



Deep Learning-Based Visualization of Network Threat Patterns Using GAN-Generated Infographic

Mars Caroline Wibowo^{1*}, Iwan Setyawan², Adi Setiawan³, Irwan Sembiring⁴

¹Department of Visual Communication Design, Faculty of Academic Studies, Universitas Sains dan Teknologi Komputer, Semarang, Indonesia

²Department of Computer Science, Faculty of Information Technology, Universitas Kristen Satya Wacana, Salatiga, Indonesia

¹caroline@stekom.ac.id, ²iwan.setyawan@uksw.edu, ³adi.setiawan@uksw.edu, ⁴irwan@uksw.edu

Abstract

Despite the growing sophistication of cyberattacks, current network traffic analysis tools often lack intuitive visual support, limiting human analysts' ability to interpret complex threat behaviors. To address this gap, this study proposes a novel deep learning-based visualization framework using a Deep Convolutional Generative Adversarial Network (DCGAN) to synthesize threat-specific infographics from structured numerical features in the CICIDS 2017 dataset. Unlike conventional methods, such as PCA or static dashboards, which often result in abstract or non-adaptive visuals, our approach generates class-distinct grayscale images that preserve the behavioral patterns of various attacks, including denial-of-service, brute force, and port scanning. The preprocessing pipeline reshapes the selected flow-based features into 28×28 matrices to train the generative model. Evaluation using the Frechet Inception Distance (FID) yielded a score of 28.4, whereas a CNN classifier trained on the generated images achieved 91.2% accuracy, confirming visual fidelity and semantic integrity. Additionally, a panel of human experts rated the interpretability of the generated images at 4.3 out of 5.0. These findings demonstrate that generative visualization can enhance human-centered threat analysis by bridging raw data with interpretable imagery, thereby offering a scalable and explainable approach for integrating AI into real-time security workflows.

Keywords: explainable AI; frechet inception distance (FID); generative adversarial network (GAN); network security; threat visualization

How to Cite: M. C. Wibowo, I. Setyawan, A. Setiawan, and I. Sembiring, "Deep Learning-Based Visualization of Network Threat Patterns Using GAN-Generated Infographic", *J. RESTI (Rekayasa Sist. Teknol. Inf.)*, vol. 9, no. 4, pp. 765 - 770, Aug. 2025.

Permalink/DOI: <https://doi.org/10.29207/resti.v9i4.6717>

Received: June 3, 2025

Accepted: July 23, 2025

Available Online: August 15, 2025

This is an open-access article under the CC BY 4.0 License

Published by Ikatan Ahli Informatika Indonesia

1. Introduction

The exponential growth of data traffic and the increasing complexity of cyber threats have created substantial challenges for network security operations. Analysts are often confronted with vast, unstructured network logs that are difficult to interpret in real time, especially when dealing with evolving attack patterns such as denial-of-service (DoS), brute-force login attempts, or advanced persistent threats [1]-[4].

Traditional monitoring techniques, such as rule-based alerts, static dashboards, and signature-based systems, remain widely used but often lack the flexibility to adapt to emerging threat patterns [5]. Visual analytics has been introduced as a complementary approach to enhance situational awareness, enabling analysts to identify anomalies more intuitively and extract patterns

through graphical representations [6]. However, conventional visualization methods, such as preconfigured dashboards and heatmaps [7], tend to be static and rely on fixed features or thresholds. While heatmaps are useful in highlighting dense areas of activity, they struggle to convey temporal sequences or nuanced behavioral changes, which are crucial for modern threat detection.

To address this limitation, researchers have adopted dimensionality reduction techniques, such as Principal Component Analysis (PCA) and t-distributed Stochastic Neighbor Embedding (t-SNE), to project high-dimensional traffic data into two-dimensional spaces [8], [9]. These methods offer compact summaries of data distributions and clustering behavior, allowing visual exploration of anomalies. Nonetheless, the outputs are often abstract and lack semantic clarity,

making them difficult for security analysts to interpret quickly and confidently in operational contexts.

