

Research Article

A Data Mining Framework for Network Intrusion Detection Using GAN-Augmented Traffic Data

Zainab Zaidon Kareem

Sunni Endowment Office, Department of Religious Education and Islamic Studies, Educational Research Section, Baghdad, Iraq.

Abstract | Data mining techniques play an important role in extracting meaningful patterns from large-scale network traffic data for Intrusion Detection Systems (IDS). But the effectiveness of traditional machine learning models is often limited by data imbalance, noisy features, and insufficient representation of rare attack classes. This study investigates an enhanced IDS framework that combines data mining techniques with Generative Adversarial Networks (GANs) for generating synthetic data. The UNSW-NB15 dataset is used, and a data mining pipeline is applied, including preprocessing, feature encoding, normalization, and class balancing. The study evaluates multiple classification algorithms, including Random Forest, K-Nearest Neighbors (KNN), and Decision Tree, under two scenarios: Before and after data augmentation using a GAN. In the first scenario, models are trained using standard data mining preprocessing on the original imbalanced dataset. In the second scenario, GANs are integrated into the data mining pipeline to generate synthetic samples and improve class distribution. The results appear that data mining combined with GAN significantly improves classification performance. Random Forest and Decision Tree achieve approximately 99% accuracy after GAN integration, while KNN improves to 88%. Overall, the findings ensure that combining advanced data mining techniques with GAN-based augmentation enhances pattern discovery and strengthens IDS performance in detecting diverse cyber-attacks.

Received | May 16, 2026; **Accepted** | May 22, 2026; **Published** | September 01, 2026

***Correspondence** | Zainab Zaidon Kareem, Sunni Endowment Office, Department of Religious Education and Islamic Studies, Educational Research Section, Baghdad, Iraq; **Email:** zainab.zaidon@taleemdeny.edu.iq

Citation | Kareem, Z.Z., 2026. A data mining framework for network intrusion detection using GAN-Augmented traffic data. *Smart Technologies in Science and Engineering*, 1(2): 134-142.

Keywords | Data mining, Machine learning models, IDS, GAN-augmented traffic data



Copyright: 2026 by the authors. Licensee ResearchersLinks Ltd, England, UK.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Introduction

In the network security domain, there are three categories of Network Intrusion Detection Systems (NIDS): Signature-based, anomaly-based, and hybrid systems. Signature-based NIDS detects malicious activities by comparing incoming traffic with previously identified attack patterns, rules, or

fingerprints stored in a database. When network behavior matches a stored pattern, the system detects malicious activity and sends an alert. This approach is highly efficient for known threats with low computational overhead and fast response time. But it has a major limitation: the inability to detect zero-day attacks, evolving malware variants, or previously unseen intrusion techniques that do not yet exist in the

signature database (Ahmad *et al.*, 2021). The second category is anomaly-based NIDS. These systems learn legitimate network behavior from historical traffic patterns, then continuously monitor new traffic to identify malicious activity from normal activity. Malicious activities may indicate denial-of-service attacks, botnet behavior, or unauthorized access. Anomaly-based detection has high performance because it can identify unknown and emerging threats without depending on predefined attack signatures. Some of these systems often generate higher false-positive rates, requiring careful threshold tuning and demanding significant processing resources when deployed in real-time environments (Thakkar and Lohiya, 2022). Anomaly-based systems are similar to classification tasks. While anomaly detection focuses on determining whether traffic is suspicious, classification aims to classify that suspicious traffic into specific categories, such as DoS, reconnaissance, exploits, or brute-force attacks. Classification models such as Random Forests, Decision Trees, K-Nearest Neighbors, and Support Vector Machines are widely used for this purpose. Overall, combining anomaly detection with classification provides security administrators with more actionable intelligence, as the system not only detects abnormal behavior but also explains the likely nature of the attack (Chindove and Brown, 2021). The third category is a hybrid NIDS that integrates two systems, signature-based and anomaly-based techniques, into one centralized framework. Hybrid systems benefit from the strengths of both methods: Rapid identification of known threats via signatures and detection of unknown threats via behavioral analysis. In conclusion, this combination often enhances detection accuracy by reducing false alarms and increasing adaptability in dynamic network environments such as cloud systems, IoT networks, and cyber-physical infrastructures (Binbusayyis and Vaiyapuri, 2021). In recent years, Generative Adversarial Networks (GANs) have demonstrated a powerful machine learning approach for improving intrusion detection systems. It includes two competing neural networks: a generator that produces synthetic samples and a discriminator that distinguishes between generated and real data. Through this adversarial learning process, GANs can generate realistic synthetic network traffic records that closely match the original datasets (Injadat *et al.*, 2020). In intrusion detection research, GANs are primarily used to address one of the most common challenges in cybersecurity datasets, such as class imbalance.

