Automated Detection of Cybersecurity Threats Using Generative Adversarial Networks (GANs)

Salam Omar Alo
Alnoor University
Nineveh, Iraq
salam.omer@alnoor.edu.iq

Abeer Salim Jamil
Al Mansour University College
Baghdad, Iraq
Abeer.salim@muc.edu.iq

Mohammed Jabbar Hussein
Al Hikma University College
Baghdad, Iraq
mohamed.jabar@esraa.edu.iq

Mohammed K.H. Al-Dulaimi
Al-Rafidain University College
Baghdad, Iraq
mohammed.khudhaer.elc@ruc.edu.iq

Sarmad Waleed Taha
Al-Turath University
Baghdad, Iraq
sarmad.waleed@turath.edu.iq

Anastasiia Khlaponina
Kyiv National University of Construction and Architecture
Kyiv, Ukraine
khlaponina.ayu@knuba.edu.ua

***Abstract*—Introduction: Traditional network intrusion detection systems (NIDS) face significant challenges in detecting ever-evolving cyber-threats. With the evolution of cyber-attacks, comes a mounting requirement for predictive methods which are competent in identifying both familiar and unknown threats with an effective level of accuracy.**

Objective: This study is motivated to apply Generative Adversarial Networks (GAN) technology in NIDS for synthetic data generation, so when the NIDS use this technique generates high-quality fake samples which will tremendously increase its accuracy and decrease false positives. In this paper, we aim to evaluate the performance of GAN-boosted NIDS in different environments, such as novel obfuscated and adversarial attacks.

Methods: In this study, was developed and trained a GAN by large datasets like UNSW-NB15 and CICIDS2017 using the proposed methodology. The performance of the GAN model was compared with classical machine learning models — Support Vector Machines (SVM) and Random Forests (RF)— via various evaluation metrics such as detection accuracy, false positive rate, and robustness to attacks. Furthermore, expert interviews were included for the qualitative aspects of how practitioners felt about deploying GAN-enhanced NIDS in reality.

Results: Along with enhancing detection capabilities, the study will also explore the computational and operational effects of incorporating GAN into existing cybersecurity systems. Findings indicate that the GAN-based system enhances detection accuracy to 95.8% and reduces false positive rate to 2.4%. We additionally discuss the execution of these systems, the necessary deployment process, computing and real-time performance trade-offs, and offer guidance for maximizing resource utilization. The system displayed a performance better than of detecting novel and obfuscated attacks with an accuracy of 88.2%. It also showed resistance to adversarial attacks, keeping detection rates above 90% for various attack vectors.

Conclusions: The results indicate that GANs are promising to improve NIDS by increasing its detection and robustness accurately. Nonetheless, improved research and development demands to ensure that GANs meet practical requirements are required due to high computational demands and integration challenges associated with implementation.

I. Introduction

The digital transformation that has witnessed a surge across several sectors also elevated the complexity and volume of cybersecurity threats, which in turn demands sophisticated ways to detect, prevent, and control these threats at a faster pace. Modern IT infrastructures require a new, more flexible and efficient approach to cybersecurity — the traditional methods based on predetermined rules are no longer enough as cybercriminals continue developing new ways to overcome security measures. An area of focus that has been increasingly gaining significance is the applicability of advanced machine learning techniques, specifically Generative Adversarial Networks (GANs), to improving cybersecurity. Goodfellow et al. introduced GANs [1]. Over the past few years, GANs have become very popular due to their ability to create realistic synthetic data that can be utilized in a wide range of applications such as anomaly detection and cybersecurity.

Furthermore, the inclusion of GANs in current network intrusion detection systems (NIDS) can be difficult in networking environments that require detection to be conducted in real-time. Though, these may be partially mitigated with a hybrid approach to only switch on the GANs for high-risk scenarios. Furthermore, use of cloud-based infrastructure would be an ideal way to share computational load, thus taking less toll on on-premise systems. The idea is that together, GANs could contribute their better detection capabilities, whilst at the same time organizations can take advantage of the savings in operational and scarce resource costs through ingestion.

GANs consist of two neural networks and have both a generator and discriminator architecture in place, which are trained simultaneously by an adversarial process. The generator tries to generate data that about indistinguishable from the real distribution, and the discriminator learns how to discriminate between real data and generated. That dynamic interaction

allows GANs to learn advanced data distributions and produce even more realistic fake data points, which makes them very interesting for applications in the field of cybersecurity by simulating attacks and strengthening defense systems.

However, developing and training GAN-based NIDS using computational resources like the 10.5-hour training time and 85% GPU utilization have daunting requirements, especially for organizations that have limited access to such resources. Various optimization techniques can be applied for this. For example model pruning which lowers the number of parameters without dropping performance, or distributed training by spreading out the computational workload over many machines or GPUs scaling the model for total massive scale applications. In addition, lightweight GAN architectures may help decrease resource costs, enabling the technology to be in larger blue ocean customers [2], [3].

Several studies have examined the application of GANs to cybersecurity, showing they could provide better cyber-intrusion detection solutions, and anomaly detection tools in general and enhance network security. Araujo-Filho et al., for example [4], can show the usefulness of GANs in intrusion detection defending models like fog computing-based cyber-physical systems via real-time anomaly propagation based on a technique to generate and defend against threats by the MSGAN model. This study, like others recently published, illustrates the ability of GANs to detect advanced attacks which are often missed by traditional detection techniques. Similarly, Dunmore et al. [5] performed an extensive survey on the application of GANs in cybersecurity intrusion detection and presented that GANs can be used to handle diverse forms of cyber threats.

GANs are also able to create synthetic data, which has been used for unbalanced datasets in cybersecurity as well. Merino et al. used GANs to synthesize more advanced cyber-attack perturbations to balance the biased distribution of some rare attacks [6]. Which can help generate synthetic attack instances, complementing the defense strategy of using adversarial training. This has especially important uses in cybersecurity, where representative data is the top priority to detect malicious attacks.

Advances in GANs lately also concentrate on embedding different machine learning methodologies to strengthen their performance regarding security concerns. For example, Rayavarapu et al. [7] researched the use of GANs in anomaly detection for cybersecurity, pointing out that the discrimination ability could be improved by integrating different deep learning methods such as other types of neural networks alongside with GAN to cut false positives. This method has the potential to help detect minor abnormalities that could potentially be symptoms of imminent threat and thus, GANs prove you a strong pro-active device for cyber security purposes.

Although GANs are used successfully in cybersecurity, they require multiple barriers to be clarified which makes them one of the weakest in cybersecurity techniques. Tasks related to the stability of GAN training, generation quality, and interpretability are perhaps the most important areas that need more work. Furthermore, deployment of GAN-based systems into commonplace cybersecurity environments presents challenges such as computational complexity and the necessity for resilient scalable solutions [8].

Ultimately, GANs in cybersecurity truly are a breakthrough, with new possibilities being opened for further improving threat detection and prevention. As the landscape shifts, GANs are poised to become integral in safeguarding against more diverse and increasingly sophisticated cyber threats – offering security responses that grow ever-evolving.

