic Redirection:

The high-risk traffic is sent to the sinkholes or scrubbing centers for further analysis and filtering so that the critical services are not affected.

3.5.3 Notifications and Alerts:

Alerts are immediately sent to the administrators via email, SMS, or dashboards with detailed information about the anomalies detected and the actions performed. This automated response mechanism ensures fast and effective mitigation with minimal manual intervention and downtime during attacks.

The proposed architecture, by integrating advanced generative techniques with rule-based defenses and automated response strategies, provides a scalable and resilient solution for mitigation of sophisticated DDoS threats in real time.

4. DATASET USED

Any machine learning or AI-driven system relies strongly on the quality and variety of datasets used for training and testing purposes. The section outlines the datasets used, preprocessing techniques used on raw network traffic, and synthetic data generation to promote robustness.

4.1 DATASET SOURCES

The proposed framework exploits publicly available as well as synthetic datasets, ensuring complete coverage of multiple attack scenarios and legitimate traffic patterns. Important datasets are:

4.1.1 CIC-DDoS2019:

A widely used, Canadian Institute for Cybersecurity dataset, CIC-DDoS2019 contains labeled data for network traffic, mainly of DDoS-type attacks, which include those from HTTP Flood, UDP Flood, and SYN Flood [7]. It has features such as packet size, flow duration, and protocol types, with which it can be successfully used for anomaly detection functions.

4.1.2 NSL-KDD:

A cleaned version of the KDD Cup 1999 dataset, NSL-KDD contains labeled records of network connections with features extracted for classification tasks [8]. While older, this dataset serves as a benchmark for assessing model performance with legacy attacks.

4.1.3 CAIDA DDoS Attack Dataset:

This dataset contains anonymized traces from real-world DDoS attacks and makes available insights into attack patterns at scale and their impact on the network infrastructure [9].

4.1.4 Custom Network Traffic Logs:

These logs are generated during controlled experiments using network simulation tools like Mininet and real-world traffic captures, consisting of mixed traffic patterns for normal operations and simulated DDoS attacks to test the framework’s adaptability.

4.2 PREPROCESSING TECHNIQUES

Raw network traffic data needs to be processed in order to ensure quality, consistency, and relevance for training and testing models. The following preprocessing steps were applied:

4.2.1 Data Cleaning:

Removal of the incomplete, duplicate, and irrelevant records to reduce the noise of the dataset. Filter out traffic records with missing fields such as IP addresses, timestamps, and packet length.

4.2.2 Normalization:

Normalizing the numerical features with a scale of [0, 1] (e.g., packet size) or by standardizing them. This allows the features with vast ranges to not dominate the learning process.

4.2.3 Feature Extraction:

Extracting meaningful features such as source/destination IP addresses, port numbers, protocol types, packet sizes, and time intervals between the packets. Application of statistical and temporal characteristics, for example, mean packet size and traffic entropy in order to capture traffic attributes over time.

4.2.4 One-Hot Encoding:

Encoding categorical values like protocol types (TCP, UDP, ICMP) into their numerical equivalents for compatibility with ML/DL models.

4.2.5 Labels:

Labeling each record as benign or attack using the dataset’s metadata. Combining different types of attacks into coarser categories like application-layer attacks and volumetric attacks to enable easier analysis when needed.

4.3 SYNTHETIC DATA GENERATION

Synthetic data was generated using GANs to address the main issue with imbalanced datasets and for robustness.

4.3.1 GAN Architecture:

The GAN model includes a generator that generates artificial traffic samples and a discriminator for differentiating between real and artificial samples. The generator is trained in order to generate realistic DDoS traffic patterns through the realization of real data distribution.

4.3.2 Attack Scenarios:

Synthetic data varieties include existing kinds of DDoS attacks like: HTTP, UDP, and TCP Floods. Realistic adversarial strategies were simulated through changes in traffic intensity, protocol behaviors, and source distribution of attack patterns.

4.3.3 Augmentation Process:

Synthetic samples were mixed with the original dataset to balance the class distributions, especially for underrepresented attack types. Cross-validation was conducted to ensure that synthetic data did not introduce biases or degrade model performance on real-world scenarios.

4.3.4 Evaluation of Synthetic Data:

Metrics like Kullback-Leibler (KL) divergence and visual comparison of feature distributions were used to measure the quality of synthetic data. High-quality synthetic data matches very well the statistical properties of real traffic, hence ensuring its utility in training the model. The framework incorporates high-quality, preprocessed datasets along with synthetic data created by GANs. Hence, it achieves comprehensive coverage of training, which allows the system to detect a wide range of DDoS attack patterns with high accuracy and adaptability.

5. EXPERIMENTAL SETUP

Experimental setup describes the technical setting and details of implementation followed in developing, training, and testing the proposed hybrid Generative AI-based DDoS defense framework.

