IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141113

Generative Shields and Adversarial Swords: A Taxonomy of GAN Applications in Network Security

Shriya Arunkumar[1], Kushal Kumar. B. N[2]

Dept. of CSE- ICB, Kammavari Sangha Institute of Technology, Bangalore, India[1]

Head of Department, Dept. of CSE-ICB, Kammavari Sangha Institute of Technology, Bangalore, India[2]

Abstract: As cyber threats rapidly evolve in complexity, Gen- erative Adversarial Networks (GANs) have emerged as trans- formative tools in network security, serving both as formidable defenses and novel avenues for attack. This survey introduces a comprehensive taxonomy of GAN applications in network secu- rity, classifying contemporary research across critical domains such as adversarial sample generation, intrusion detection, syn- thetic traffic modeling, federated security architectures, IoT and edge protection, and encrypted traffic analysis. By systematically mapping these domains, the paper illustrates how diverse GAN variants are leveraged for simulating threats, resolving class imbalance, and circumventing conventional detection strategies. The taxonomy uncovers key trends in the development and deployment of GAN-driven security models, providing a robust framework for assessing progress and identifying persistent challenges. The review concludes by outlining emerging research directions rooted in the taxonomy, and calls for standardized benchmarks and ethical guidelines to support secure, scalable integration of GANs into modern network defenses.

Index Terms: GANs, Network Security, Intrusion detection, Generative AI, Cybersecurity, Adversarial attacks.

INTRODUCTION

The proliferation of internet-connected systems across crit- ical domains has made robust network security more crucial than ever. Furthermore, traditional intrusion detection methods, including signature-based and machine learning approaches, face challenges against novel or adaptive threats due to their dependence on labeled data and lack of adaptability. Rec- ognizing these limitations, recent advances in deep learning, especially Generative Adversarial Networks (GANs), have shown promise in generating realistic synthetic attack data and strengthening intrusion detection systems. In response, this survey reviews the latest defensive and offensive applications of GANs in network security, highlights major contributions, and discusses ongoing challenges and future research directions.

Yet, to frame this discussion, the remainder of this paper is organized as follows: Having motivated the need for GANs, Section II presents an overview of GANs and their relevance to network security. Section III highlights key application areas. Section IV presents the methodology used in the paper.

With this context established Section V discusses representa- tive studies and significant research contributions. Section VI outlines open challenges and limitations. Finally, Section VII offers concluding remarks and directions for future research.

II. OVERVIEW

Generative Adversarial Networks (GANs) are a powerful class of generative models in deep-learning. Introduced by Goodfellow et al. in 2014 [1], GANs are designed to learn complex data distributions through a two-player min-max game involving two neural networks: a generator (G) and a discriminator (D). The generator creates synthetic data, while the discriminator learns to differentiate it from real data. As training progresses, the generator improves its ability to mimic real samples, and the discriminator becomes more effective at identifying fakes.
Specifically, the standard GAN objective function is defined as:

$$\min_G \max_D V(D, G) = E_{x \sim pdata(x)} [\log D(x)]$$

DOI: 10.17148/IJARCCE.2025.141113

+ Ez~pz (z) [log (1 − D(G(z)))] (1)

where:

- D(x) is the discriminator's estimated probability that x

is a real sample.

- G(z) is the generator's output given noise vector z.
- pdata(x) represents the true data distribution.
- pz(z) is the prior distribution (e.g., Gaussian or uniform) from which z is drawn.

In the domain of network security, GANs are applied in both defensive and adversarial contexts. On one hand, they are used to generate synthetic training data, simulate network traffic, and enhance intrusion detection systems (IDS). On the other hand, they may be employed to craft adversarial samples that imitate normal behavior, enabling them to bypass detection systems.

An *adversarial attack* refers to deliberately crafted inputs designed to deceive machine-learning models into making incorrect predictions. In cybersecurity, such attacks can target

IDS, malware classifiers, or anomaly detectors. GANs are particularly effective for these purposes because they can learn the underlying patterns of normal network behavior and generate malicious samples that closely resemble benign traffic.