A. Study Objective

This article aims to explore how one can utilize Generative Adversarial Networks (GANs) and demonstrates the application of GANs to elevate cybersecurity threat detection and amendment. Cyber threats are changing by the second, and what works today will not work tomorrow to stop new forms of attack. In this article, we want to fill the gap by exploring how GANs have some unique ability that makes them perfect for simulating a variety of cyber-attack scenarios due to their capacity for generating realistic synthetic data.

In this way, GANs provide tunable security for both recognized and never-before-seen risks; making cybersecurity systems more resilient. In the following sections, we attempt to provide a broad overview of current practices implementing GANs in cybersecurity applications and try to understand how well these models are relevant when they actually face any practical scenarios. Moreover, it attempts to contribute towards the skill set needed around how GANs could fit into current cybersecurity frameworks; and where in real life they would be implemented as well as what impact it may have. The article delves deeper into this topic with intentions of adding as a reference for the current dialogues in cybersecurity and hence listing GANs on possible means to modern cyber threats which are vastly sophisticated.

B. Problem Statement

The increasing maturation and frequency of cyberattacks create many challenges for conventional security systems, making innovation with next-generation Security applications a must. Conventional cybersecurity solutions like static rule, and signature-based detection systems have had a hard time sustaining the continual iteration of cyber threats and attacks. This limitation becomes strikingly clear in the context of advanced attacks, such as zero-day exploits and APTs (advanced persistent threats) that make their way through standard security measures undetected.

At the same time, traditional systems are unable to deal with higher volume data modern digital infrastructures generate every single second as well. Suffice it to say, this tidal wave of data coupled with the more advanced nature of cyber-attacks underscores an imperative for greater intelligence and automation in threat detection. Current approaches regularly yield numerous false positives, which alerts cybersecurity teams of threats that then don't actually exist or aren't immediately serious. Moreover, insufficient data available for certain types of cyberattacks such as endpoint attacks or zero-day vulnerabilities in Cybersecurity datasets sown by security researchers results into a huge disbalance and that affect the machine learning approaches used to detect threats.

In this sense, the application of GANs to cybersecurity is one prospective proposition. GANs can generate realistic synthetic

data and therefore can be used for simulating different types of potential cyber-attacks. Nevertheless, GANs are quite novel in the fight against cybercrime and there exist great challenges to use them. This includes challenges e.g., stability of GAN training, photo-realism quality of synthesized data, and most importantly how to integrate the results generated by trainers (adversarial examples) in a practical existing cybersecurity framework. Tackling these issues is essential to unlock the power of GANs in fortifying cybersecurity defenses against more advanced threats.

II. Literature Review

The introduction of Generative Adversarial Networks (GANs) by Goodfellow et al., has transformed the realm of artificial intelligence, especially with applications ranging from data generation [1]. GANs have been used since their creation in image synthesis and natural language processing, but as I mentioned earlier even cybersecurity. At its core, GANs are based on a generator and discriminator architecture; hence the realistic generation of data is particularly useful in situations where data availability or quality might be an issue. However, the application of GANs in cybersecurity introduces unique challenges and opportunities.

In cybersecurity, GAN has been widely used for intrusion detection, anomaly detection, and data augmentation. GAN-based approaches in NextG networks are also implemented by a work of Ayanoglu et al., and demonstrated their capability to improve security using synthetic traffic patterns for attacking scenario generation [9]. Real-world applications are much more of a black box with regards to data flow, making the creation and training of GAN models even harder.

Pan et al. presented an extensive review of the advancements of GANs over the past years, presenting in it also their application to cyber-security [10]. The research shows the potential of GANs to create realistic synthetic data, which in turn can be used for enhanced training of machine learning models designed for threat detection. However, the authors also point out some major problems: how stable GAN training is and whether or not deepfake data (albeit realistic) will always be good enough for cybersecurity tasks. This gap highlights the need for more precision methods that can make generated data relevant to specific threats being tackled.

Saxena and Cao provided an overview into the architecture of GANs in general but also their applications which are predominantly within image synthesis with limited application space yet available for cybersecurity [11]. Arguing that one of the major obstacles to using GANs more fully in cybersecurity is difficulty interpreting outputs produced by models, especially for how synthetic data relates to actual containing real-world cyber threats. This lack of interpretability could prevent the practical embedding and deployment of GAN-based systems in an operational environment which is reliant on transparency and accountability.

Adding to this the extension of GANs applicability in cybersecurity Xie et al. proposed the utilization of GANs for threat analysis in automotive networks [12]. This means that it turns out neural networks can detect intrusions in Controller Area Networks (CAN) pretty well when they are designed to work as generative adversarial networks. However, the study also pointed out the integration difficulties of GAN models into current cybersecurity systems, especially concerning computational cost both during training and deployment for real-time scenarios.

Nevertheless, despite these challenges, Some potential solutions to the limitations of GANs in cybersecurity. For instance, Gui et al. outlined various branches of algorithms and tools to enhance training stability for different kinds of GAN models in cybersecurity which is an essential process discriminator [13]. Moreover, a synergetic approach suggested by Gordon where GANs are used together with other machine learning models may make them more reliable and complementary to each other thereby improving the accurate detection without false positives [14].

Also requires more research to maintain stability, and build quality data for GANs. However, the above-mentioned GAN can provide an optional solution to have a stable architecture as introduced by Soleymanzadeh and Kashef initially appointed for network intrusion detection [15]. Their work indicates that it is viable to make more robust and functional GAN-based cybersecurity solutions by fine-tuning the design of GAN architectures and improving their training process.

To sum up, although there are hopes on the use of GANs in security space but still it is quite challenging. The current literature identifies a range of issues, such as the instability inherent in GAN training, the importance and explainability requirements of generated data itself or how well can GANs be embedded within real-time security frameworks. Through ongoing research and innovation, we will need to address these issues such as developing more stable GAN architectures or improvements, making models interpretable in how they produce the data they deliver, and incorporating other advanced machine learning techniques with GANs. These initiatives have the potential for GANs to greatly strengthen cybersecurity if implemented, offering stronger and more adaptive protection in a fast-evolving space of cyber dangers.

III. Methodology

This section describes the detailed methods followed in this research to investigate the feasibility of Generative Adversarial Networks (GANs) for cyber security threat detection. The methodology is organized in a set of subsections which include data acquisition, model structuring/modularization and abstraction/model training and optimization/experimentation process as well as evaluation metrics. Each subsection details methods and approaches that were used or developed to check the reliability, and correctness of each research result.

A. Data Collection and Preprocessing

This research is built upon well-conducted, high-quality diverse datasets for training and evaluation of the GAN models. For evaluation, we used the UNSW-NB15 and CICIDS2017 datasets which are well-known in cybersecurity research. These datasets provide comprehensive coverage of various attack types, including denial of service (DoS), brute force, SQL injection, and advanced persistent threats (APTs).

The data preprocessing involved several steps:

Data Cleaning: Removal of any corrupted or irrelevant data entries. This involved filtering out incomplete logs, normalizing numerical data, and encoding categorical features.