Many datasets consist of many normal traffic samples but relatively few examples of rare attacks, such as reconnaissance, shellcode, or worms. This imbalance makes classifiers become biased toward majority classes. Using GANs to generate attack samples can rebalance the training dataset, enabling machine learning models to learn minority attack patterns more effectively (Tama and Lim, 2021). Also, GANs can enhance robustness by generating adversarial traffic samples that simulate real attackers; training classifiers on these adversarial samples can strengthen resilience against sophisticated cyberattacks. In addition, advanced tabular GAN models, such as CTGAN, are particularly well-suited for structured intrusion detection datasets because they preserve relationships among categorical and numerical traffic features (Yang *et al.*, 2021). Therefore, integrating data mining classifiers with GAN-augmented traffic data provides a modern and effective direction for intrusion detection research. Machine learning models serve as classification models, while GANs enhance data quality, improve recognition of minority attacks, and increase the overall reliability of IDS performance in realistic network environments (Lee and Park, 2021).

This study proposes a data-mining-based intrusion-detection framework that leverages GAN-augmented network traffic data to improve multi-class cyberattack detection on the UNSW-NB15 dataset. The proposed model addresses class imbalance, enhances minority-attack recognition, compares multiple classifiers, and evaluates the practical effectiveness of synthetic traffic generation in modern IDS environments.

Related work

NIDS are critical cybersecurity tools used to identify malicious traffic and unauthorized activities in computer networks. There are recent studies on implementing NIDS to enhance security by detecting threats. The authors proposed a GAN-based intrusion detection framework to address the challenge of imbalanced attack classes. Their study showed that GAN-generated traffic samples improved IDS performance and outperformed traditional oversampling methods such as SMOTE (Zhang and Liu, 2022). This study introduced G-IDS, in which GAN-generated synthetic samples were merged with the NSL-KDD dataset before classifier training. The results showed that the GAN-enhanced IDS achieved higher detection rates than conventional standalone IDS models (Bourou *et al.*,

2021) proposed multiple tabular GAN architectures, including CTGAN, CopulaGAN, and TableGAN, for generating synthetic DoS attack records using the NSL-KDD dataset. Their findings confirmed that synthetic data preserved useful statistical patterns and improved machine learning model training (Patil *et al.*, 2022) developed a BiGAN-based anomaly detection framework combined with Principal Component Analysis (PCA) using the KDD Cup 99 dataset. The findings showed that the proposed model achieved strong detection performance compared with several deep learning baselines. Truong-Huu *et al.* (2020) evaluated two GAN models with customized generator and discriminator networks using CICIDS2017 and UNSW-NB15. The experiments showed that GAN-based unsupervised learning can effectively detect abnormal traffic patterns. Mustapha *et al.* (2023) proposed an adversarial neural network approach to generate perturbed DDoS samples that resemble benign traffic. The results showed that adversarially modified traffic significantly reduced the IDS's detection capability. Lin *et al.* (2022) introduced IDSGAN, a GAN-based framework that transforms malicious traffic into benign-like traffic while preserving attack functionality. Their generated adversarial traffic successfully evaded black-box IDS models. Similarly, this study (Chauhan and Heydari, 2020) proposed a polymorphic adversarial DDoS attack generation model using a GAN, in which attack features were dynamically modified to bypass IDS detection. Liu *et al.* (2022) employed two augmentation approaches, namely Variational Autoencoder (VAE) and Conditional VAE (CVAE), to improve IDS classification performance. Their study confirmed that synthetic data generation enhanced minority attack recognition and overall

generalization. Finally, (Tabassum *et al.*, 2022) proposed Fed GAN-IDS, which combines federated learning with GAN-based data generation to preserve privacy while collaboratively training distributed intrusion detection systems.

As shown in Table 1, although previous studies have shown promising results in applying GANs to intrusion detection systems, several important research gaps remain. Many studies relied on outdated benchmark datasets, such as KDD Cup 99, NSL-KDD, and older traffic collections. While these datasets are useful for comparison, they do not fully represent modern network environments, including encrypted traffic, IoT devices, and recent cyberattacks. Several studies mainly evaluated GANs based on their ability to generate synthetic data, without fully measuring how much the generated samples improve downstream IDS classifier performance. Many IDS studies focused on binary classification, classifying traffic as normal or attack, rather than identifying specific attack categories such as DoS, Botnet, Port Scan, Web Attack, and DDoS. Multi-class detection is more practical for real security operations. Several previous evaluations of system performance have focused on accuracy, but in intrusion detection, metrics such as Precision, Recall, F1-score, ROC-AUC, False Positive Rate, and confusion matrix analysis are also essential.

Materilas and Methods

This study designs and implements a GAN-based approach to improve the accuracy of an intrusion detection system. The main pipelines of the proposed methodology are shown in Figure 1.