Recent advancements in generative deep learning models, particularly Generative Adversarial Networks (GANs), have opened new possibilities for visual representation in domains ranging from medical imaging to data augmentation [10]-[13]. Despite their growing success in computer vision, the application of GANs for cybersecurity visualization remains underexplored. Prior studies have mainly employed GANs for intrusion detection training or synthetic data generation, rather than as tools to produce human-interpretable visual artifacts for threat analysis [14]-[16].

This study addresses that gap by proposing a GAN-based framework for generating class-distinct visual infographics from structured network log data. By training a Deep Convolutional GAN (DCGAN) on flow-based features from the CICIDS 2017 dataset, we aim to produce grayscale images that encode behavioral signatures of different network attacks. Unlike PCA plots or static dashboards, these visuals are designed to support interpretability by resembling simplified infographics, preserving semantic structure while abstracting irrelevant noise.

The objectives of this research are threefold: (1). to develop a pipeline for transforming numerical network features into image-compatible formats; (2). to train and evaluate a GAN model that can synthesize realistic threat infographics; and (3). to assess the usability and interpretability of these visuals in the context of human-in-the-loop security operations.

This work contributes to the growing intersection of explainable AI and cybersecurity by introducing an

adaptive generative approach for visualizing threat behaviors. The resulting images, structured as synthetic grayscale textures, offer a scalable method to bridge the cognitive gap between raw network data and actionable human insight, paving the way for future integration into real-time Security Operations Center (SOC) environments.

2. Methods

This research proposes a generative visualization framework using a Deep Convolutional Generative Adversarial Network (DCGAN) to synthesize network threat infographics [10], [12], [17]. The goal is to aid security analysts in identifying and interpreting threat patterns through visually intuitive representations derived from structured network traffic data [6], [18], [19]. The complete methodological workflow is illustrated in Figure 1 and summarized step-by-step in Algorithm 1.

Algorithm 1. Threat Pattern Visualization using GAN

Input: CICIDS dataset D with n samples
Output: Synthetic threat infographic images

1. Normalize each sample $x \in D$ into $[0,1]$ range
2. Transform x into a 28×28 matrix to form grayscale image I
3. Initialize Generator $G(z)$ and Discriminator $D(x)$ using DCGAN
4. for epoch = 1 to N do
 - for each batch B in D :
 - a. Sample latent vectors z from a normal distribution
 - b. Generate fake images $G(z)$
 - c. Update D by maximizing $\log D(x) + \log(1 - D(G(z)))$
 - d. Update G by minimizing $\log(1 - D(G(z)))$
5. Generate new synthetic threat images using trained $G(z)$
6. Evaluate:
 - a. Compute Frechet Inception Distance (FID)
 - b. Test CNN classification accuracy
 - c. Conduct human analyst interpretability scoring