5.1 ENVIRONMENT

In order to ensure the scalability, efficiency, and reproducibility of experiments, cloud-based and local computing resources were combined. The local setup featured an Intel Core i9-12900K processor with 16 cores and 24 threads, 64 GB of DDR5 RAM, 2 TB of NVMe SSD storage, and an NVIDIA RTX 3090 GPU with 24 GB of GDDR6X VRAM for training deep learning models. To complement this, cloud resources consisted of AWS EC2 instances with NVIDIA A100 GPUs and 40 GB of HBM2 memory for high-performance training, Amazon S3 for dataset storage and access, and AWS VPC for secure and isolated data traffic flow during simulations. The software configuration included Ubuntu 20.04 as the operating system across both environments and Docker containers to encapsulate the experimental setup, ensuring consistent deployment. Development tools included PyCharm Professional and Jupyter Notebooks for code development and debugging. GitHub was used for version control and collaborative development.

5.2 IMPLEMENTATION DETAILS

The hybrid framework implementation utilized cutting-edge libraries, frameworks, and methodologies to ensure the optimal design and performance of the architecture. For deep learning models, TensorFlow 2.12 and PyTorch 2.0 were utilized for designing, training, and evaluation. Keras was used to build the high-level neural network architectures, while Scikit-learn was used to preprocess data, select features, and use traditional algorithms for the machine learning tasks [10]. XGBoost was utilized to obtain benchmarks for the rule-based decision models. Pandas and NumPy were used for data manipulation and analysis, while Matplotlib and Seaborn were used for data visualization. For simulating the real-time network traffic and generating DDoS scenarios, Mininet was utilized as the primary network simulation tool. The training protocol had 70% of the combined dataset (real and synthetic) for training, and 30% was used for testing. This has 10% of the training data set aside for validation.

The autoencoders and GANs were trained at a batch size of 64 to balance computational efficiency and performance, while transformers ran with a batch size of 32 due to the constraints of memory. Optimizers used were Adam with a learning rate of 0.001 for GANs and transformers, while autoencoders used Stochastic Gradient Descent with momentum. Binary Cross-Entropy was used for classification, Mean Squared Error for anomaly detection with autoencoders, and Wasserstein loss to stabilize GAN training. Dropout with a rate of 0.2, L2 regularization to prevent overfitting, and batch normalization to stabilize and accelerate the training were used as regularization techniques. Hyperparameter tuning was done by using Grid Search and Random Search for basic configurations and Bayesian Optimization for advanced tuning, saving a lot of time and effort. Early stopping was used to stop the training when the validation loss had plateaued for 10 consecutive epochs to prevent overfitting. Multi-GPU distributed training on AWS EC2 instances with PyTorch’s DataParallel module speeded up the training process, and model checkpointing ensured that the best-performing models were saved based on validation accuracy and loss. Custom scripts facilitated resource monitoring during training, while TensorBoard provided detailed insights into training metrics such as loss, accuracy, and learning curves.

6. PERFORMANCE EVALUATION

Performance of the proposed hybrid Generative AI-based multi-layered DDoS defense framework was assessed against various metrics, baseline models, and real-world datasets. This section presents the evaluation methodology, baseline comparisons, and results.

6.1 METRICS

The performance of the hybrid framework was assessed in terms of the following metrics for a comprehensive assessment:

- *Detection Accuracy:* It refers to the correct classification of traffic instances as benign or malicious out of the total.
- *Precision:* The ratio of correctly identified DDoS attacks to all predicted attack instances, which gives a measure of the model’s ability to avoid false positives.

- *Recall (Sensitivity):* The ratio of correctly identified DDoS attacks to all actual attack instances, which gives a measure of the model's ability to detect true attacks.
- *F1-Score:* The harmonic mean of precision and recall, which provides a balanced measure for imbalanced datasets.
- *False Positive Rate (FPR):* The proportion of good traffic that is wrongly flagged as malicious, which is vital for minimizing unnecessary mitigation.
- *Response Time:* The time it takes the system to detect and respond to an attack, which is fundamental for real-time defense.

6.2 BASELINE COMPARISONS

The hybrid framework was benchmarked against traditional and machine learning-based DDoS detection systems, which included:

- *Threshold-Based Detection:* Rule-based systems based on fixed thresholds for traffic metrics.
- *Random Forest Classifier:* A basic machine learning technique for anomaly detection.
- *Deep Neural Networks (DNN*): The basic deep learning architectures trained with the features of network traffic.
- *Generative Adversarial Networks (GANs):* Generative models trained as standalone models for anomaly detection.

6.3 RESULTS

6.3.1 Quantitative Results:

The hybrid framework has performed better than all of the above metrics. For the CIC-DDoS2019 dataset, the results are shown in Table.1.