Generative Adversarial Networks (GANs), are a type of deep learning model consisting of two neural networks, the generator and the discriminator, that compete against each other in a zero-sum game. As illustrated in Figure.1, the generator creates synthetic data samples, while the discrimi- nator evaluates them against real data to improve authenticity. Over time, this adversarial process leads the generator to produce increasingly realistic outputs, making GANs powerful tools for data generation, image synthesis, and cybersecurity applications.

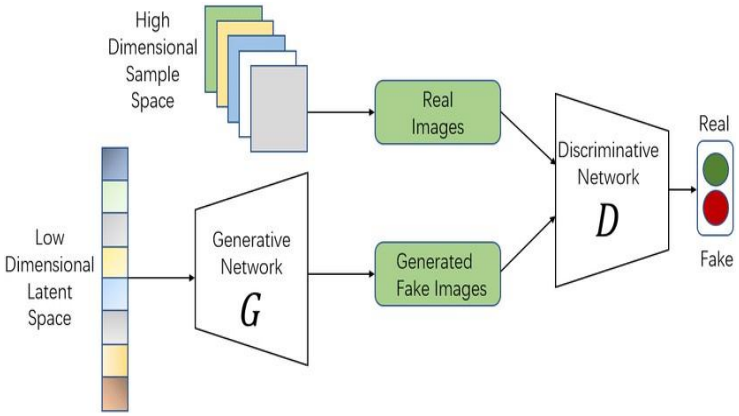

Fig. 1. Generative Adversarial Networks

Recent research highlights several emerging applications of GANs in this field:

- Generating realistic attack traffic to test IDS robustness,
- Creating synthetic variants of zero-day attacks,
- Poisoning training datasets to reduce detection accuracy, and
- Evaluating models under both white-box and black-box conditions.

I. APPLICATIONS OF GANS IN NETWORK SECURITY

Building on this foundation, GANs have shown strong po- tential in improving network security by generating synthetic data that mirrors real-world patterns. This capability aids both in strengthening defensive models and in stress-testing their robustness. This section outlines the primary applications of GANs in the cybersecurity domain.

A. Adversarial Attack Generation

A key application of GANs in cybersecurity is generating adversarial examples that evade IDS and other defenses. These examples are crafted to resemble benign network traffic while preserving malicious intent. Unlike conventional adversarial attacks that rely on minor perturbations, GAN-generated at- tacks can learn and reproduce statistical

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141113

patterns of legitimatebehavior, resulting in highly realistic adversarial traffic. This capability enables the evaluation of IDS performance in both white-box and black-box threat models.

B. Intrusion Detection System (IDS) Enhancement

Conversely, GANs are widely used to enhance IDS perfor- mance by generating synthetic training data, especially for rare or underrepresented attack types. This is especially beneficial in imbalanced datasets where traditional classifiers struggle to detect rare but critical threats. Consequently, by augmenting the dataset with realistic attack samples, GANs contribute to improved generalization and detection accuracy in both supervised and semi-supervised IDS frameworks.

C. Network Traffic Simulation and Augmentation

The use of GANs for simulating network traffic has gained traction in the contexts of research, system testing, and model training. GAN-generated traffic can accurately emulate both benign and malicious behaviors, facilitating the creation of large-scale datasets without relying exclusively on real-world traffic captures. It is particularly effective when labeled data is scarce, privacy-restricted, or expensive to generate.

D. Data Anonymization and Privacy Preservation

Although less common, GANs have also been explored for data anonymization in network environments. GANs en- able privacy-preserving data sharing by generating synthetic data that mimics real distributions while masking sensitive information, supporting collaborative machine learning across organizational boundaries. This application underscores the broader role of GANs in enabling secure and ethical data practices in cybersecurity.

E. Model Robustness Evaluation

GANs help evaluate the resilience of ML-based security sys- tems and guide improvements against adversarial threats. By generating tailored attack samples that exploit known model vulnerabilities, GANs help simulate adversarial conditions and worst-case scenarios. These simulations aid in the development of more resilient models through adversarial training and robustness-enhancing strategies.