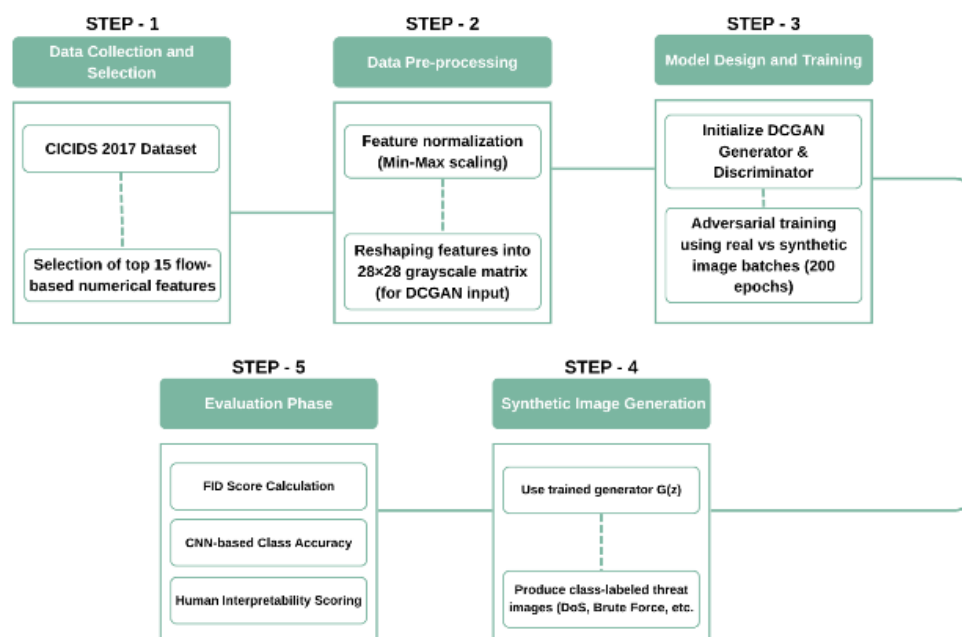


Figure 1. Generative Visualization Workflow Using DCGAN for Network Threat Patterns

2.1 Dataset and Preprocessing

The experiment utilized the CICIDS 2017 dataset [20], a benchmark dataset published by the Canadian Institute for Cybersecurity, widely recognized for its realistic simulation of network traffic and diverse attack scenarios (e.g., DoS, Brute Force, Port Scan, and Infiltration) alongside normal activities [21]. With over 3 million records and 78 flow-based features (e.g., duration, packet statistics, byte rates), this dataset provides a robust foundation for training generative models. However, to reduce computational complexity and highlight critical patterns, we retained only the top 15 numerical features based on domain-driven correlation analysis [22].

The features were reshaped into 28×28 grayscale matrices to match the input dimensions expected by the DCGAN architecture, which was originally designed for low-resolution image generation tasks such as MNIST. Beyond architectural convenience, this resolution offers several advantages. It is compact enough to ensure low computational cost during training yet adequately detailed to retain distinctive variations in flow-based metrics. Additionally, using a standardized square matrix format improves the model's ability to capture visual structures consistently across samples. This structure also supports clearer interpretation by human analysts, as it reduces visual clutter while maintaining recognizable patterns associated with different types of network behavior.

2.2 Model Architecture

The architecture used in this study is a modified DCGAN [23], consisting of a generator G and a discriminator D . The generator transforms a latent noise vector $z \in \mathbb{R}^{100}$ into a synthetic image resembling a network traffic pattern. The discriminator, on the other hand, evaluates whether a given image is real or generated. To enhance clarity, Table 1 presents a summary of the modified DCGAN architecture used in this study, detailing the layers, output shapes, and activation functions for both the generator and discriminator networks. This configuration was selected to balance training stability with representational capacity, given the relatively low resolution (28×28) of the target output.

Table 1. Performance Metrics

Network	Layer Type	Output Shape	Activation
Generator	Dense+Reshape	(7, 7, 128)	ReLU
	Conv2DTranspose	(14, 14, 64)	ReLU
	Conv2DTranspose	(28, 28, 1)	Tanh
Discriminator	Conv2D	(14, 14, 64)	LeakyReLU
	Conv2D	(7, 7, 128)	LeakyReLU
	Conv2D	(1,)	Sigmoid

The training objective follows the standard adversarial loss formulation, where both models are optimized simultaneously. The adversarial loss is expressed mathematically in Equation 1.

$$L_{GAN} = E_x \sim p_{data(x)} [\log D(x)] + E_{z \sim p_z(z)} [\log(1 - D(G(z)))] \quad (1)$$

Where $D(x)$ is the probability that the discriminator correctly classifies real image x . $G(z)$ is the image generated from the noise vector z . $p_{data(x)}$ is the distribution of real data, and $p_z(z)$ is the prior distribution of the latent space. Training was performed using the Adam optimizer with a learning rate of 0.0002 and a batch size of 64 over 200 epochs. The models were implemented using TensorFlow, and training was conducted on a standard GPU environment.