Table 1: *Summary of related works.*

No.	Reference	Dataset	Methodology	Main Contribution
1	(Lee and Park, 2021)	IDS benchmark datasets	GAN + IDS	Solved class imbalance
2	(Zhang and Liu, 2022)	NSL-KDD	ANN-GAN + IDS	Improved detection accuracy
3	(Bourou <i>et al.</i> , 2021)	NSL-KDD	CTGAN, CopulaGAN, TableGAN	Synthetic DoS generation
4	(Patil <i>et al.</i> , 2022)	KDD Cup 99	PCA + BiGAN	Enhanced anomaly detection
5	(Truong-Huu <i>et al.</i> , 2020)	CICIDS2017, UNSW-NB15	Dual GAN models	Unsupervised IDS
6	(Mustapha <i>et al.</i> , 2023)	DDoS traffic	Adversarial GAN	Tested IDS robustness
7	(Lin, 2022)	Network traffic data	IDSGAN	Generated evasive attacks
8	(Chauhan and Heydari, 2020)	DDoS traffic	GAN adversarial attack	IDS evasion testing
9	(Liu <i>et al.</i> , 2022)	IDS datasets	VAE / CVAE	Better minority detection
10	(Tabassum <i>et al.</i> , 2022)	Distributed IDS data	FedGAN + FL	Privacy-preserving IDS

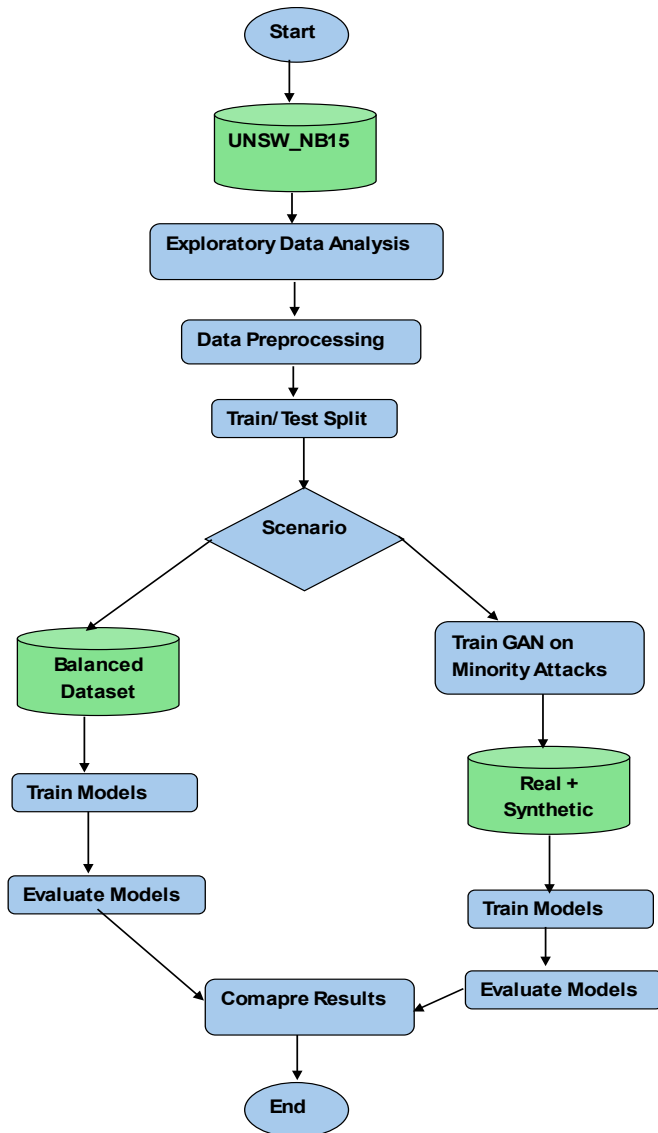


Figure 1: Methodology.

Dataset

In this study, the UNSW-NB15 dataset was selected because it is considered one of the modern and realistic benchmark datasets for cybersecurity research. Unlike older datasets; UNSW-NB15 includes contemporary attack behaviors and legitimate traffic patterns, making it more suitable for evaluating machine learning and deep learning intrusion detection models. It contained 257,673 network records with 45 attributes (Kaggle, 2024).

The important features are defined as shown in Table 2. Protocol and service features help distinguish attack communication types. Packet and byte statistics reveal flooding or scanning activities. Timing and jitter features identify suspicious traffic irregularities. Connection-counting features help detect malicious repeated attempts. Attack labels are required for supervised learning classification, which is the target

feature.

Table 2: Dataset samples.

Feature	Type	Description
dur	float64	Connection duration
proto	Object	Protocol type
service	Object	Requested service
state	Object	Connection state
spkts	int64	Packets from source
dpkts	int64	Packets from destination
sbytes	int64	Bytes from source
dbytes	int64	Bytes from destination
rate	float64	Transaction rate
sttl	int64	Source TTL
dttl	int64	Destination TTL
sload	float64	Source load
dload	float64	Destination load
sinpkt	float64	Source inter-packet time
dinpkt	float64	Destination inter-packet time
sjit	float64	Source jitter
djit	float64	Destination jitter
tcprtt	float64	TCP round trip time
ct_srv_src	int64	Same service from source
ct_dst_ltm	int64	Recent same destination
attack_cat	object	Attack category
label	int64	0=Normal, 1=Attack