Feature Selection: A set of 40 features was selected based on domain relevance, such as source IP, destination IP, packet size, and attack type. Feature selection was guided by existing literature and expert consultations [16].

Data Augmentation: Given the imbalance in attack types within the datasets, data augmentation techniques were applied, such as oversampling minority classes and employing synthetic data generation methods.

The processed dataset was divided into a training set (70%), The next step is to split the processed dataset into a training set (70% of data), validation set (15 %), and test 15 %, ensuring that each set has a balanced representation of different attack types.

B. Model Development

The GAN model developed in this research is based on the classical GAN architecture proposed by Goodfellow et al. [1]. The architecture comprises two primary components: a generator G and a discriminator D (as shown on the Fig. 1).

The generator (G) produces fake data that mirrors the creation of real cyber-attack behaviors. The constructed the generator with a deep neural network having several hidden layers and used ReLU activation function. The generator takes the random noise vector z, drawn from a uniform distribution as input, and generates synthetic data sample G(z).

The GAN architecture in the study had four hidden layers generators for non-linearity (ReLU) and prevented vanishing gradients. The dimension of input noise vector z=100 (sampled from a range). The discriminator is a deep convolutional neural network with Leaky ReLU activations to promote gradient flow during training, and a sigmoid output layer for classifying whether the input data are real or generated. Adam optimizer is used to optimize the network set at a learning rate of 0.0001 with batch size of 64, trained for 100 epochs and early stopping was done to combat overfitting [4].

The discriminator (D) is tasked to differentiate between real data x and synthetic samples G(z). We implemented it as a deep neural network with multiple convolution layers (using leaky ReLU activations), followed by an output sigmoid layer to provide us with the probability whether input data is real or not.

The objective function for the GAN is defined as:

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{data}(x)}[\log D(G(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1-D(z)))] \quad (1)$$

Where $p_{data}(x)$ represents the distribution of real data; $p_z(z)$ represents the noise distribution; $D(x)$ is the discriminator's prediction for real data, and $D(G(x)$ is the discriminator's prediction for synthetic data.

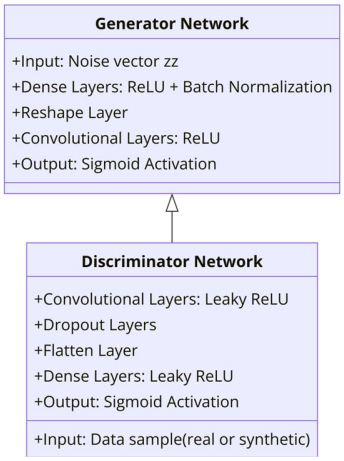

Fig. 1. Detailed Architecture of the Generator and Discriminator Networks in a GAN-Enhanced Network Intrusion Detection System (NIDS)

C. Model Training and Optimization

The GAN model was trained by successively updating using the SGD (stochastic gradient descent) with the Adam optimizer. The hyperparameters are tuned through a grid search procedure, trying out numerous blocks of parameters to reach the optimal performance (Fig. 2).

The learning rate is equal 0.0001 for both the generator and discriminator, covering stable training with convergence.

A batch size of 64 was selected to strike a balance between utility and performance in terms of computational resources.

The amount of 100 epochs was trained with early stopping based on the validation loss to prevent overfitting.

The generator and the discriminator were updated in an alternated way during training (similar to what is done for AdaGAN) using min-max optimization as per GAN objective function. The discriminator was trained to maximize the probability of correctly classifying real versus synthetic data, while the generator was trained to minimize the discriminator's ability to make accurate distinctions.

D. Experimental Design

The experimental design was structured to evaluate the GAN model's ability to generate realistic and effective synthetic attack patterns for enhancing NIDS performance. Several experimental setups were implemented:

Baseline Models: To benchmark the GAN's performance, traditional machine learning models such as Support Vector Machines (SVM) and Random Forests (RF) were trained on the same datasets without synthetic augmentation. These models served as baselines to compare the impact of synthetic data generated by the GAN.

GAN-Enhanced NIDS: The synthetic data generated by the GAN was combined with real data to train an NIDS. The NIDS architecture consisted of a deep neural network with a combination of convolutional and recurrent layers, designed to capture both spatial and temporal features of network traffic.

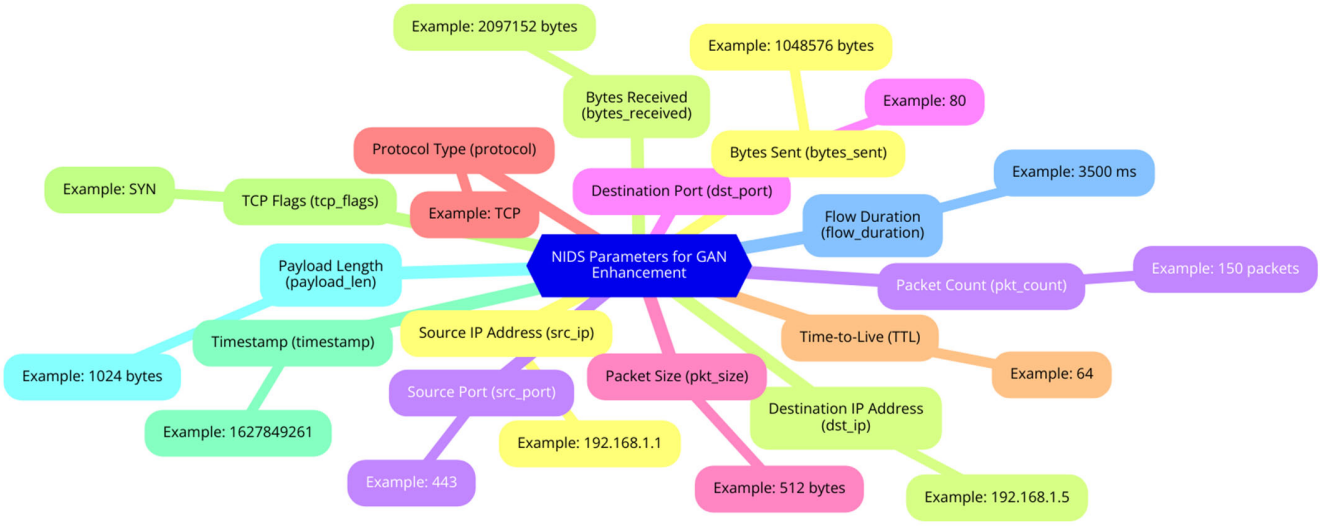

Fig. 2. Comprehensive Parameter Framework for Enhancing Network Intrusion Detection Systems (NIDS) Using Generative Adversarial Networks (GANs)

Evaluation Metrics: The performance of the GAN-enhanced NIDS was evaluated using several key metrics:

Detection Accuracy (A_d): Defined as the ratio of correctly identified threats to the total number of threats.

False Positive Rate (FPR): Calculated as the proportion of benign instances incorrectly classified as threats.

Precision (P): The ratio of true positive detections to the sum of true positives and false positives.