In summary, the versatility of GANs in generating, simu- lating, and manipulating network data has positioned them as a key focus of cybersecurity research.

II. METHODOLOGY

To systematically assess these applications, the survey methodology was conducted in six steps. Initially, five ma- jor digital libraries (IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and WSEAS Transactions) were queried for-reviewed publications on GANs applied to net- work security, covering the period January 2014–June 2025. Consequently, inclusion criteria required each study to present experimental validation of GAN-based IDS enhancement, ad- versarial attack generation, data augmentation, or architectural innovation; works without quantitative results or outside the

network-security scope were excluded. Subsequently, after duplicate removal, titles and abstracts of the remaining records were screened, yielding 102 candidate papers for full-text review. Later on, each paper was coded for key attributes, GAN variant, training protocol, target domain (e.g., IoT, SDN, in-vehicle networks), evaluation metrics, and dataset characteristics—using a standardized extraction form. Then, papers were grouped into eight thematic categories (A-H) to facilitate cross-comparison of approaches, common datasets, performance gains, and reported limitations. Finally, a gap analysis synthesized findings across categories to identify underexplored areas, such as encrypted-traffic analysis and federated GANs, and to propose directions for future research in adversarial robustness and practical deployment.

III. REPRESENTATIVE STUDIES

This section reviews key research contributions exploring the application of Generative Adversarial Networks (GANs) in cybersecurity. Each work highlights unique use cases, architec- tures, or methodologies that demonstrate the evolving role of GANs in both offensive and defensive security contexts. The selected papers span foundational surveys, attack-generation techniques, IDS enhancement methods, and broader AI im- plications. Together, they provide a representative view of current trends and research directions in this rapidly advancing field.Table I, which appears on the following page, overviews the primary research themes and representative GAN methods categorized in this section.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141113

A. Surveys, Reviews, and Theoretical Landscape Studies

First Ankalaki et al. [2] provide a comprehensive analysis of artificial intelligence techniques in cybersecurity, comparing traditional machine learning and deep learning methods with emerging generative AI approaches such as GANs and NLP- based threat simulations which together enhance cyber-attack prediction and response capabilities.
Dunmore et al. [3] systematically survey the application of GANs in intrusion detection systems, categorizing existing work across network trespass, botnet detection, malware detection, and other domains, and highlight how GAN-based synthetic data generation addresses class imbalance and im- proves IDS robustness.
Gupta et al. [4] examine the dual role of large language models in cybersecurity and privacy, detailing how generative AI can automate defense tasks like secure code generation and threat intelligence while also presenting risks such as automated social engineering, malware synthesis, and data leakage.
Khazane et al. [22] conduct a holistic review of adversarial machine learning in IoT networks, redefining attack and defense taxonomies and offering technical insights into state-of- the-art adversarial methods and mitigation strategies for IDSs, MDSs, and DISs in heterogeneous IoT environments.
Lim et al. [13] provide a comprehensive review of recent advancements in applying GANs to anomaly detection within network security, examining the strengths and limitations of various GAN-based approaches and highlighting their effec- tiveness in handling data imbalance and detecting sophisticated attacks.