Data analysis

In this phase, identify the different categories of network traffic represented in the target variable in the UNSW-NB15. As shown in Figure 2, 10 traffic classes were identified, including 1 normal traffic category and 9 attack categories: Normal, Reconnaissance, Backdoor, DoS, Exploits, Analysis, Fuzzers, Worms, Shellcode, and Generic. The frequency distribution for each attack appears to be class-imbalanced. This imbalance may negatively affect the learning of classification models, leading to biased predictions toward the majority classes and a weak ability to detect rare attacks. To simplify the multi-class classification task and focus on the most representative categories, six major classes were selected: Normal, Generic, Exploits, Fuzzers, DoS, and Reconnaissance (Yang et al., 2021). The six selected classes used in this study represent the most common and informative traffic categories in the UNSW-NB15 dataset. These types are Normal, which refers to legitimate network traffic generated by authorized users and standard system operations,

without malicious behavior. Generic represents exploits encryption mechanisms through brute-force or hash-cracking techniques. Exploits exploit software vulnerabilities to gain unauthorized access and disrupt systems. Fuzzers sent random input data to applications or services to discover vulnerabilities and trigger failures. DoS (Denial of Service) describes attacks designed to overwhelm network resources or services, making them unavailable to legitimate users by sending huge amounts of traffic from a single source. Reconnaissance involves scanning networks to identify open ports and collect system details before launching further attacks.

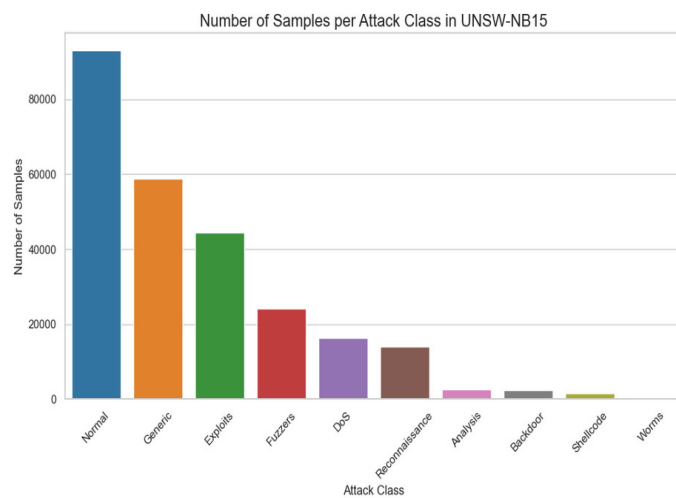


Figure 2: Attack categories.

Data preprocessing

To improve dataset quality and enhance model performance, several preprocessing steps are applied. Scale numerical features to normalize the feature space and improve model performance. Split the dataset into training and testing sets using an 80:20 stratified split to preserve class distribution across both sets. Train a GAN model on the minority classes to generate synthetic network traffic samples. A combination of the synthetic data with the original dataset to form an augmented dataset. The class distribution was rebalanced by applying up-sampling to ensure equal representation across all attack categories. Encode label to prepare data for machine learning models.

Train GAN on minority classes

To address class imbalance, this study employed a GAN that focused on the minority classes in the dataset. During this stage, only underrepresented attack categories such as Fuzzers, DoS, and Reconnaissance were selected to train the GAN model. The main objective of the GAN model is to learn the

underlying data distribution of these minority classes and generate realistic synthetic samples that resemble real network traffic patterns. The GAN model consists of a generator that generates synthetic data and a discriminator that distinguishes between real and synthetic samples. Through adversarial training, both components improve iteratively, enabling the generator to produce high-quality synthetic records that preserve statistical properties of the original minority data. Once training is complete, the GAN generates additional synthetic samples to improve the representation of minority classes. This approach helps reduce class imbalance, increase dataset diversity, and improve machine learning models' ability to learn discriminative patterns from previously underrepresented attack categories (Liu *et al.*, 2022).

Train models

In this study, several machine learning models are trained, including Random Forest, K-Nearest Neighbors (KNN), and Decision Tree. There are two scenarios for training: in the first, train models on downsampled, balanced datasets of attackers; in the second, train models on balanced, synthetic data generated using a GAN. This approach allowed the models to learn more representative decision boundaries across all attack categories (Yang *et al.*, 2021).

Train models

The performance of the machine learning models was evaluated using several metrics, including accuracy, classification reports, and normalized confusion matrices. Accuracy is the ratio of correctly classified instances to the total number of instances in the dataset and provides an overall measure of model performance. The classification report provides a more detailed evaluation by presenting several metrics such as precision, recall, and F1-score for each class. It summarises performance across all classes equally, proportional to each class's support. The normalized confusion matrix is a visualization tool for evaluating classification performance at the class level. Unlike a standard confusion matrix, the normalized version presents values as percentages rather than raw counts, enabling better interpretation of how well each class is correctly predicted. Each row corresponds to the actual class, while each column represents the predicted class. It benefits from identifying misclassification patterns, such as confusion between similar attack types or bias toward majority classes. Finally, comparing results

between two scenarios: before GAN was used and after GAN was used, to show the enhancement and the effectiveness of applying GAN.