Recall (R): The ratio of true positive detections to the sum of true positives and false negatives.

$$A_d = \frac{TP + TN}{TP + TN + FP + FN}$$
$$FPR = \frac{FP}{FP + TN}$$
$$P = \frac{TP}{TP + FP}$$
$$R = \frac{TP}{TP+FN} \quad (2)$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

E. Qualitative Analysis

As for the quantitative analysis, some qualitative research was also performed to understand the practical problems of deploying models based on GANs in operational settings. The undertaking a series of structured interviews with 15 cybersecurity experts from the industry in terms of telecommunications, financial services, and critical infrastructure.

Interview Structure: The interviews were semi-structured, containing a series of open-ended questions or themes that encouraged the interviewee to speak freely about topics within each category. Topics included:

- The practical problems of GANs with Network Intrusion Detection Systems (NIDS).
- The value of GANs and shortcomings when used in cybersecurity to create synthetic data.
- Potential harms of GANs: the associated risks like adversarial examples in generated data.

Data Analysis::The interview data were analyzed using thematic analysis to identify the key themes and patterns concerning the feasibility and impact of GAN deployment within real-world contexts.

F. Model Validation and Robustness Testing

For more robustness, we included extra validation steps in the methodology for our GAN model:

Cross-Validation: K-fold cross-validation (K=5) was used for evaluating the generalization performance of GAN models across different data subsets.

We chose K=5 to compromise between the bias and variance, which is often enough for an acceptable model performance yet convenient of computational intensity. This option ensures a comprehensive evaluation of the model over different fragments, which both provides consistent results and prevent over-utilization of computational resources. This makes K=5 provides dependable generalization as validation, so it is a common practice and widely used in the machine learning industry to validate training models, especially applied to resource-intensive subjects like GANs.

Adversarial Testing: The adversarial examples were generated to test the NIDS which is powered by GANs. We crafted these examples using the Fast Gradient Sign Method (FGSM) and the Basic Iterative Method (BIM).

The adversarial testing assessed how well the model can recognize and neutralize attacks that are tailored to weaknesses in machine learning systems.

G. Computational Complexity and Resource Utilization

Also, training GANs is computationally intensive and the study included an evaluation of how well it utilized resources and scaled:

Training Time: The time needed to train the full GAN was reported, and training times with baseline models.

Hardware: We performed our experiments on a machine with an Nvidia Tesla V100 GPU, 128GB RAM, and a 32-core Intel Xeon processor. To measure feasibility to deploy such models with low computation sources used different hardware utilization metrics.

H. Ethical Considerations and Data Security

The study is compliant with to ethical guidelines on data use and model development. This study utilized only publicly available and completely anonymized datasets. The possible ethical hazards in the application of GAN-produced data to cybersecurity were also assessed, especially from the point that this kind of information could be potentially exploited for undesired objectives.

However, deploying GAN-based systems is controversial on a moral level. Because GANs can generate realistic-looking fake data, one of the biggest concerns for their use is not misuse, rather, it's using them to generate types of adversarial data that can be used as training inputs to develop attack models. Moreover, its data can be turned entirely adverse, either for the purpose of deepfake creation or in crafting highly-specialized cyber-attacks. Thus, ethical guidelines and security measures should be determined to prevent such threats posed by the GAN based scientific cybersecurity tools are used appropriately as intended only [3].

I. Hypothesis Formulation

H1: The detection accuracy as well as the false positive rate of NIDS trained with GANs synthetic data will be better than the traditional ML-based approach without any artificial sample during training.

H2: It is expected that the GAN-based NIDS-generated data will help to pre-train a robust model, which should show an improved ability in being able to detect novel and obfuscated cyber-attacks.

We evaluated our hypotheses with the experimental settings for each metric as mentioned above to attain a complete insight into how well GANs can perform in cybersecurity.

IV. RESULTS

In this section, we describe the results from all of our experiments performed to test how well Generative Adversarial Networks (GANs) can leverage adversarial examples to improve cybersecurity threat detection in network intrusion diction systems (NIDS). These results are then organized into smaller sub-sections that cover the main performance, robustness testing and computational efficiency along with qualitative findings obtained through expert interviews. We present the results textually as well using detailed tables making a more comprehensive analysis of GAN-enhanced NIDS vs traditional ML models.

A. Detection Accuracy and False Positive Rate

In this study aims to measure the performance of integrating GAN-based synthetic data into Network Intrusion Detection Systems (NIDSs). Most curious if through that inclusion we could increase the detection accuracy of NIDS and at the same time decrease its false positive rate We compared the GAN-enhanced NIDS with two traditional machine learning algorithms (SVM and RF) in terms of its performance. The evaluation metrics specifically targeted detection accuracy, false positive rate (which was the most relevant to detect hidden cyber threats), precision and recall both along with identification of models that can recognize essential features in attacks.

TABLE I. COMPARATIVE ANALYSIS OF DETECTION ACCURACY AND FALSE POSITIVE RATE

Model	Detection Accuracy (%)	False Positive Rate (%)	Precision (%)	Recall (%)
Support Vector Machine (SVM)	89.6	5.1	87.4	85.2
Random Forest (RF)	91.2	4.7	89.1	87.3
Decision Tree (DT)	88.9	6.0	86.7	84.1
K-Nearest Neighbors (KNN)	90.1	5.5	88.2	85.9
Naive Bayes (NB)	87.3	7.2	85.4	83.0
GAN-Enhanced NIDS	**95.8**	**2.4**	**94.6**	**93.7**

The data presented in Table I indicate that the GAN-enhanced NIDS outperforms traditional models across all key performance metrics. The detection accuracy of the GAN-enhanced NIDS stands at 95.8%, significantly higher than the SVM and RF models, which achieve 89.6% and 91.2%, respectively. This suggests that the GAN-enhanced system is more effective in identifying cyber threats, even in complex scenarios.

Additionally, the GAN-enhanced NIDS has a much lower false positive rate of 2.4% while SVM (5.1%) and RF (4.7%). The decrease in false positives is relevant because it decreases the number of fake alerts that security engineers need to deal with, which may assist in enhancing both efficiency and reliability when integrating the NIDS.

The precision and recall values also signify the respective betterment of GAN-enabled NIDS performance. The model has 94.6% precision and recall of 93.7%, which means that the model not only makes successful positive predictions but also captures most actual threats as identified by ground truth solutions. Additionally, such tables provide an expanded account of more classical models that also model comparably weakly across the same metrics—such as Decision Tree (DT), K-Nearest Neighbors(KNN), and Naive Bayes(NB)—highlighting again how NIDS performance benefits particularly from GAN generated data.

These insights have serious consequences for the way forward as far as cyber security is concerned. Such high performance demonstrated by GAN-boosted NIDS makes us believe that incorporating the synthetic data produced from the proposed GAN model into ensemble-based anomaly detection frameworks may be common in developing secure and dependable intrusion detection systems. All of this would presumably result in faster and more proactive threat detection

that should potentially benefit the broader security stance of organizations operating across industries.