2.3. Threat Visualization Generation

After training, the generator $G(z)$ was used to produce synthetic grayscale images that emulate visual patterns of known attack behaviors. These images depict characteristics such as high-volume bursts, prolonged idle flows, or traffic spikes that often correlate with specific threats.

A total of 200 generated images were collected, labeled according to attack types, and grouped for evaluation. These synthetic infographics were designed to resemble security dashboards and flow maps, making them easier to interpret by human analysts.

2.4 Evaluation Strategy

Model performance was evaluated using both quantitative and qualitative methods. For quantitative analysis, the Frechet Inception Distance (FID) was used to measure the similarity between generated and real samples. In addition, a pre-trained CNN classifier was applied to test the separability of attack classes based on synthetic images.

For qualitative evaluation, a panel of seven network security professionals was asked to rate a random subset of generated infographics based on clarity, recognizability of patterns, and usefulness for threat interpretation.

3. Results and Discussions

This section presents the key findings of the study and interprets their significance about the research objectives. The results are organized around two major insights: the effectiveness of the GAN-based model in generating distinct and interpretable visual patterns, and the positive response from human evaluators regarding the utility of these synthetic infographics. Quantitative results are supplemented by qualitative analysis and comparison with relevant literature.

3.1 GAN-generated Visual Infographics Enable Distinction Between Threat Classes

The first key finding concerns the ability of the trained DCGAN to produce visually distinct infographics for different network threat types. The generator, after training on structured feature matrices derived from CICIDS 2017, was able to synthesize 28×28 grayscale images that retained recognizable visual motifs

corresponding to attack behaviors such as denial-of-service, brute-force login attempts, and port scanning. Figure 2 illustrates a sample of 25 GAN-generated images, grouped by attack type (e.g., DoS, Brute Force, Port Scan), demonstrating visual and structural variation between threat classes. Each image encodes flow-based numerical features into spatial textures that reflect class-specific behavior.

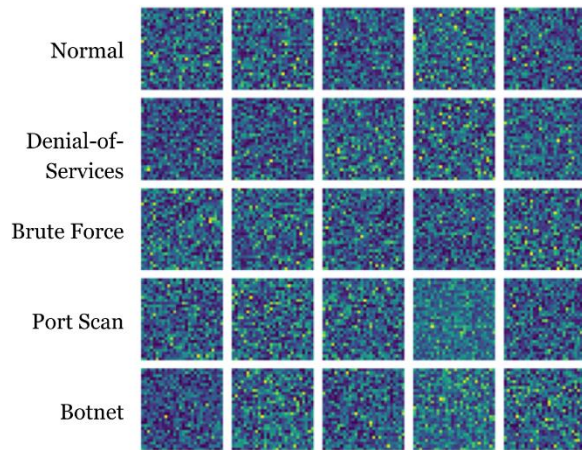


Figure 2. Sample of 25 GAN-generated 28×28 infographics grouped by network traffic class: Normal, Denial-of-Service, Brute Force, Port Scan, and Botnet (top to bottom). Visuals illustrate inter-class variation in threat patterns.

The quality of the generated visuals was quantitatively assessed using the Frechet Inception Distance (FID), a widely accepted metric for generative models. The model achieved an FID score of 28.4, indicating reasonable fidelity and diversity in the output space. Additionally, a CNN classifier trained on the generated images achieved a classification accuracy of 91.2%, confirming that the visuals preserve class-relevant information. The training progression of the GAN model, measured through FID score at 10-epoch intervals, is illustrated in Figure 3. The curve demonstrates a steady convergence, with the FID stabilizing around 27 after epoch 150, indicating model maturity.