Results

In this section, the study presents results for two scenarios: The first before using GAN and the second after using GAN.

Scenario before using GAN

Based on the normalized confusion matrix shown in Figure 3, the random forest model achieves strong classification performance with an accuracy of 87.58%. The results indicate that the model classified the normal and generic classes very effectively, with most samples correctly predicted and recall values close to 0.98. Meaning that the majority of benign traffic and generic attack records were correctly recognized with minimal confusion. On the other hand, the model achieved acceptable performance for exploits, Fuzzers, and reconnaissance classes, with diagonal values in the normalized confusion matrix ranging from 0.77 to 0.80. Suggesting that moderate consistency in identifying these attack categories, although some misclassification occurred between similar intrusion types. The main weakness in the normalized confusion matrix was the DoS class, which had the lowest diagonal value at approximately 0.39. Meaning only 39% of actual DoS samples were correctly classified, while the remaining samples were incorrectly assigned to other categories. Suggesting that the model had difficulty distinguishing DoS traffic patterns from similar attacks (Liu et al., 2022).

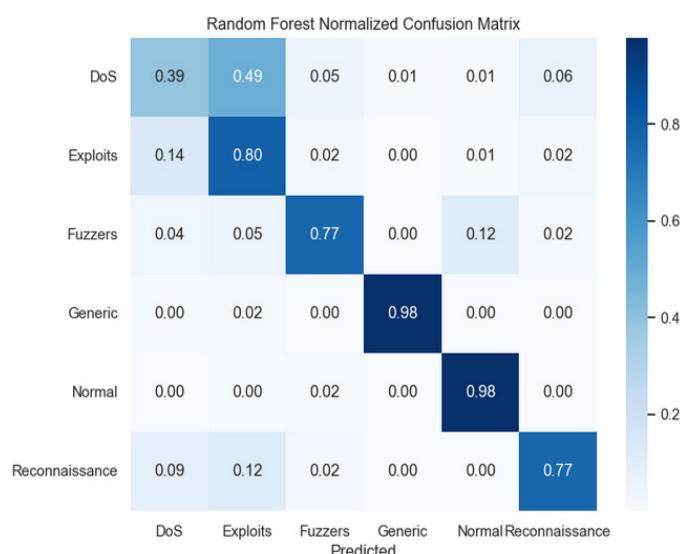


Figure 3: Normalize the confusion matrix for Random Forest.

As shown in Figure 4, the KNN model achieved an overall accuracy of 80.82%, which is lower than that of the random forest model. The matrix indicates that most legitimate network traffic was accurately recognized. But for the exploits class, the model achieved a moderate recall of 0.70, suggesting reasonable classification capability. Also, for both Fuzzers and reconnaissance classes, the model achieved only 0.55 recall, meaning nearly half of their samples were misclassified into other categories. The weakest performance was observed in the DoS class, with a recall of 0.37 and a precision of 0.35. Meaning a large portion of DoS attacks were incorrectly predicted as other classes, while many predicted DoS samples were false positives. Overall, the results indicate that KNN struggled to learn clear decision boundaries for this minority or overlapping class (Patil et al., 2022).

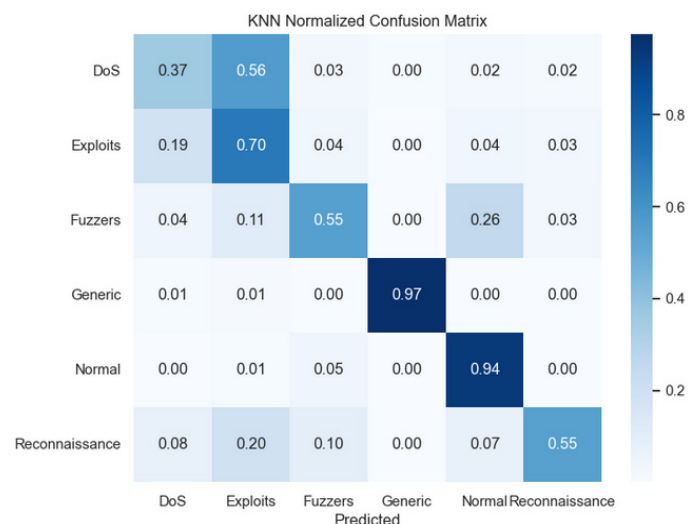


Figure 4: Normalize the confusion matrix for KNN.

Based on the normalized confusion matrix in Figure 5, the DT model achieved an overall accuracy of 87.56%, ranking among the best-performing models in the initial experiments. But for the reconnaissance class, a recall of 0.76 was achieved, while the Exploits class reached 0.74, indicating moderate detection effectiveness for these attack categories. However, the main weakness in the DoS category was the model's lowest recall of 0.43. Meaning that less than half of the actual DoS samples were correctly classified, while the remaining records were confused with other attack types. Suggesting that DoS traffic patterns overlap with other categories (Patil et al., 2022).