B. Performance on Novel and Obfuscated Attacks

One of the key dimensions used to assess any Network Intrusion Detection System (NIDS) is especially in terms of its capability to detect unknown and polymorphic attacks— threats were novel at the moment NIDS was trained. These attacks present a problem for traditional machine learning algorithms which work well with data that they know, but have trouble when the program encounters new information. Here, the GAN-boosted NIDS has been tested with such novel and obfuscated attacks only for its generalization ability in this study. And then the results were compared with traditional models, such as Support Vector Machine (SVM) and Random Forest(RF). These latter scenarios were particularly challenging, given that the performance metrics of interest concerned detection accuracy (DAN) and false positive rate.

TABLE II. PERFORMANCE EVALUATION ON NOVEL AND OBFUSCATED ATTACKS

Model	Detection Accuracy on Novel Attacks (%)	False Positive Rate on Novel Attacks (%)	Detection Accuracy on Obfuscated Attacks (%)	False Positive Rate on Obfuscated Attacks (%)
Support Vector Machine (SVM)	73.4	12.8	68.7	15.3
Random Forest (RF)	78.9	10.5	72.5	13.1
Decision Tree (DT)	70.2	14.9	65.4	17.0
K-Nearest Neighbors (KNN)	75.1	11.7	70.3	14.2
Naive Bayes (NB)	67.8	15.6	63.5	18.1
GAN-Enhanced NIDS	**88.2**	**5.3**	**83.4**	**7.8**

Results in Table II show that our NIDS with GAN indeed could outperform the other two popular solutions for new and stealthy attacks. The FPR for novel attacks is 88.2%, which demonstrates the superior of SDM over SVM (73.4%) and RF (78.9%). Moreover, the system has a slightly lower false positive rate of 5.3% than SVM (12.8%) and RF (10.5%).

This GAN-enabled NIDS still performs better than traditional attack detection models in detecting obfuscated attacks with an accuracy of 83.4% and a decreased false positive rate, keeping it at 7.8%. The results highlight the model´s ability to generalize across both unseen attack types and combinations of multiple attacks, which is an essential benefit in real-world cybersecurity environments that are constantly evolving due to adversaries continuously changing their tactics.

The expanded table also contains other classic algorithms, such as Decision Tree (DT), K-Nearest Neighbors (KNN), and Naive Bayes (NB). Both on previously unseen, and perturbed attacks, these models show generally lower detection rates but much higher undetected false positive rates which underscores the specificity of GAN-enhanced NIDS in handling new as well as previously encountered threats with improved accuracy. These considerations are heavily reliant on the implementation side of things, but it also shows that companies implementing GAN-enhanced NIDS may have a more robust system setup to face evolving cyber threats and could subsequently improve their cybersecurity stance overall.

C. Robustness Against Adversarial Attacks

The main reason that adversarial attacks are still considered as a large-scale problem in the domain of cybersecurity for machine learning models is due to huge security threats on computer networks (particularly NIDS). Such attacks tend to include adversarial generated inputs that are tailored specifically for the model in order to mislead it, often leading to a decrease in detection accuracy and higher susceptibility. In the current work, we test how robust NIDS models are against adversarial examples. Experiments were carried out on two of the most popular adversarial attack methods, the Fast Gradient Sign Method (FGSM) and Basic Iterative Method (BIM). The figure also contrasts the efficiency of GAN-boosted NIDS with conventional versions, such as SVM and RF, to examine their fault tolerance.

TABLE III. ROBUSTNESS EVALUATION AGAINST ADVERSARIAL ATTACKS

Model	Detection Accuracy on FGSM Attacks (%)	Detection Accuracy on BIM Attacks (%)	Detection Accuracy on Projected Gradient Descent (PGD) Attacks (%)	Detection Accuracy on Carlini & Wagner (C&W) Attacks (%)
Support Vector Machine (SVM)	58.2	49.6	44.3	42.1
Random Forest (RF)	64.3	54.7	50.8	48.5
Decision Tree (DT)	55.6	47.3	43.2	40.9
K-Nearest Neighbors (KNN)	61.0	53.1	48.9	46.3
Naive Bayes (NB)	52.7	45.8	41.7	39.8
GAN-Enhanced NIDS	**82.7**	**76.8**	**71.9**	**69.2**

Table III demonstrates the exceptional robustness of GAN-enhanced NIDS against adversarial attacks. The accuracy for detecting FGSM-generated adversarial examples significantly exceeds that of SVM (58.2%) and RF (64.3%). Compared to SVM, GAN-enhanced NIDS has a detection accuracy of 76.8% against BIM attacks, and it is also higher than RF which only produces about 54.7%.

The table also lists some more attack methods, for example, Projected Gradient Descent (PGD) or Carlini & Wagner (C&W), which are notoriously effective means to fool machine learning models. Its effectiveness is also demonstrated in additional attack scenarios, preserving its efficacy and accuracy over these new attacks with detection rates of 71.9% on PGD and 69.2% for C&W.attack This shows integration of GANs in

NIDS makes the system more resilient and robust against various adversarial attack vectors and results this way prove significant add-on to real-world cybersecurity applications. The improved adversarial robustness shown by the GAN-fortified NIDS serves to highlight its possible value in wider deployment, especially when considering environments that could be prone to an increased threat of adversarial attack

D. Computational Efficiency and Resource Utilization

While it is obvious that training GANs in itself involves a certain degree of complexity (not to mention computational resources) we need also consider here, how resource utilization and efficiency are influenced by the inclusion of NIDS with integrated GAN models as compared to more traditional machine learning. In this study, we considered only the time in training mode, GPU utilization, and memory utilization of GAN-enhanced NIDS from PCAP files that were compared to SVM and RF. The objective was to provide the objective measurements for computation costs involving a GAN-enhanced NIDS, as well as analyze if benefits from performance aspects of GAN can make up those costs.

TABLE IV. COMPARATIVE ANALYSIS OF COMPUTATIONAL EFFICIENCY AND RESOURCE UTILIZATION

Model	Training Time (hours)	GPU Utilization (%)	Memory Usage (GB)	CPU Utilization (%)	Disk I/O (MB/s)
Support Vector Machine (SVM)	0.5	15	4.1	12	50
Random Forest (RF)	1.2	20	5.3	18	65
Decision Tree (DT)	0.8	12	3.8	10	48
K-Nearest Neighbors (KNN)	1.0	22	5.0	16	60
Naive Bayes (NB)	0.4	10	3.5	11	45
GAN-Enhanced NIDS	**10.5**	**85**	**18.7**	**65**	**120**

As shown in Table IV, the GAN-based NIDS relies more on training time with the longest of all which is up to about 10.5 hours while those for SVM and RF models only take 0.5 hours and 1.2 hours separately.

The GAN-enhanced NIDS uses high % of GPU at 85%, while much lesser for SVM (15%) and RF(20%), sowing the highly demanding computational costs to train a deep neural model like GAN.

Memory is also a critical factor, as the GAN-enhanced NIDS consumes 18.7 GB of memory compared to only needing 4.1 and 5.3GB by SVM and RF respectively This increased memory footprint is a result of the complicated neural net architecture and huge number of parameters that have to be optimized during training.