B. Adversarial Attack Generation / IDS Evasion

Ghanem et al. [5] leverage memetic algorithms to craft adversarial malware examples that evade machine-learning detectors by integrating local search into traditional genetic algorithms. Their method achieves 98% evasion rate against the MalConv deep learning model while using fewer generations and a smaller population size. The results demonstrate that memetic algorithms surpass standard evolutionary techniques in producing functionality-preserving, evasive malware samples.
Zhang et al. [6] develop a GAN-based framework combining a generator and substitute detector to automatically produce attack traffic that remains functional and significantly lowers detection rates across multiple IDS models. Their findings underscore GANs' potential to expose vulnerabilities in existing intrusion detection solutions.
Randhawa et al. [7] present a GAN framework tailored for low-data, imbalanced settings that synthesizes realistic minority-class evasion samples while training the discriminator to recognize such attacks, yielding improved detection accuracy and resilience. Experimental validation on cybersecurity and computer vision datasets confirms the approach's versatility.
Aldhaheri and Alhuzali [8] introduce a self- attention–enhanced GAN that generates sophisticated adversarial network flows, resulting in notable reductions in IDS detection rates. Their study highlights current IDS architectures' susceptibility and calls for adversarially aware defense mechanisms.
Chowdhary et al. [21] propose a GAN-driven system for autonomous web-application penetration testing that generates realistic attack payloads to uncover vulnerabilities without predefined signatures. The framework demonstrates enhanced scalability and effectiveness over manual testing, efficiently identifying a broad spectrum of security flaws.

C. Intrusion Detection System (IDS) Enhancement.

Next, M. H. Shahriar et al. [9] develop a GAN-driven IDS that synthesizes realistic attack samples to strengthen detection models and address class imbalance, resulting notable improvements in accuracy and adaptability. Their generator crafts high-fidelity malicious traffic, while the discriminator refines its decision boundary between benign and adversarial flows, yielding superior generalization.
Abdelaty et al. [10] propose an adversarial training pipeline for DDoS mitigation, using GANs to generate challenging attack scenarios that harden detectors against both known and novel traffic patterns. This method significantly boosts detector resilience and accuracy in the presence of crafted evasion attempts.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141113

TABLE I
TAXONOMY OF GAN APPLICATIONS IN NETWORK SECURITY (GROUPED BY MAJOR RESEARCH THEMES)

Research Category	Security Task	Representative GAN	Dataset	Key Performance / Impact
Survey & Theoretical	N/A (Survey)	Dunmore et al. [3], Khazane et al. [22]	–	Summarizes GAN architectures; proposes taxonomy
Adversarial Attack Generation / IDS Evasion	Malware evasion; IDS bypass; packet adversaries	IDSGAN [6], SGAN-IDS [8], Attack-GAN [14]	NSL-KDD, CICIDS2017, Custom	Up to –95% TPR; effective black-box evasion
IDS Enhancement	Imbalanced data; synthetic traffic for IDS	G-IDS [9], CWVAEGAN-1DCNN [19]	CIC-IDS2017, NSL-KDD	+12% recall; superior to SMOTE
Data Augmentation / Rare Attack Handling	Synthetic traffic / oversampling; rare class boosting	SYN-GAN [25], GAN-FS [11]	IoT datasets, NSL-KDD, CICIDS2017	Improved IDS metrics; reduced false alarms
Architectural & Framework Innovations	Hybrid; distributed/federated GAN-IDS	GAN+Transformer [15], FEDGAN-IDS [16]	TON-IoT, CIC-IoT	¿98% accuracy; privacy-preserving
IoT & Edge Security Applications	Edge/vehicle/CAN bus security	GIDS [12], SecureNet [20], SSGAN [17]	CAN bus, IoT-23, Ton-IoT	Unsupervised detection; high F_1; low latency
Encrypted Traffic Analysis	Encrypted traffic classification	GAN+CNN [24]	ISCX VPN, CICFlowMeter-V3	Outperforms conventional methods under limited labels

Cheng et al. [14] analyze flow-based IDS vulnerabilities by creating adversarial examples with GANs and demonstrate that such samples can markedly degrade model performance. Their findings underscore the urgent need for IDS architectures capable of resisting adaptive adversarial attacks under real- world conditions.
He et al. [19] integrate a conditional Wasserstein variational autoencoder with GANs and one-dimensional CNNs to enrich feature extraction and detect complex threats. Their hybrid framework augments training data with realistic synthetic traffic and employs deep learning to identify both existing and emerging attacks. Experimental results confirm that this composite approach outperforms conventional IDS techniques in detection accuracy and robustness.
Overall, these studies highlight the pivotal role of generative models in advancing IDS effectiveness and underscore the importance of adversarially informed training strategies.