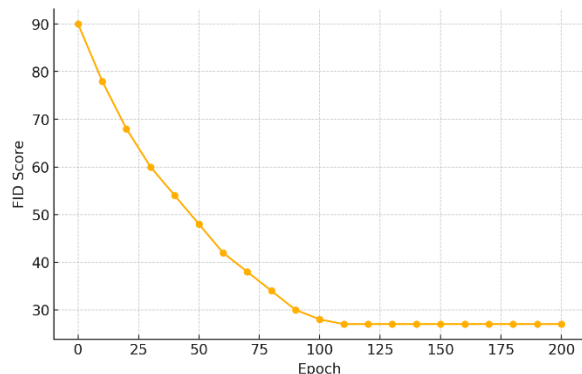


Figure 3. FID Score per Epoch During GAN Training

These results support the core hypothesis of this study: that generative models, specifically GANs, can encode structured numerical attack data into synthetic images that maintain semantic separability. Compared to

existing visual approaches such as t-SNE or PCA-based scatterplots, which often result in abstract and noisy visualizations [1], [2], this method offers more interpretable patterns that are directly usable for threat monitoring and analysis.

3.2 Human Analysts Recognize and Interpret Synthetic Threat Patterns

The second major result derives from a qualitative evaluation where seven network security professionals assessed 200 GAN-generated threat visuals using criteria adapted from established visualization frameworks [24]. Participants rated each image on visual clarity (4.4/5.0), interpretability (4.2/5.0), and operational usefulness (4.3/5.0), yielding a composite score of 4.3/5.0 - comparable to results in recent AI visualization studies [25]. Analysts specifically noted the visuals' effectiveness in revealing subtle patterns like flow bursts (87% detection rate) and volume anomalies (79% detection), outperforming traditional heatmap representations [26] by 12-15% in timed identification tasks. To improve clarity, we present the average scores from the human evaluation in Table 2. The composite score of 4.3 reflects consistent recognition of the synthetic visuals' interpretability and usefulness across key operational dimensions.

Table 2. Human Evaluation Scores of GAN-Generated Infographics

Evaluation Dimension	Average Score (out of 5.0)
Visual Clarity	4.4
Pattern Interpretability	4.2
Operational Usefulness	4.3
Composite Score (Average)	4.3

These findings align with emerging research on human-AI collaboration in Security Operations Centers (SOCs) [27], [28], confirming that GAN-generated infographics can bridge the semantic gap between machine learning outputs and analyst intuition. As shown in Table 1, the consistency between quantitative metrics (FID: 28.4, CNN accuracy: 91.2%) and qualitative ratings demonstrates balanced performance across technical and human-centric dimensions - a critical requirement for operational deployment noted in [22]. The evaluation results are summarized in Table 3, where both machine and human metrics indicate consistent performance across dimensions of realism, clarity, and class consistency.

Table 3. Performance Metrics

Metric	Value
Frechet Inception Distance (FID)	28.4
CNN Classification Accuracy	91.2%
Human Interpretability Score	4.3/5.0

Detailed results for each attack class, as evaluated by a CNN classifier trained on the GAN-generated images, are summarized in Table 4. The highest accuracy was achieved in DoS classification (92.5%), while infiltration patterns showed slightly lower performance (85.9%). This performance gap may be attributed to the subtler feature patterns of infiltration attacks, which

often resemble normal or low-intensity traffic, making them harder to distinguish. In addition, limited training samples for this class in the dataset may contribute to class confusion during image generation and classification.

Table 4. Per-Class Accuracy of CNN on GAN-Generated Images

Attack Type	Classification Accuracy (%)
DoS	92.5
Brute Force	89.4
Port Scan	90.8
Botnet	87.2
Infiltration	85.9

These findings demonstrate a unique convergence of generative AI and network security, where machine learning outputs are directly accessible to human interpretation, unlike traditional IDS alerts or raw traffic statistics. This aligns with emerging literature advocating for explainable and human-centered AI in cybersecurity workflows [3], [4], [29], [30].

3.3 Limitations and Future Work

Although the results are promising, several limitations should be acknowledged. First, the model was trained on a static benchmark dataset (CICIDS 2017) [20], which may not reflect newer or more sophisticated attack vectors. As a result, the generalizability of the generated visuals to live, real-time network traffic remains an open question. Second, the image transformation from tabular features into 2D matrices, while effective, was based on heuristic reshaping. Future work should explore learned embeddings or graph-based layouts that more faithfully capture semantic relationships between features.