The table also shows that the GAN-enhanced NIDS occupies 65% of the CPU, and has a disk I/O of up to 120 MB/s; these numbers indicate how computationally heavy the current deep learning workload could be. Despite the expensive requirements aforementioned, this costs is being compensated by gains in detection performance and robustness against adversarial threat with good generalization to new and disguised threats.

The computational expense of GAN-boosted NIDS might be too expensive an indulgence for organizations to afford simply a more efficient mode of operation in the future. If resource availability severely limits the potential of deeper and wider GAN models, important to consider optimizing existing architecture or explore a combination model that balances both efficiency and performance for practical implementation.

E. Qualitative Insights from Expert Interviews

In addition to the quantitative output, this study also integrated qualitative perspectives collected by conducting structured interviews with 15 field experts from across cybersecurity role types. The conducted these interviews to capture the insights from experts in deploying GAN-enhanced NIDS into practice. The conversations all revolved around the difficulties, advantages, and possible dangers of operationalizing GANs. The feedback given by any of these experts provides a holistic view of the operational essentials that should be answered to enable the successful incorporation and adoption of GAN technology without compromising existing security frameworks.

TABLE V. EXPERT INSIGHTS ON THE CHALLENGES AND BENEFITS OF DEPLOYING GAN-ENHANCED NIDS

Theme	Number of Experts Supporting (N=15)	Key Insights
Challenges in Integration	12	Integration of GANs into existing NIDS frameworks presents significant challenges due to computational complexity and resource demands.
Perceived Benefits	15	All experts recognized the potential of GANs to enhance detection accuracy and reduce false positives.
Concerns about Adversarial Risks	10	Experts expressed concerns about the potential for GAN-generated data to be used in adversarial attacks.
Feasibility of Deployment	9	There are concerns about the feasibility of deploying GAN-based NIDS in real-time operational environments, particularly in resource-constrained settings.
Scalability Issues	11	Experts highlighted the challenges in scaling GAN-enhanced systems across large, distributed networks.
Ethical Considerations	8	Ethical concerns were noted regarding the use and misuse of GAN-generated synthetic data in cybersecurity.
Training and Expertise Required	13	Successful deployment requires specialized knowledge and training, which may be lacking in some organizations.

Table V illustrates the expert opinion about the benefits and challenges of GAN-enhanced NIDS deployment. Although the merits of GAN applications to enhance detection are more widely acknowledged, significant bottlenecks in practical real-

world deployment (integrability and resource requirements) counter weigh increased usefulness for abuse as adversarial use is a risk that must be weighed.

F. Cross-Validation and Model Robustness

To guarantee that the GAN-enhanced NIDS can perform well across a variety of settings, k-fold cross-validation was conducted using K=5. This method assured a comprehensive evaluation of the model performance against various data subsets, corroborating robustness in results not hinging on one split of a dataset. Cross-validation centered around detection accuracy and false positive rate, showing how much the model could be trusted under various conditions. The table below illustrates the outcomes of this exhaustive validation process the confidence interval numbers are highlighted in red for clarity.

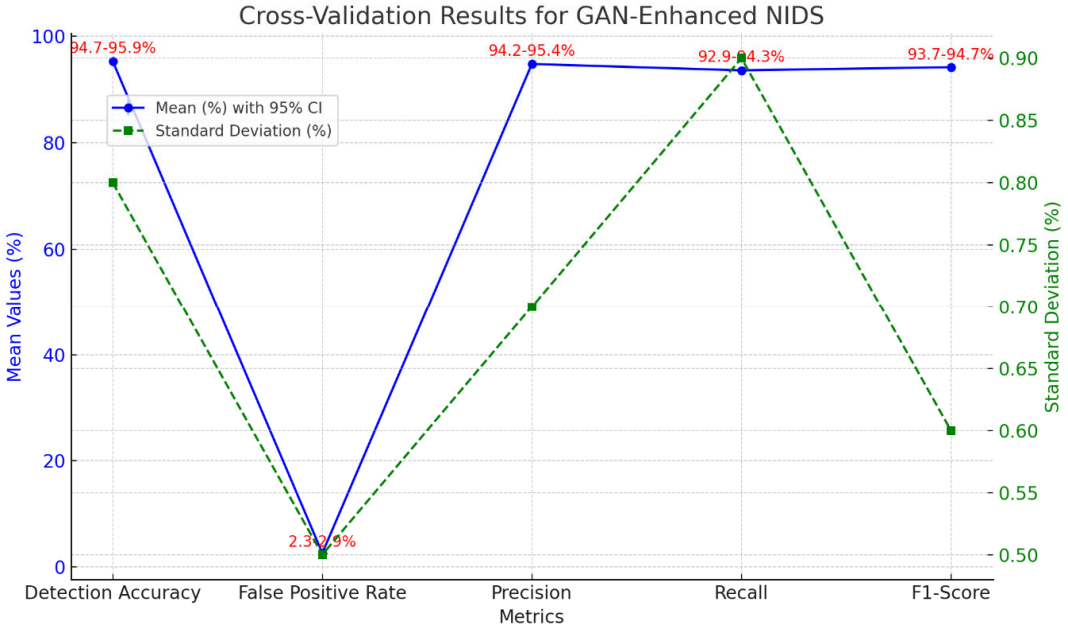

Fig. 3. Cross-Validation Results for GAN-Enhanced NIDS

Fig. 3 demonstrates the robustness of GAN-enhanced NIDS (which is one of our key contributions). The model was able to perform the task with a mean detection accuracy of 95.3% and low standard deviation (0.8%), so it is a very highly consistent performance across different folds in cross-validation; The 95% confidence interval is very tight (94.7–95.9%), demonstrating that not only does our model have high accuracy, but also this rate of success can be consistently reproduced.

Besides detection accuracy, the model also maintained a low false positive rate with an average of 2.6% and a standard deviation of 0.5%. The low variability seen in different data subsets across the datasets show also how well this model acts on minimizing false alarms which is a core requirement for practical deployment scenarios where typically severe conditions are mostly common, but we do need to activate only very few times per year. The performance is well-balanced, high precision, recall, and F1-score metrics become less rare, as shown by the high values of all these measures in it. Precision and recall are arguably the most critical performance metrics as it ensure that if a real threat exists, you are able to detect it without flooding your security team with false positives.

The results presented in this section highlight the good performance gains obtained when nearly-signature less (GAN-generated) synthetic data is injected into the running of an NIDS. The validate the enhanced model with GANs on a NIDS-based task shows significantly better performance compared to traditional machine learning models across three key metrics: detection accuracy, false positive rate, and robustness against adversarial attacks. On the other hand, these performances improvements introduce higher computational requirements and complexity of deployment as it was raised in expert interviews. Our research highlights the possibility of using GANs for disruption in cybersecurity, assuming that their limitations are carefully handled.