Scenario after using GAN

As shown in Figure 6, the normalized confusion matrix for random forests after using GAN. The result

shows a well-balanced classification distribution, with all diagonal values very high and off-diagonal errors minimal. Suggesting that generated synthetic samples using GANs successfully enhanced class representation, reduced imbalance effects, and improved the model's ability to learn discriminative patterns across all attack types (Tabassum *et al.*, 2022).

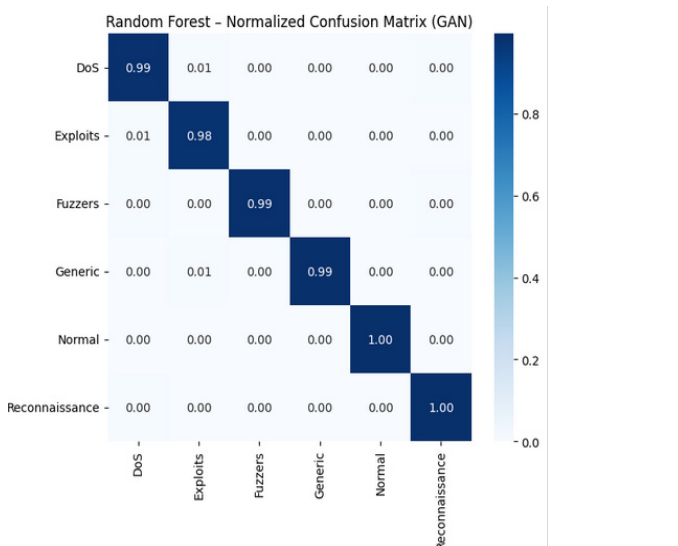


Figure 5: Normalize the confusion matrix for KNN.

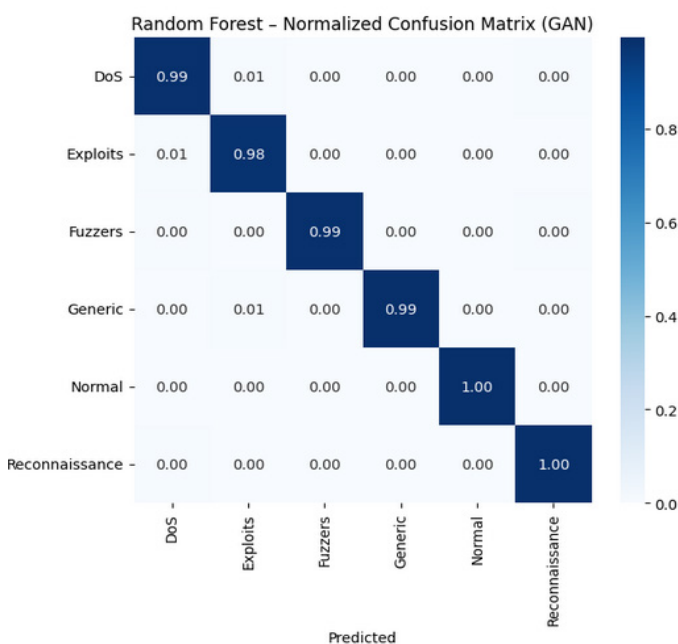


Figure 6: Random forest confusion matrix after GAN.

According to Figure 7, after applying GAN data augmentation, the KNN model shows a clear improvement in overall classification performance by achieving an accuracy of 88.34%. The matrix indicates a more balanced distribution of correct predictions across all classes compared to the pre-GAN results, and the DoS class improved substantially, reaching a recall of 0.84, suggesting that most DoS attacks are

now correctly identified (Tabassum *et al.*, 2022).

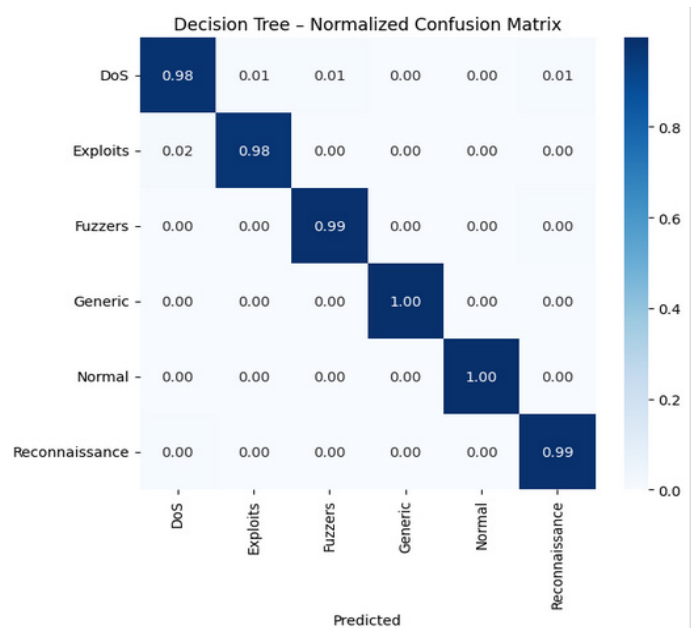


Figure 7: KNN confusion matrix after GAN.