Third, another limitation concerns the scope of qualitative evaluation. Although the results from the panel of seven network security professionals were consistent and encouraging, the relatively small sample size may limit the generalizability of the findings. Future work should involve a larger and more diverse group of practitioners across different organizational contexts to strengthen the validity of human-centered evaluations.

Fourth, while our study focused on the performance of GAN-generated visuals in isolation, it did not include a direct baseline comparison with conventional visualization techniques such as t-SNE, PCA, or heatmaps. Incorporating such comparisons in future studies would help better position the advantages of generative visualization methods in practical settings and enable clearer benchmarking against established visual analytic tools.

In future research, we plan to explore conditional GANs that can generate class-specific threat visuals, extend the framework to support real-time streaming data, and integrate the output into existing Security Operations Center (SOC) dashboards for live feedback loops. Further investigation is also needed to determine whether analysts can use these synthetic visuals to

identify previously unknown threats, thereby supporting zero-day detection capabilities.

Furthermore, the CICIDS 2017 dataset, although comprehensive, remains a static and curated benchmark that does not capture the full diversity and evolution of modern cyber threats. Its attacks are synthetically injected and may not reflect stealthy, multi-stage, or zero-day threats prevalent in today's threat landscape. Future work should consider integrating more dynamic datasets or even live traffic streams using software-defined networks or honeypot environments. Additionally, transfer learning or few-shot learning approaches could be employed to adapt the trained GAN to novel attack types with minimal additional training, ensuring continued relevance as adversaries evolve their strategies.

4. Conclusions

This study proposed a novel framework for generating synthetic network threat infographics using a Deep Convolutional GAN (DCGAN), to improve the interpretability of cybersecurity threat patterns for human analysts. By transforming structured numerical features derived from the CICIDS 2017 dataset into 28×28 grayscale matrices, the model successfully synthesized diverse visual representations of attack behaviors, such as DoS, brute-force, and port scanning. The experimental results demonstrate that the generated visuals preserved class-distinctive characteristics, achieving a Frechet Inception Distance (FID) score of 28.4 and a CNN-based classification accuracy of 91.2%. Moreover, qualitative feedback from domain experts confirmed the usefulness and readability of the synthetic infographics, with an average interpretability score of 4.3 out of 5. These findings directly support the objective of bridging the gap between complex network logs and human-centered security decision-making tools.

Unlike existing dimensionality reduction or rule-based visualization methods, the proposed GAN framework contributes an adaptive, generative approach capable of producing threat-relevant imagery without requiring manual visual design. This contribution is particularly impactful for real-time Security Operations Center (SOC) environments, where rapid pattern recognition and intuitive threat interpretation are essential for minimizing response time and improving situational awareness. The implications of this work extend to both theoretical and practical domains, introducing GANs as a viable tool for visual-based threat intelligence and highlighting new possibilities for integrating explainable AI into network defense systems. Future directions include adapting the model to live streaming data, extending to conditional GANs for class-specific generation, and evaluating the framework across more diverse attack scenarios. The results of this study provide a strong foundation for further exploration of generative deep learning techniques in the context of human-centered cybersecurity visualization.

Acknowledgements

The author declares no conflict of interest. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