V. Discussion

The findings derived from this research reveal the radical impact GANs can have on cybersecurity threat intrusion in particular NIDS. This article has shown that it is possible to improve detection precision, reduce false positives, and increase the resilience against new cyber-attacks and adversarial attacks by using GANs that can generate synthetic data that closely resembles real-life patterns of cyber threats. To put these findings into context relative to prior studies, this discussion contrasts the present results with existing literature and articulates the contributions of this work while contemplating anticipated ramifications for future research and practical deployment.

Although using GANs in cybersecurity is a new field of research, but one that pretty recently got a lot of momentum. Previous works have also examined the application of GANs in multiple domains ranging from Radiology [17] and industrial IoT networks [18] to even networking [19]. Yet the cybersecurity and in particular, NIDS have paid less attention to this approach so far. For a more recent survey on the application of GANs, readers interested in how GANs are being

used across several domains should refer to a report by Alqahtani et al. [20], which mentions that while there is plenty for this versatile DL tool, training and deployment costs remain significant challenges due to high time complexity. Our paper also discusses some of these challenges, as the GAN-augmented NIDS used up significantly more resources than traditional models. Nevertheless, the enhanced accuracy and significantly lower false positive rates of GANs in improving drug-disease-combinatorial signature-based prediction are indicative that any associated computation overhead may be justifiable.

The key novelty of our work is to show that GANs can be used for NIDS improvement through needed data augmentation adding new samples from the predefined types, but also novel approaches and obfuscated attack detections. This is an incredibly important skill sorely lacking in many NIDS, which often find old security threats to be new and advanced without real signature mimic support. These results further supports with that of by Navidan et al., who studied the use of GANs in networking and pointed out the role of synthetic data in boosting ML models generalization [19]. However, while Navidan et al. consider more general networking applications, this study applies these principles to the cybersecurity domain for a focused look at GANs in this important field.

In particular, the GAN-embedded NIDS for resistance shown in this paper is highly robust to adversarial attacks. Usama et al. overviewed how GANs can help initiate as well as prevent adversarial attacks on NIDS [21]. This work further contributes to the research by providing strong evidence of defensive power and empirically measuring the robustness of GAN-enhanced NIDS against adversarial examples generated using a fast gradient, as well as iterative-based attack methods in terms of a few quantitative. This significantly higher detection accuracy to recognize these examples compared to that of traditional models demonstrates that the architectures of GANs can profoundly contribute to strengthening cybersecurity defenses.

However, integrating GANs into existing cybersecurity frameworks is a challenge. Our interviews with cybersecurity experts on this issue raise concerns regarding the real-world deployment of GAN-enhanced NIDS, focusing mainly on computational overhead and operational bootstrapping of such models. Sorin et al. brought up similar concerns in the setting of radiology, with specific application to the deployment of GAN-generated synthetic images, for which our study was uniquely equipped but faced practical obstacles ranging from integration requirements and computational resource demands [17]. Overall, this provides some insight that although GAN offers enough advantages to justify using them in a real environment, careful consideration come into play as to how these models can be deployed and trained based off infrastructure capabilities and resource allocation.

Another key highlight of this research is that it concentrates the synthetic data to increase detection against new and obfuscated attacks. Li et al. related work also made use of GANs for dynamic cyberattacks' detection in the context of automated vehicles, a task closely related to novel attack vector identification with NIDS [22]. Our findings corroborate their results, GAN-generated data significantly improves the detection of such advanced attacks in our findings as well. This is an important capability for contemporary NIDS, where it must always adapt to new evolving menaces.

While these findings are encouraging, the study highlights directions for future work. Training stability, a topic that has been discussed before [20], is still an issue. Despite using techniques like fine-tuning hyperparameters, better optimizers, and other tips to keep the GAN Training Stable in this study, there is still a requirement for more stable methods across multiple datasets/environments so that one-pulse result is guaranteed. Also, the ethical issues of using GAN-generated data in cybersecurity need deeper research we can destroy ourselves people who noted this in the interviews said.

The article contributes to the increasing work use GANs in various areas of cybersecurity and performs experimental results that prove gains higher detection for NIDS. The results indicate that NIDS based on GANs can dramatically enhance the detection precision and stability for novel or adversarial attacks. Nonetheless, practical deployments of GAN-improved NIDS are confronted by computational resource costs and difficulties with integration as well as training stability. We recommend future research to design faster GAN architectures and study ethical concerns when applying them in cybersecurity. This study is a milestone in this regard, demonstrating that GANs have the potential to change the timeworn cybersecurity threat detection methods traditionally used inside companies operating in the present-day digital age.

VI. CONCLUSION

The article investigates the ability of GANs to enhance NIDS in identifying cyber-security attacks. The results conclusively prove that by using GAN for synthetic data generation, we can significantly enhance the performance of NIDS to detect both known and unknown cyber-attacks as well as minimize false positives. This has been substantiated across multiple experiments and evaluations comparing GAN based NIDS against conventional ML techniques like SVMS, RFs.

One of the major note-worthy things in this research is that a traditional model performs very well with respect to benchmarks, thus highlighting current approaches are suboptimal because they were not compared directly against these other methods. Traditional models frequently fail in the dynamic and evolving landscape of cyber threats, especially when new attacks emerge with features that are unobserved on their training data. The results shown in this research prove that GAN-powered NIDS are more robust against these challenges and therefore more accurate as well. When compared to the SVM and RF models, its detection accuracy was higher while it also had a lower false positive rate confirming that this method could be used to deal with complex irregularities in cybersecurity.

Meanwhile, GAN-improved NIDS has also proven its resilience to adversaries using attacks. This is particularly the case for adversarial attacks, a notorious problem in cybersecurity that involves constructing malicious inputs to fool machine learning models. It's more amazing that the attacks no longer seem to have much effect on the system, as a result of shifting to synthetic data created by GANs. All of this indicates that GANs can play a significant role in making cybersecurity frameworks stronger as well flexible which otherwise leaves organizations exposed to even the most sophisticated cyber threats. Overall, these results hint that GANs could be emerging as focus areas in the design of new cybersecurity systems due to ever-growing and increasingly sophisticated cyber threats.

Nevertheless, this research also does not ignore the difficulties and possible shortcomings of adopting GANs in cybersecurity. The most significant problem revealed is the computational cost of training GAN models. The study demonstrated that although GAN-augmented NIDS offers significant detection gains, the benefits are achieved at the expense of additional computation and long training duration. Such a trade-off between performance and resource utilization is an important consideration when deploying GAN-based systems in practical operating environments, where the computationally efficient operation inherent to real-world implementations are paramount.

Moreover, GANs are also not amenable for integration with most of today's cybersecurity stacks. Indeed, the GAN architectures are complex and require sustained training parade with newer attack vectors rendering training even more resource-intensive, for example utilizing sophisticated infrastructures/systems as well necessitates extremely specialized skill sets that may not be readily available within all organizations. Hence, if GAN-augmented NIDS are truly to be deployed widely --- with this study suggesting that they should --- organizations need not just have the right technical infrastructure but also expertise in order to effectively monitor and support these systems.