D. Data Augmentation / Oversampling / Rare Attack Handling

Liu et al. [11] propose an intrusion detection oversampling method that combines generative adversarial networks with feature selection to address class imbalance in network se- curity datasets. Their technique generates high-quality synthetic minority class samples, improving the effectiveness of machine-learning-based intrusion detectors. Experimental results show significant gains in detection accuracy and ro- bustness compared to traditional oversampling methods.

Rahman et al. [25] present SYN-GAN, an intrusion detec- tion framework that leverages generative adversarial networks to produce synthetic IoT attack data, addressing issues of data scarcity and class imbalance. Their method enables robust training of detection models, resulting in improved accuracy and resilience against diverse IoT security threats. Experimen- tal results demonstrate that SYN-GAN significantly enhances detection performance compared to traditional approaches reliant on limited real attack samples.

Framework & Architectural Innovations

Moghaddam et al. [15] present an intrusion detection framework for IoT environments that synergistically combines generative adversarial networks and transformer models to improve robustness against evolving cyber threats. Their approach leverages GANs to generate realistic synthetic intrusion data and utilizes transformers for advanced feature extraction and classification. Experiments demonstrate that this combined method achieves higher detection accuracy and resilience compared to traditional models, especially in the complex landscape of IoT security.

E. Federated / Distributed / Privacy-Preserving IDS

Tabassum et al. [16] propose FEDGAN-IDS, a privacy- preserving intrusion detection system that integrates generative adversarial networks with federated learning to enhance cyber- security without sharing sensitive local data. Their approach enables distributed training of intrusion detection models using GAN-generated synthetic samples while maintaining user pri- vacy across different organizations. Experimental evaluations demonstrate improved detection accuracy and privacy protec- tion compared to traditional centralized methods.

F. IoT and Edge Network Security Applications

Nukavarapu and Nadeemi [17] propose a semi-supervised GAN framework for edge-based IoT intrusion detection, blending labeled and unlabeled data to bolster identification under limited annotation conditions. Their generator

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141113

synthe- sizes plausible attack instances while the discriminator refines its detection boundary using both real and synthetic samples, resulting in notably higher detection rates. The authors report improved adaptability to evolving threat patterns compared to standard supervised models.

Seo et al. [12] develop a GAN-powered IDS for in- vehicle networks that crafts realistic CAN-bus attack traffic to strengthen classifier robustness. By training the discrimina- tor on normal and adversarial flows, their method achieves

accurate differentiation of malicious packets. Experimental evaluation demonstrates consistent low false-positive rates across diverse automotive attack scenarios.

Lent et al. [18] introduce an unsupervised GAN approach for SDN security, learning baseline traffic distributions to autonomously flag DDoS anomalies. Their model operates without labeled data, leveraging the discriminator's anomaly scoring to detect distributed denial-of-service events in real time. Results show strong detection performance with minimal false alarms under varied network conditions.

Kalyanaraman et al. [20] present an adversarial learning framework for wireless sensor networks, where the GAN gen- erator fabricates sophisticated intrusion samples to challenge the classifier. The discriminator's exposure to both genuine and crafted data enhances its resilience to stealthy attacks. The study reports substantial gains in detection accuracy and robustness within resource-limited sensor deployments.

Almars et al. [23] design a GAN-based IDS for IoT environments that oversamples minority (botnet) traffic to address class imbalance. Their generator produces high-fidelity attack samples, enabling the discriminator to better distinguish malicious communications. Empirical results confirm signifi- cant improvements in identifying malicious IoT traffic while maintaining low false-positive rates, underscoring the practical viability of GAN-driven augmentation.

G. Encrypted Traffic Analysis and Classification

Refat Al-Milli and Al-Khassawneh [24] propose an in- trusion detection system that combines convolutional neural networks with generative adversarial networks to improve the identification of malicious network traffic. Their approach uses GANs to generate realistic synthetic attack data, aiding the CNN in accurately learning complex attack patterns and addressing data imbalance issues. Experimental results show enhanced detection accuracy and reduced false positives com- pared to traditional machine learning approaches.