Based on Figure 8, the DT model after GAN is highly robust and balanced, with nearly all diagonal values close to 1 and very minimal off-diagonal errors. Suggesting that synthetic data generated with a GAN effectively improved class representation, reduced imbalance issues, and strengthened the model's ability to generalize across all intrusion categories (Patil *et al.*, 2022).

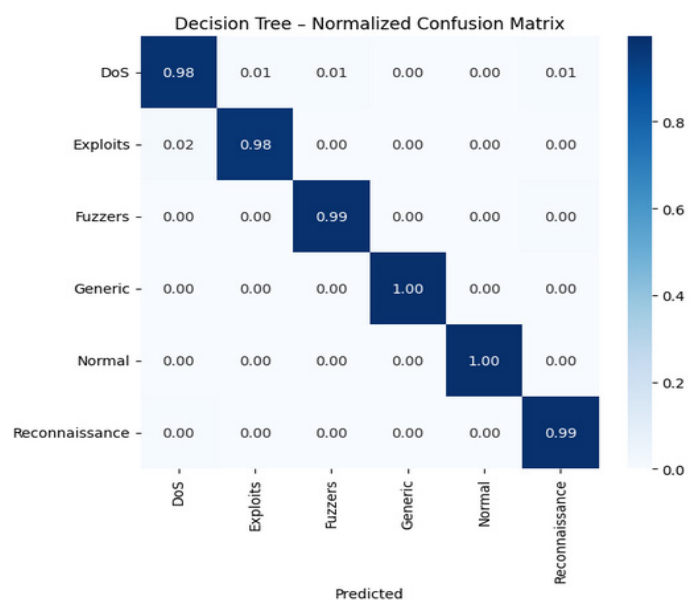


Figure 8: DT confusion matrix after GAN.

As shown in Figure 9, comparing model performance before and after GAN data augmentation reveals a significant improvement across all evaluated machine learning models. Before GAN enhancement, the

models achieved moderate performance, with random forests and DT achieving approximately 0.87 accuracy, while KNN performed slightly worse at around 0.81. Suggesting that the original dataset suffered from limitations such as class imbalance and insufficient representation of attack patterns. After integrating GAN synthetic samples, all models have a clear performance increase. Random forest and DT achieved a near-perfect accuracy of approximately 0.99, while KNN improved to 0.88. Meaning that GAN-based data augmentation significantly enhances the learning capability of all models. In summary, the improvement is especially notable in minority attack classes, where previously misclassification was higher. The GAN helped balance the dataset distribution, allowing models to learn more representative decision boundaries and reducing bias toward dominant classes such as normal and generic traffic (Tabassum *et al.*, 2022).

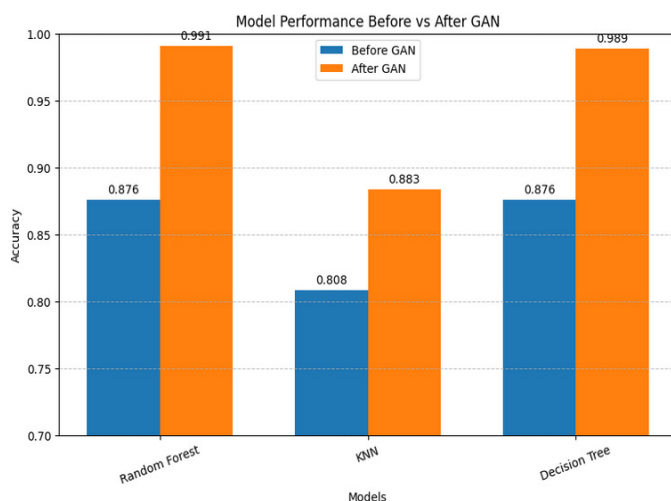


Figure 9: Comparison between models.

Conclusion

The results show a significant improvement in all evaluated models after applying GAN-based data augmentation. Random Forest achieved the highest gain of 13.11%, followed closely by Decision Tree with 12.95%. Also, KNN showed a noticeable improvement of 9.32%, although its gain was comparatively lower than that of tree-based models. Meaning that ensemble and tree-based models benefit more from GAN-generated synthetic data, as they are better able to exploit improved class balance and richer feature distributions. The enhancement ensures that GAN integration substantially improves the learning capability and generalization performance of IDS models.

Acknowledgement

The author acknowledges the support of colleagues and academic staff who provided constructive feedback and technical guidance throughout this work. Finally, the authors appreciate the efforts of the open-source machine learning and deep learning communities whose tools and frameworks facilitated the implementation and evaluation of the proposed IDS framework.

Novelty Statement

This study presents a novel intrusion detection framework that integrates advanced data mining techniques with Generative Adversarial Networks (GANs) to enhance the performance of Intrusion Detection Systems (IDS). The research systematically compares the performance of Random Forest, K-Nearest Neighbors (KNN), and Decision Tree classifiers before and after GAN-based augmentation using the UNSW-NB15 dataset. The findings demonstrate that combining data mining preprocessing with GAN augmentation significantly improves attack detection accuracy, achieving approximately 99% accuracy for Random Forest and Decision Tree models.

