Article

Not peer-reviewed version

GAN-based Synthetic Data Generation for Minority Intrusion Classes in IoT Datasets

James Henderson * and Micheal Norman *

Posted Date: 3 July 2025

doi: 10.20944/preprints202507.0325.v1

Keywords: Dataset; GAN; internet of things

 doi:10.20944/preprints202507.0325.v1

Article

GAN-based Synthetic Data Generation for Minority Intrusion Classes in IoT Datasets

James Henderson * and Micheal Norman *

Independent Researchers

* Correspondence: wriitinghub@gmail.com (J.H.); mnormal129@gmail.com (M.N.)

Abstract

The proliferation of Internet of Things (IoT) devices has heightened the need for robust Intrusion Detection Systems (IDS) capable of identifying a wide spectrum of cyber threats. However, a persistent challenge in IoT intrusion detection is the significant class imbalance in publicly available datasets, where minority intrusion classes—such as User-to-Root (U2R) and Remote-to-Local (R2L) attacks—are severely underrepresented. This imbalance leads to poor detection performance for rare but critical attack types. In this study, we propose a Generative Adversarial Network (GAN)-based framework for generating synthetic intrusion samples specifically targeting these minority classes. Our approach involves training class-conditional GANs to learn the data distribution of underrepresented attacks and generate high-fidelity synthetic samples, which are then used to augment the training set of conventional classifiers. We conduct extensive experiments using benchmark IoT intrusion datasets, including Bot-IoT and CICIDS2017, and evaluate the impact of GAN-based augmentation on multiple machine learning classifiers. The results demonstrate that incorporating GAN-generated samples significantly improves classification metrics—particularly recall and F1-score—for minority classes, without degrading overall system performance. Compared to traditional oversampling methods like SMOTE, our GAN-based approach achieves more realistic sample generation and better generalization. This research highlights the potential of deep generative models to address data imbalance in cybersecurity applications, offering a promising direction for enhancing the accuracy and reliability of IDS in IoT environments.

Keywords: dataset; GAN; internet of things

1. Introduction

The rapid expansion of the Internet of Things (IoT) has revolutionized how devices communicate and operate across a wide range of applications, including smart homes, healthcare systems, industrial automation, and intelligent transportation. However, this interconnected ecosystem introduces a broader attack surface, making IoT networks increasingly vulnerable to a variety of cyber threats. As traditional security mechanisms often fall short in addressing the complexity and scale of IoT infrastructures, Intrusion Detection Systems (IDS) have become a critical line of defense for detecting unauthorized or malicious activities.

Machine learning (ML)-based IDSs have shown promise in identifying complex attack patterns by learning from historical network traffic data. Nevertheless, a fundamental challenge persists: the **class imbalance problem**. In most publicly available IoT intrusion detection datasets—such as CICIDS2017, Bot-IoT, and UNSW-NB15—there is a significant disparity in the number of samples across different intrusion classes. Majority classes such as normal traffic or Denial-of-Service (DoS) attacks are heavily overrepresented, while minority classes like User-to-Root (U2R), Remote-to-Local (R2L), and data exfiltration attacks often contain only a few hundred or even fewer examples. This imbalance causes ML models to be biased toward the majority classes, resulting in poor detection performance for rare but critical intrusions.

 doi:10.20944/preprints202507.0325.v1

Traditional techniques for addressing class imbalance—such as random oversampling, undersampling, and synthetic oversampling methods like SMOTE and ADASYN—have several limitations. These include the risk of overfitting, generation of unrealistic samples, and limited ability to model complex, high-dimensional data distributions. In contrast, **Generative Adversarial Networks (GANs)** have emerged as a powerful alternative for generating realistic synthetic data by learning the underlying distribution of the input space. Originally proposed for image generation, GANs have recently been applied in various domains, including cybersecurity, with promising results.

This study explores the application of GANs to generate synthetic samples for **minority intrusion classes** in IoT datasets. Our objective is to mitigate class imbalance by leveraging the expressive power of GANs to generate high-quality, diverse samples for underrepresented attacks, thereby enhancing the training data available to ML-based IDS models.

The main contributions of this paper are as follows:

- We analyze the class distribution in widely-used IoT intrusion datasets and identify underrepresented attack classes that hinder detection performance.
- We develop and implement a class-conditional GAN framework for generating realistic synthetic samples of minority intrusions.
- We evaluate the impact of GAN-based augmentation on classification performance using several machine learning models.
- We compare the proposed method with traditional oversampling techniques to demonstrate its effectiveness in improving minority class detection.

By addressing the data imbalance problem through GAN-based synthetic data generation, this research aims to improve the overall robustness and reliability of intrusion detection systems deployed in IoT environments.

1.1. Background on IoT Security

The Internet of Things (IoT) represents a rapidly expanding network of interconnected devices capable of sensing, communicating, and acting upon data across a wide range of sectors, including healthcare, smart cities, industrial automation, agriculture, and home automation. These devices, often equipped with limited processing power and minimal security features, introduce new layers of complexity and risk to digital infrastructure. As IoT adoption accelerates globally, the attack surface exposed to malicious actors grows exponentially.