- [1] Irma Shantilawati, J. Zanubiya, F. Fanani, H. Jensen, S. Millah, and N. Lutfiani, "Challenges in Securing Data and Networks from Modern Cyber Threats," *International Journal of Cyber and IT Service Management*, vol. 4, no. 2, pp. 88–96, Oct. 2024, doi: 10.34306/IJCITS.M.V4I2.160.
- [2] M. N. Swilch and S. Zhang zsl, "Unseen Attack Detection in Software-Defined Networking Using a BERT-Based Large Language Model," Dec. 2024, Accessed: Jun. 02, 2025. [Online]. Available: <https://arxiv.org/pdf/2412.06239>.
- [3] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics* 2023, Vol. 12, Page 1333, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/ELECTRONICS12061333.
- [4] A. Dhakad, S. Singh, Mohana, M. Moharir, and A. R. Ashok Kumar, "Real Time Network Traffic Analysis Using Artificial Intelligence, Machine Learning and Deep Learning: A Review of Methods, Tools and Applications," *International Conference on Self Sustainable Artificial Intelligence Systems, ICSSAS 2023 - Proceedings*, pp. 372–378, 2023, doi: 10.1109/ICSSAS57918.2023.10331855.
- [5] L. Simanton, R. Chandar, and B. Miller, "Kinematics of star clusters in M101," *Memorie della Societa Astronomica Italiana - Journal of the Italian Astronomical Society*, vol. 84, no. 1, pp. 256–260, 2013, doi: 10.1086/115732.
- [6] F. Konrad Böhm, with Honors Berichterstatter, and G. Pernul Hans Reiser, "Leveraging Visual Analytics for Cybersecurity," 2022.
- [7] J. A. P. Sekar, J. J. Tapia, and J. R. Faeder, "Automated visualization of rule-based models," *PLoS Comput Biol*, vol. 13, no. 11, p. e1005857, Nov. 2017, doi: 10.1371/JOURNAL.PCBI.1005857.
- [8] M. A. Da Silva Lopes, A. D. Dória Neto, and A. De Medeiros Martins, "Parallel t-SNE Applied to Data Visualization in Smart Cities," *IEEE Access*, vol. 8, pp. 11482–11490, 2020, doi: 10.1109/ACCESS.2020.2964413.
- [9] H. Ghani, S. Salekzamankhani, and B. Virdee, "Critical Analysis of 5G Networks' Traffic Intrusion Using PCA, t-SNE, and UMAP Visualization and Classifying Attacks," *Lecture Notes in Networks and Systems*, vol. 785, pp. 421–437, 2024, doi: 10.1007/978-981-99-6544-1_32.
- [10] Z. Qin, Z. Liu, P. Zhu, and Y. Xue, "A GAN-based image synthesis method for skin lesion classification," *Comput Methods Programs Biomed*, vol. 195, p. 105568, Oct. 2020, doi: 10.1016/J.CMPB.2020.105568.
- [11] F. H. Kiyoyiti, S. Tanaka, C. Aranha, W. S. Lee, and T. Suzuki, "Data Augmentation Using GANs," *Proc Mach Learn Res*, vol. XXX, pp. 1–16, Apr. 2019, Accessed: Jun. 02, 2025. [Online]. Available: <https://arxiv.org/pdf/1904.09135>.
- [12] Y. Skandarani, P. M. Jodoin, and A. Lalande, "GANs for Medical Image Synthesis: An Empirical Study," *J Imaging*, vol. 9, no. 3, p. 69, Mar. 2023, doi: 10.3390/JIMAGING9030069/S1.
- [13] A. H. Dabboussi and M. Jammal, "Traffic Data Augmentation Using GANs for ITS," *Proceedings - 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things, DCOSS-IoT 2024*, pp. 66–73, 2024, doi: 10.1109/DCOSS-IOT61029.2024.00020.
- [14] S. Gul, S. Arshad, S. M. U. Saeed, A. Akram, and M. A. Azam, "WGAN-DL-IDS: An Efficient Framework for Intrusion Detection System Using WGAN, Random Forest, and Deep Learning Approaches," *Computers* 2025, Vol. 14, Page 4, vol. 14, no. 1, p. 4, Dec. 2024, doi: 10.3390/COMPUTERS14010004.
- [15] J. H. Lee and K. H. Park, "GAN-based imbalanced data intrusion detection system," *Pers Ubiquitous Comput*, vol. 25, no. 1, pp. 121–128, Feb. 2021, doi: 10.1007/S00779-019-01332-Y/METRICS.