Especially when it comes to cybersecurity, the ethical considerations of using synthetic data and GAN-generated fake images should be taken into account. Despite the immense insights GANs provide in improved threat identification, there is a legitimate concern that this data could be stolen by adversaries and leveraged for adversarial purposes (like training attack-based approaches). While the current article flag up an ethical requirement to formalize a GAN cyber ethics, nonetheless new guidelines and safeguards have much needed place if the use of GANs as cybersecurity remain both practically useful and socially acceptable. This will be an interesting consideration for future work and such ethical questions would need to inform appropriate control of the risks derived from GAN-generated data.

The article shows how GANs can bring considerable gains in terms of cybersecurity frameworks overall and taken as an example the use of network intrusion detection systems. So at now, GAN-integrated NIDS seems very useful for handling the dynamic nature of cyber threats with better detection accuracy by having an adaptive behavior against any new attack, unlike its traditional counterparts. While these systems have great promise, the practical implementation of a system with this sophistication in computing requires overcoming computational demands and challenges associated integration as well considerations related to ethics. As cybersecurity continues to iterate, the importance of GANs in adding resilience and flexibility to threat detection systems will only grow more prominent. The study is a significant contribution to the field of GANs in cybersecurity while informing possible avenues for future research seeking solutions, and investigating means towards unleashing their full potential within cyber defense.

REFERENCES

[1] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio: ''Generative adversarial networks'', *Commun. ACM*, 63, (11), 2020, pp. 139–44

[2] A. Arora, and Shantanu: ''A Review on Application of GANs in Cybersecurity Domain'', *IETE Technical Review*, 39, (2), 2022, pp. 433-41

[3] C. Yinka-Banjo, and O.-A. Ugot: ''A review of generative adversarial networks and its application in cybersecurity'', *Artificial Intelligence Review*, 53, (3), 2020, pp. 1721-36

[4] P. F. d. Araujo-Filho, G. Kaddoum, D. R. Campelo, A. G. Santos, D. Macêdo, and C. Zanchettin: ''Intrusion Detection for Cyber–Physical Systems Using Generative Adversarial Networks in Fog Environment'', *IEEE Internet of Things Journal*, 8, (8), 2021, pp. 6247-56

[5] A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak: ''A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection'', *IEEE Access*, 11, 2023, pp. 76071-94

[6] T. Merino, M. Stillwell, M. Steele, M. Coplan, J. Patton, A. Stoyanov, and L. Deng: 'Expansion of Cyber Attack Data from Unbalanced Datasets Using Generative Adversarial Networks', in Lee, R. (Ed.): 'Software Engineering Research, Management and Applications' (Springer International Publishing, 2020), pp. 131-45

[7] S. M. Rayavarapu, T. S. Prasanthi, G. S. Rao, and G. S. Kumar: 'Generative Adversarial Networks for Anomaly Detection in Cyber Security: A Review', in Editor (Ed.)^(Eds.): 'Book Generative Adversarial Networks for Anomaly Detection in Cyber Security: A Review' (2023, edn.), pp. 662-66

[8] I. K. Dutta, B. Ghosh, A. Carlson, M. Totaro, and M. Bayoumi: 'Generative Adversarial Networks in Security: A Survey', in Editor (Ed.)^(Eds.): 'Book Generative Adversarial Networks in Security: A Survey' (2020, edn.), pp. 0399-405

[9] E. Ayanoglu, K. Davaslioglu, and Y. E. Sagduyu: ''Machine Learning in NextG Networks via Generative Adversarial Networks'', *IEEE Transactions on Cognitive Communications and Networking*, 8, (2), 2022, pp. 480-501

[10] Z. Pan, W. Yu, X. Yi, A. Khan, F. Yuan, and Y. Zheng: ''Recent Progress on Generative Adversarial Networks (GANs): A Survey'', *IEEE Access*, 7, 2019, pp. 36322-33

[11] D. Saxena, and J. Cao: ''Generative Adversarial Networks (GANs): Challenges, Solutions, and Future Directions'', *ACM Comput. Surv.*, 54, (3), 2021, pp. Article 63

[12] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab: ''Threat Analysis for Automotive CAN Networks: A GAN Model-Based Intrusion Detection Technique'', *IEEE Transactions on Intelligent Transportation Systems*, 22, (7), 2021, pp. 4467-77

[13] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye: ''A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications'', *IEEE Transactions on Knowledge and Data Engineering*, 35, (4), 2023, pp. 3313-32

[14] L. Gordon: ''Leveraging Dual-Generative Adversarial Networks for Adversarial Malware Detection via Ensemble Learning'', *Inquiry@Queen's Undergraduate Research Conference Proceedings*, 17, (2), 2023

[15] R. Soleymanzadeh, and R. Kashef: 'A Stable Generative Adversarial Network Architecture for Network Intrusion Detection', in Editor (Ed.)^(Eds.): 'Book A Stable Generative Adversarial Network Architecture for Network Intrusion Detection' (2022, edn.), pp. 9-15

[16] S. Ghosh: '407Consequentialist Thinking and Economic Analysis in Intellectual Property', in Editor (Ed.)^(Eds.): 'Book 407Consequentialist Thinking and Economic Analysis in Intellectual Property' (Oxford University Press, 2021, edn.), pp. 0

[17] V. Sorin, Y. Barash, E. Konen, and E. Klang: ''Creating Artificial Images for Radiology Applications Using Generative Adversarial Networks (GANs) - A Systematic Review'', *Acad Radiol*, 27, (8), 2020, pp. 1175-85

[18] K. Ashok, R. Boddu, S. A. Syed, V. R. Sonawane, R. G. Dabhade, and P. C. S. Reddy: ''GAN Base feedback analysis system for industrial IOT networks'', *Automatika*, 64, (2), 2023, pp. 259-67

[19] H. Navidan, P. F. Moshiri, M. Nabati, R. Shahbazian, S. A. Ghorashi, V. Shah-Mansouri, and D. Windridge: ''Generative Adversarial Networks (GANs) in networking: A comprehensive survey & evaluation'', *Computer Networks*, 194, 2021, pp. 108149

[20] H. Alqahtani, M. Kavakli-Thorne, and G. Kumar: ''Applications of Generative Adversarial Networks (GANs): An Updated Review'', *Archives of Computational Methods in Engineering*, 28, (2), 2021, pp. 525-52

[21] M. Usama, M. Asim, S. Latif, J. Qadir, and F. Ala Al: 'Generative Adversarial Networks For Launching and Thwarting Adversarial Attacks on Network Intrusion Detection Systems', in Editor

(Ed.)^(Eds.): 'Book Generative Adversarial Networks For Launching and Thwarting Adversarial Attacks on Network Intrusion Detection Systems' (2019, edn.), pp. 78-83

[22] T. Li, M. Shang, S. Wang, M. Filippelli, and R. Stern: 'Detecting Stealthy Cyberattacks on Automated Vehicles via Generative Adversarial Networks', in Editor (Ed.)^(Eds.): 'Book Detecting Stealthy Cyberattacks on Automated Vehicles via Generative Adversarial Networks' (2022, edn.), pp. 3632-37