IV. LIMITATIONS AND CHALLENGES

Despite their growing popularity, the use of Generative Adversarial Networks (GANs) in network security comes with several open challenges and limitations that must be addressed for safe and effective deployment.

As depicted in Figure.2 , GAN training is inherently un- stable due to the adversarial dynamics between the generator and discriminator. This competition often leads to difficulty in reaching equilibrium, largely stemming from differences in learning speeds between the two networks. A common issue is vanishing gradients, where the generator fails to receive meaningful updates, thereby stalling progress. These factors exacerbate mode collapse, where the generator produces lim- ited, repetitive outputs. Furthermore, such instabilities hinder the model's ability to maintain continuous learning, especially in evolving environments like network security where threat landscapes shift rapidly.

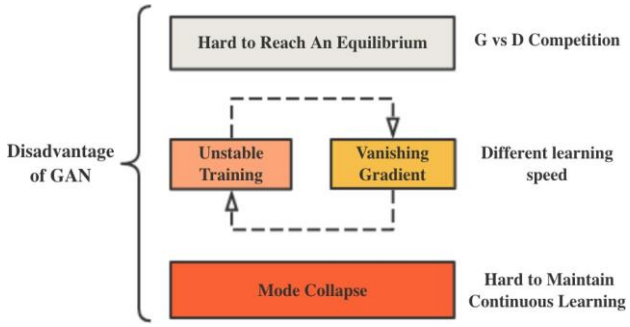

Fig. 2. Disadvantages of GANs

A. Data Quality and Availability

GAN performance is heavily dependent on the quality and diversity of training data. In many network security scenarios, especially involving rare or sophisticated attacks, labeled data is either scarce or imbalanced. This makes it difficult for GANs to learn meaningful patterns and can lead to poor generalization or biased outputs. Additionally, access to real- world network data is often limited due to privacy, compliance, or organizational constraints.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141113

B. *Training Instability and Mode Collapse*

GANs are notoriously difficult to train. Issues such as non- convergence, mode collapse (where the generator produces limited output diversity), and sensitivity to hyperparameters are still open research problems. In cybersecurity contexts, these instabilities can result in unrealistic or repetitive traffic patterns that fail to mimic true malicious behavior.

C. *Evaluation Challenges*

Unlike traditional classifiers, evaluating the effectiveness of GANs is not straightforward. Metrics such as accuracy or precision do not directly apply to generative models. In the context of network security, it becomes even more difficult to quantify how "realistic" or "evasive" the synthetic traffic is. Most studies rely on indirect evaluation methods such as testing generated traffic against an IDS, which may not always reflect real-world performance.

D. *Security and Misuse Risks*

GANs can be a double-edged sword. While they can strengthen intrusion detection systems, they can also be used to generate more advanced, evasive attacks. This dual-use nature raises ethical concerns. If such models are not handled responsibly, they could be misused to develop highly stealthy malware or attack traffic capable of bypassing security mech- anisms.

E. *Computational Cost and Deployment Constraints*

Training GANs, particularly on large-scale network traffic data, requires significant computational resources. In real-time

or resource-constrained environments, deploying GAN-based models for either detection or simulation can be impractical.

CONCLUSION AND FUTURE DIRECTIONS

In Summary, Generative Adversarial Networks (GANs) are rapidly reshaping the landscape of network security, offering innovative ways to both strengthen and challenge traditional defense mechanisms. Through this survey, we examined how GANs are being used across various applications, including adversarial attack generation, intrusion detection enhancement, and synthetic traffic simulation. These techniques demonstrate the versatility of GANs in addressing real-world security problems, especially in complex or data-scarce environments. At the same time, our review highlights critical concerns. Training instability, lack of standardized evaluation methods, and the ethical implications of adversarial generation remain significant hurdles. The dual-use nature of GANs—where the same tools can be employed for both defense and eva- sion—demands thoughtful governance, transparency, and on-

going oversight.