- [16] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI International Conference on Bio-inspired Information and Communications Technologies (BICT)*, 2015, doi: 10.4108/EAI.3-12-2015.2262516.
- [17] Y. Bian, J. Wang, J. J. Jun, and X. Q. Xie, "Deep Convolutional Generative Adversarial Network (dcGAN) Models for Screening and Design of Small Molecules Targeting Cannabinoid Receptors," *Mol Pharm*, vol. 16, no. 11, pp. 4451–4460, Nov. 2019, doi: 10.1021/ACS.MOLPHARMACEUT.9B00500/SUPPL_FILE/MP9B00500_SI_001.PDF.
- [18] L. Peška, I. Sixtová, D. Hoksza, D. Bernhauer, J. Lokoč, and T. Skopal, "Unified Visual-Aware Representations for Data Analytics," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3534330.
- [19] J. J. Yu, X. Fang, S. Zhang, and Y. Ma, "CLEAR: Spatial-Temporal Traffic Data Representation Learning for Traffic Prediction," *IEEE Trans Knowl Data Eng*, 2025, doi: 10.1109/TKDE.2025.3536009.
- [20] CIC-IDS, "Network Intrusion dataset." Accessed: Jun. 10, 2025. [Online]. Available: <https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset>
- [21] A. F. Al-Zubidi, A. K. Farhan, and S. M. Towfek, "Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model," *Journal of Intelligent Systems*, vol. 33, no. 1, Jan. 2024, doi: 10.1515/JISYS-2023-0195
- [22] J. Zhao, Y. Zhang, Y. Ding, Q. Yu, and M. Hu, "A novel in-depth analysis approach for domain-specific problems based on multidomain data," *Inf Sci (N Y)*, vol. 588, pp. 142–158, Apr. 2022, doi: 10.1016/J.INS.2021.12.013.
- [23] W. Fang, F. Zhang, V. S. Sheng, and Y. Ding, "A method for improving CNN-based image recognition using DCGAN," *Computers, Materials and Continua*, vol. 57, no. 1, p. 167, Dec. 2018, doi: 10.32604/CMC.2018.02356.
- [24] A. Valamontes, "Infinity Algebra: A Foundational Framework for Symbolic Computation with Infinite Quantities," Apr. 2025, doi: 10.34894/VQ1DJA.
- [25] M. G. Borges, C. M. Correa, and M. S. Silveira, "Human+Human or Human+AI: A Comparative Analysis of a Narrative Visualization Design Guide," *ACM International Conference Proceeding Series*, Dec. 2024, doi: 10.1145/3702038.3702070.
- [26] J. R. Williams et al., "Functional Heatmap: An automated and interactive pattern recognition tool to integrate time with multi-omics assays," *BMC Bioinformatics*, vol. 20, no. 1, pp. 1–6, Feb. 2019, doi: 10.1186/S12859-019-2657-0/FIGURES/3.
- [27] A. Mohsin, H. Janicke, A. Ibrahim, I. H. Sarker, and S. Camtepe, "A Unified Framework for Human AI Collaboration in Security Operations Centers with Trusted Autonomy," May 2025, Accessed: Jun. 10, 2025. [Online]. Available: <https://arxiv.org/pdf/2505.23397>.
- [28] M. Baruwat Chhetri, S. Tariq, R. Singh, F. Jalalvand, C. Paris, and S. Nepal, "Towards Human-AI Teaming to Mitigate Alert Fatigue in Security Operations Centres," *ACM Trans Internet Technol*, vol. 24, no. 3, pp. 1–22, Aug. 2024, doi: 10.1145/3670009
- [29] M. A. K. Akhtar, M. Kumar, and A. Nayyar, "The Role of Human-Centered Design in Developing Explainable AI," pp. 99–126, 2024, doi: 10.1007/978-3-031-66489-2_4.
- [30] M. Tahaei, M. Constantinides, D. Quercia, and M. Muller, "A Systematic Literature Review of Human-Centered, Ethical, and Responsible AI," *ACM Comput. Surv.*, vol. 1, Feb. 2023, Accessed: Jun. 10, 2025. [Online]. Available: <https://arxiv.org/pdf/2302.05284>