Author's Contribution

Zainab Zaidon Kareem: Conceptualization, methodology, formal analysis, writing original draft, and visualization. Methodology, formal analysis, data curation, review and editing, supervision, Validation, investigation, data curation, review and editing, supervision. Validation, investigation, visualization, review and editing, supervision.

Generative AI and AI-assisted technology statement

The authors declare that no generative AI and AI-assisted technology were used in the creation of this manuscript.

Funding

No funding received.

Declaration of competing interest

The author disclosed no competing financial interests.

References

Ahmad, Z., Khan, A.S., Shiang, C.W. and

- Abdullah, J., 2021. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Trans. Emerg. Telecommun. Technol.*, 32(1): e4150. <https://doi.org/10.1002/ett.4150>
- Binbusayyis, A. and Vaiyapuri, T., 2021. Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class svm. *Appl. Intell.*, 51(10): 7094-7108. <https://doi.org/10.1007/s10489-021-02205-9>
- Bourou, S., El Saer, A., Velivassaki, T.-H., Voulkidis, A. and Zahariadis, T., 2021. A review of tabular data synthesis using GANs on an IDS dataset. *Information*, 12(9): 375. <https://doi.org/10.3390/info12090375>
- Chauhan, R. and Heydari, S.S., 2020. Polymorphic adversarial DDoS attack on IDS using GAN. In: 2020 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, pp. 1-6. <https://doi.org/10.1109/ISNCC49221.2020.9297264>
- Chindove, H. and Brown, D., 2021. Adaptive machine learning based network intrusion detection. In: *Proceedings of the International Conference on Artificial Intelligence and its Applications*. pp. 1-6. <https://doi.org/10.1145/3487923.3487938>
- Injadat, M., Moubayed, A., Nassif, A.B. and Shami, A., 2020. Multi-stage optimized machine learning framework for network intrusion detection. *IEEE Transactions on Network and Service Management*, 18(2): 1803-1816. <https://doi.org/10.1109/TNSM.2020.3014929>
- Kaggle, 2024. UNSW-NB15 dataset. Available at: Kaggle UNSW-NB15 Dataset.
- Lee, J. and Park, K., 2021. GAN-based imbalanced data intrusion detection system. *Personal Ubiquit. Comput.*, 25: 121-128. <https://doi.org/10.1007/s00779-019-01332-y>
- Lin, Z., Shi, Y. and Xue, Z., 2022. IDSGAN: Generative adversarial networks for attack generation against intrusion detection. In: *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, pp. 79-91. https://doi.org/10.1007/978-3-031-05981-0_7
- Liu, R., Antypenko, I., Sushko, I. and Zakharchenko, O., 2022. Intrusion detection system after data augmentation schemes based on the VAE and CVAE. *IEEE Trans. Reliabil.*, 71(2): 1000-1010. <https://doi.org/10.1109/TR.2022.3164877>
- Mustapha, A., Khatoun, R., Zeadally, S., Chbib, F., Fadlallah, A., Fahs, W. and El-Attar, A., 2023. Detecting DDoS attacks using adversarial neural network. *Comput. Secur.*, 127: 103117. <https://doi.org/10.1016/j.cose.2023.103117>
- Patil, R., Biradar, R., Ravi, V., Biradar, P. and Ghosh, U., 2022. Network traffic anomaly detection using PCA and BiGAN. *Internet Technol. Lett.*, 5(1): e235. <https://doi.org/10.1002/itl2.235>
- Tabassum, A., Erbad, A., Lebda, W., Mohamed, A. and Guizani, M., 2022. FedGAN-IDS: Privacy-preserving IDS using GAN and federated learning. *Comput. Commun.*, 192: 299-310. <https://doi.org/10.1016/j.comcom.2022.06.015>
- Tama, B.A. and Lim, S., 2021. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. *Comput. Sci. Rev.*, 39: 100357. <https://doi.org/10.1016/j.cosrev.2020.100357>
- Thakkar, A. and Lohiya, R., 2022. A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artif. Intell. Rev.*, 55(1): 453-563. <https://doi.org/10.1007/s10462-021-10037-9>
- Truong-Huu, T., Dheenadhayalan, N., Kundu, P.P., Ramnath, V., Liao, J., Teo, S.G. and Kadiyala, S.P., 2020. An empirical study on unsupervised network anomaly detection using generative adversarial networks. In: *Proceedings of the 1st ACM Workshop on Security and Privacy on Artificial Intelligence*. pp. 20-29. <https://doi.org/10.1145/3385003.3410924>
- Yang, L., Moubayed, A. and Shami, A., 2021. MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles. *IEEE Internet Things J.*, 9(1): 616-632. <https://doi.org/10.1109/JIOT.2021.3084796>
- Zhang, Y. and Liu, Q., 2022. On IoT intrusion detection based on data augmentation for enhancing learning on unbalanced samples. *Future Generat. Comput. Syst.*, 133: 213-227. <https://doi.org/10.1016/j.future.2022.03.007>