Looking forward, there is a growing need for research that focuses on improving the robustness, interpretability, and efficiency of GAN-based models in dynamic network environments.

Ultimately, while GANs are not a silver bullet, they open new pathways toward intelligent, adaptive, and more resilient cybersecurity systems. With careful development and respon- sible use, GANs have the potential to play a vital role in defending the digital infrastructure of the future.

REFERENCES

[1] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley,
S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in Advances in Neural Information Processing Systems, vol. 27, 2014, pp. 2672–2680.

[2] S. Ankalaki, A. R. Atmakuri, M. Pallavi, G. S. Hukkeri, T. Jan, and G. R. Naik, "Cyber attack prediction: From traditional machine learning to generative artificial intelligence," IEEE Access, 2025, doi: 10.1109/ACCESS.2025.3547433.

[3] A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, "A comprehen- sive survey of generative adversarial networks (GANs) in cybersecurity intrusion detection," IEEE Access, vol. 11, pp. 76071–76094, 2023, doi: 10.1109/ACCESS.2023.3296707.

[4] M. Gupta, C. Akiri, K. Aryal, E. Perker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2023.

[5] K. Ghanem, Z. Kherbache, and O. Ourdighi, "Enhancing Adversarial Examples for Evading Malware Detection Systems: A Memetic Al- gorithm Approach," International Journal of Computer Network and Information Security (IJCNIS), vol. 17, no. 1, pp. 1–16, 2025, doi: 10.5815/ijcnis.2025.01.01.

DOI: 10.17148/IJARCCE.2025.141113

[6] Z. Lin, Y. Shi, and Z. Xue, ”IDSGAN: Generative adversarial networks for attack generation against intrusion detection,” in Advances in Knowl- edge Discovery and Data Mining — PAKDD 2022, LNCS, vol. 13282, pp. 79–91, 2022.

[7] R. H. Randhawa, N. Aslam, M. Alauthman, and H. Rafiq, ”EVAGAN: Evasion generative adversarial network for low data regimes,” IEEE Trans. Artif. Intell., vol. 4, no. 5, pp. 1076–1088, Oct. 2023, doi: 10.1109/TAI.2022.3196283.

[8] S. Aldhaheri and A. Alhuzali, ”SGAN-IDS: Self-Attention-Based Gen- erative Adversarial Network against Intrusion Detection Systems,” Sen- sors, vol. 23, no. 18, Art.7796, Sep. 2023, doi: 10.3390/s23187796.

[9] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso Jr., ”G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System, ”IEEE Trans. Artif. Intell., vol. 4, no. 5, pp. 1076–1088, Oct. 2023, doi: 10.1109/TAI.2022.3196283.

[10] M. Abdelaty, S. Scott-Hayward, R. Doriguzzi-Corin, and D. Siracusa, ”GADoT: GAN-based Adversarial Training for Robust DDoS Attack Detection,” in Proc. 9th IEEE Conf. Commun. Netw. Secur. (CNS), pp. 1–9, IEEE, 2021, doi: 10.1109/CNS53000.2021.9705040.

[11] X. Liu, T. Li, R. Zhang, D. Wu, Y. Liu, Z. Yang, and S. Sciancalepore, ”A GAN and feature selection-based oversampling technique for intru- sion detection,” Security and Communication Networks, vol. 2021, Art. ID 9947059, 2021, doi: 10.1155/2021/9947059.

[12] E. Seo, H. M. Song, and H. K. Kim, ”GIDS: GAN based Intrusion Detection System for In-Vehicle Network,” in Proc. 16th Annu. IEEE Conf. Privacy, Security Trust (PST), Belfast, Ireland, Aug. 2018, pp.1–6, doi: 10.1109/PST.2018.8514157.

[13] W. Lim, K. S. C. Yong, B. T. Lau, and M. R. Arshad, ”Future of generative adversarial networks (GAN) for anomaly detection in network security: A review,” Computers & Security, vol. 139, pp. 103733, 2024. doi:10.1016/j.cose.2024.103733.