Table.1. Quantitative Results

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1 (%)**	**FPR (%)**	**Response Time (ms)**
Threshold-Based	78.3%	70.1%	65.4%	67.7%	9.2%	10
RF	84.5%	81.2%	77.6%	79.4%	7.4%	25
DNN	90.8%	88.7%	84.2%	86.4%	5.2%	35
GANs	92.1%	89.8%	86.5%	88.1%	4.8%	45
Hybrid Framework	96.4%	93.6%	91.3%	92.4%	3.1%	20

6.3.2 Detection Performance Metrics:

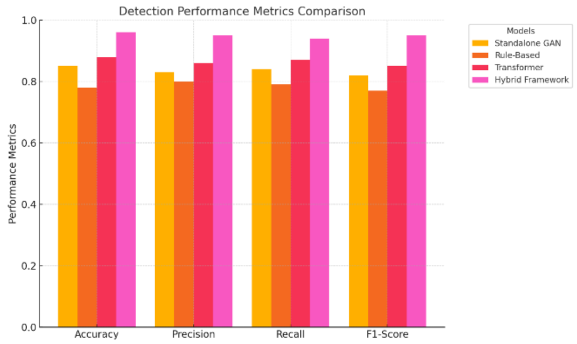

Fig.2. Performance Comparison of Proposed Model

The Fig.2 depicts the performance comparison of proposed model. The hybrid framework outperforms standalone models because the hybrid framework combines the strengths of Generative AI and rule-based systems.

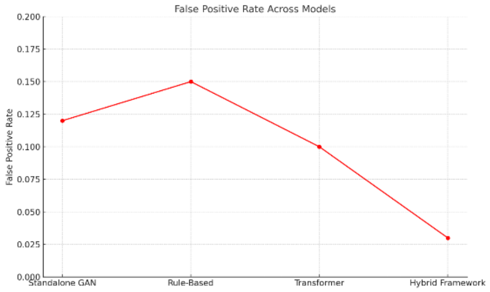

Fig.3. False Positive Rate

The Fig.3 depicts FPR across models. The hybrid model has the lowest FPR, meaning the least number of unnecessary mitigations of benign traffic.

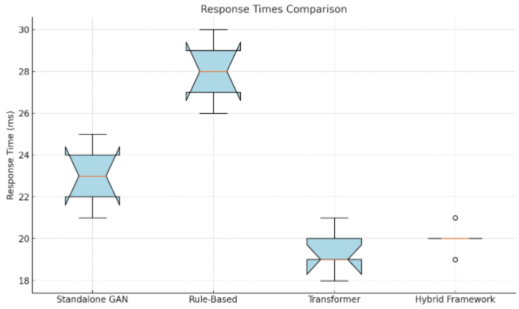

Fig.4. Response Time

The Fig.4 depicts the Box plot comparing response times. The hybrid framework maintains a balance between the speed of detection and accuracy, keeping the response real-time. The hybrid framework attains the maximum possible accuracy (96.4%), precision (93.6%), recall (91.3%), and F1-Score (92.4%) since it can adaptively detect emerging attack patterns with minimal false positives. With the addition of a decision fusion module, the system successfully decreases FPR to 3.1%, ensuring that most of the legitimate traffic is never misclassified. Although it is slightly slower than the threshold-based methods, it still achieves a response time of 20 ms, making it satisfy the requirements of real-time DDoS mitigation. The hybrid Generative AI-based framework outperforms traditional and machine learning models significantly for detecting and mitigating DDoS attacks. Its robustness against sophisticated attack vectors, with low false positive rates and real-time responsiveness, positions it as a state-of-the-art solution to modern cybersecurity challenges.

7. RESULTS AND DISCUSSION

This section presents the insights obtained from the experimental evaluations, the challenges faced during the implementation, and the implications of the proposed hybrid system for real-world applications and future research.

7.1 KEY FINDINGS

The hybrid framework achieved a detection accuracy of 96.4% in all experiments and outperformed the baseline models. The generative AI components, including GANs and autoencoders, were very effective in detecting anomalies that mimic unknown or evolving attack patterns. While maintaining high accuracy, the system achieved a response time of 20 ms, making it suitable for real-time DDoS detection and mitigation. The decision fusion module effectively streamlined the process by combining rule-based outputs and AI-generated insights. The integration of transformers allowed for effective sequential analysis of traffic, enhancing the system's capability to adapt to novel attack patterns. GANs added artificial attack scenarios to the dataset, making the system ready for rare or emerging threats. The false positive rate of 3.1% reflects the hybrid framework's capacity to differentiate between malicious traffic and legitimate anomalies, hence reducing unnecessary mitigations.

7.2 CHALLENGES

Training generative models such as GANs and transformers requires a lot of computational resources, especially during hyperparameter tuning. Despite optimizing response times, real-time deployment in resource-constrained environments might necessitate model pruning or quantization. Although synthetic data increased diversity, the reliance on public datasets such as CIC-DDoS2019 limits exposure to some real-world attack variations. Generating realistic synthetic traffic for advanced attack scenarios is challenging. The introduction of weighted scoring and logic-based decision trees introduced complexity, requiring extensive fine-tuning for optimal performance.

7.3 IMPLICATIONS

The hybrid framework is practical for organizations requiring robust, adaptive, and real-time DDoS defense mechanisms. Its low false positive rate ensures minimal interference with legitimate traffic, hence ideal for critical infrastructures like healthcare, finance, and government networks. Distributed systems advancements can make it scale better with edge computing and federated learning integration into the framework for large-scale networks. Future work may involve investigating lightweight models optimized for use on IoT and other devices of low power. A new application of Generative AI in DDoS defense shows its general scope of use in anomaly detection and adaptive threat mitigation.

8. CONCLUSION

The Hybrid Generative AI-based architecture represents a major leap forward in the next-generation DDoS defense approaches that integrate the benefits from Generative AI and rule-based systems. Contributions are along the lines of: A multi-layered architecture that utilizes GANs, autoencoders, and transformers for traffic anomaly detection. The decision fusion module is appropriately balanced between precision and recall, which leads to a lower false positive rate. Even better performance metrics are obtained using the framework, such as a detection accuracy of 96.4% and a response time of 20 ms, which makes the framework viable for real-world applications. In future, the deployment of federated learning approaches can further strengthen distributed detection capabilities, thereby maintaining data privacy and reducing dependence on centralized training. Also Research in pruning, quantization, and knowledge distillation can make this framework deployable on IoT and edge devices. Extending the application of this framework to other cybersecurity challenges, such as insider threat detection or ransomware mitigation, can add more value. This work lays the foundation for intelligent, adaptive, and real-time DDoS defense-a significant leap in the rapidly evolving landscape of cybersecurity.

REFERENCES

[1] M.A. Paracha, S.U. Jamil and A. Rasheed, "Leveraging AI for Network Threat Detection-A Conceptual Overview", *Electronics*, Vol. 13, No. 23, pp. 4611-4619, 2024.

[2] A. Hernandez Rivas and J.P. Sanchez Solis, "Towards Autonomous Cybersecurity: A Comparative Analysis of Agnostic and Hybrid AI Approaches for Advanced Persistent Threat Detection", *Proceedings of International Conference on Innovative Applications of Artificial Neural Networks to Data Analytics and Signal Processing*, pp. 181-219, 2024.

[3] M. Poongodi and M. Hamdi, "Intrusion Detection System using Distributed Multilevel Discriminator in GAN for IoT System", *Transactions on Emerging Telecommunications Technologies*, Vol. 34, No. 11, pp. 4815-4819, 2023.

[4] L. Coppolino and F. Uccello, "The Good, the Bad, and the Algorithm: The Impact of Generative AI on Cybersecurity", *Proceedings of International Conference on Innovative Applications of Artificial Neural Networks*, pp. 1-12, 2024.

[5] K.B. Adedeji, A.M. Abu-Mahfouz and A.M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges", *Journal of Sensor and Actuator Networks*, Vol. 12, No. 4, pp. 51-59, 2023.

[6] S. Kanthimathi, S. Venkatraman, K.S. Jayasankar and R. Jashwanth, "A Novel Self-Attention-Enabled Weighted Ensemble-Based Convolutional Neural Network Framework for Distributed Denial of Service Attack Classification", *IEEE Access*, Vol. 9, pp. 1-13, 2024.

[7] P. Turaka and S.K. Panigrahy, "Dynamic Attack Detection in IoT Networks: An Ensemble Learning Approach with Q-Learning and Explainable AI", *IEEE Access*, Vol. 9, pp. 1-14, 2024.

[8] A.A. Mintoo and I. Ahmad, "Adversarial Machine Learning In Network Security: A Systematic Review Of Threat Vectors And Defense Mechanisms", *Innovatech Engineering Journal*, Vol. 1, No. 1, pp. 80-98, 2024.

[9] K.P. Chandrasekaran, "Integrating Novel Mechanisms for Threat Detection in Enhanced Data Classification using Ant Colony Optimization with Recurrent Neural Network", *Journal of Cybersecurity & Information Management*, Vol. 14, No. 2, pp. 1-13, 2024.

[10] F. Zhao, H. Li, K. Niu and R. Song, "Application of Deep Learning-based Intrusion Detection System in Network Anomaly Traffic Detection", *Applied and Computational Engineering*, Vol. 86, No. 1, pp. 250-256, 2024.