[14] Q. Cheng, A. Navidan, A. Abusnaina, and S. Al-Hashimi, ”Investigating on the robustness of flow-based intrusion detection system against ad- versarial samples using Generative Adversarial Networks,” J. Inf. Secur. Appl., vol. 73, Art.103472, Mar. 2023, doi: 10.1016/j.jisa.2023.103472.

[15] P. S. Moghaddam, A. Vaziri, S. S. Khatami, F. Hernando-Gallego, and D. Mart´ın, ”Generative Adversarial and Transformer Network Synergy for Robust Intrusion Detection in IoT Environments,” Future Internet, vol. 17, no. 6, Art. 258, Jun. 2025, doi: 10.3390/fi17060258.

[16] A. Tabassum, A. Erbad, W. Lebda, A. A. Mohamed, and M. Guizani, ”FEDGAN-IDS: Privacy-preserving Intrusion Detection System using Generative Adversarial Networks and Federated Learn- ing,” Comput. Commun., vol. 192, pp.299–310, Aug. 2022, doi: 10.1016/j.comcom.2022.06.015.

[17] S. K. Nukavarapu and T. Nadeemi, ”Securing Edge-based IoT Networks with Semi-Supervised GANs,” in Proc. 2021 IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), Mar. 2021, pp. 1–6, doi: 10.1109/PerComWorkshops51409.2021.9431112.

[18] D. M. B. Lent, V. G. da Silva Ruffo, L. F. Carvalho, J. Lloret, J. J. P. C. Rodrigues, and M. L. Proenc¸a Jr., ”An Unsupervised Gen- erative Adversarial Network System to Detect DDoS Attacks in SDN,” IEEE Access, vol. 12, pp. 70690–70706, May 2024, doi: 10.1109/ACCESS.2024.3402069.

[19] J. He, X. Wang, Y. Song, X. Qian, and C. Chen, ”Network Intrusion Detection Based on Conditional Wasserstein Variational Autoencoder with Generative Adversarial Network and One-Dimensional Convolutional Neural Networks,” Appl. Intell., vol. 53, no. 10, pp. 12416–12436, Sep. 2022, doi: 10.1007/s10489-022-03995-2.

[20] S. Kalyanaraman, S. Ponnusamy, S. Saju, S. Sangeetha, and R. Karthikeyan, ”Adversarial Learning for Intrusion Detection in Wire- less Sensor Networks: A GAN Approach,” Enhancing Security in Public Spaces Through Generative Adversarial Networks (GANs), ch. 4, pp. 39– 52, IGI Global, 2024, doi: 10.4018/979-8-3693-3597-0.ch004.

[21] A. Chowdhary, K. Jha, and M. Zhao, ”Generative Adversarial Network (GAN)-Based Autonomous Penetration Testing for Web Applications,” Sensors, vol. 23, no. 18, Art. 8014, Sep. 2023, doi: 10.3390/s23188014.

[22] A.H. Khazane, M. Ridouani, F. Salahdine, and N. Kaabouch, ”Ad- versarial Machine Learning in IoT: A Holistic Survey of Attack and Defense Methods,” Future Internet, vol. 16, no. 1, Art. 32, Jan. 2024, doi: 10.3390/fi16010032.

[23] M. Almars, M. Aldwairi, and M. Younis, ”IoT Intrusion Detection Using Generative Adversarial Networks: A Case Study with Botnet Datasets,” IEEE Internet of Things Journal, vol. 10, no. 6, pp. 5164–5173, Mar. 2023, doi: 10.1109/JIOT.2022.3222626.

[24] R. Al-Milli and Y. A. Al-Khassawneh, ”Intrusion Detection System using CNNs and GANs,” WSEAS Transactions on Computer Research, vol. 12, pp. 281–290, 2024, doi: 10.37394/232018.2024.12.27.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141113

[25] M. S. Rahman, S. Pal, S. Mittal, T. Chawla, and C. Karmaka, ”SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security”, Internet of Things, vol. 26, Jul.2024, Art. 101212, doi: 10.1016/j.iot.2024.101212.