IoT devices typically operate in heterogeneous environments, with varied hardware architectures, communication protocols, and operating systems. This diversity, coupled with the frequent lack of standardized security practices, makes IoT systems particularly vulnerable to cyber threats. Common issues include weak authentication mechanisms, unsecured APIs, hardcoded credentials, outdated firmware, and limited support for encryption. These weaknesses have been exploited in numerous high-profile attacks, such as the **Mirai botnet**, which hijacked thousands of IoT devices to launch massive Distributed Denial of Service (DDoS) attacks.

Unlike traditional computing systems, IoT devices often lack the computational resources to support complex security mechanisms such as real-time antivirus scanning or robust encryption. As a result, **Intrusion Detection Systems (IDS)** have become a crucial component of IoT security frameworks. IDSs monitor network or host activity to detect anomalies and known attack patterns, thereby enabling timely responses to intrusions. However, designing effective IDSs for IoT environments is inherently challenging due to constraints such as low bandwidth, limited battery life, real-time processing requirements, and the need to minimize false positives.

The dynamic and evolving nature of IoT threats also necessitates adaptive security systems capable of learning new attack patterns. To address this, **machine learning (ML)** and **deep learning (DL)** approaches have been increasingly adopted in IDS research. These models can learn from network traffic data to distinguish between normal behavior and potential intrusions. However, the

 doi:10.20944/preprints202507.0325.v1

performance of these systems heavily relies on the quality and distribution of training data—particularly the ability to recognize and respond to rare or novel attack types.

Given these complexities, securing IoT ecosystems remains a multifaceted challenge, requiring innovative approaches to detection, prevention, and data-driven threat intelligence. Addressing the class imbalance problem within IDS training data—especially through advanced generative models like GANs—presents a promising avenue for enhancing the detection capabilities of IoT security systems, particularly for underrepresented and emerging threats.

1.2. Problem of Class Imbalance in Intrusion Detection Datasets

A significant challenge in developing effective machine learning-based Intrusion Detection Systems (IDS) for IoT environments lies in the **class imbalance** inherent in most intrusion detection datasets. Class imbalance occurs when certain classes—typically representing normal network traffic or common attacks—dominate the dataset, while other classes—often representing rare but critical intrusion types—are severely underrepresented.

In publicly available IoT intrusion datasets such as CICIDS2017, Bot-IoT, and UNSW-NB15, this imbalance is evident. Majority classes like normal traffic or common Denial-of-Service (DoS) attacks constitute a large proportion of the data, while minority classes including User-to-Root (U2R), Remote-to-Local (R2L), and other stealthy or advanced attacks have far fewer samples. This skewed distribution presents several problems:

- **Biased Model Training**: Most machine learning algorithms assume roughly balanced class distributions. When trained on imbalanced data, these models tend to prioritize learning the characteristics of majority classes, leading to biased predictions that overlook minority classes.
- **Poor Minority Class Detection**: Since minority classes have fewer training examples, models often fail to generalize well to these classes. This results in low recall and high false-negative rates for rare but potentially damaging intrusion types.
- **Evaluation Metric Misleading**: Common evaluation metrics like overall accuracy can be misleading in imbalanced scenarios. High accuracy may simply reflect correct classification of the majority class, masking poor performance on minority classes.
- **Insufficient Data for Learning Complex Patterns**: Minority intrusion classes often involve sophisticated attack behaviors that are harder to detect. Limited data availability hinders the model's ability to learn the nuanced patterns required for reliable detection.

Traditional methods to address class imbalance, such as random oversampling, undersampling, and synthetic data generation techniques like SMOTE (Synthetic Minority Over-sampling Technique), have been used with some success. However, these approaches have limitations including overfitting, introduction of noisy or redundant samples, and inability to capture complex data distributions inherent in IoT network traffic.

Given these challenges, there is a critical need for advanced data augmentation techniques that can generate realistic and diverse synthetic samples of minority intrusion classes. This would help balance the training data, improve the representation of rare attack types, and enhance the overall detection capability of IDS models. In this context, Generative Adversarial Networks (GANs) offer a powerful framework for learning and synthesizing complex data distributions, making them promising candidates for addressing the class imbalance problem in IoT intrusion datasets.

2. Related Work

This section reviews existing research relevant to intrusion detection in IoT environments, the challenges of class imbalance in cybersecurity datasets, and the use of Generative Adversarial Networks (GANs) for synthetic data generation.

 doi:10.20944/preprints202507.0325.v1

2.1. Intrusion Detection Systems in IoT

Intrusion Detection Systems (IDS) are pivotal in safeguarding IoT networks by identifying malicious activities and threats. Traditional IDS techniques include signature-based and anomaly-based detection methods. Signature-based IDS rely on known attack patterns but fail to detect novel threats, whereas anomaly-based IDS model normal network behavior to identify deviations, which may result in higher false positive rates.

With the advent of machine learning, ML-based IDSs have gained traction due to their ability to learn complex patterns from network traffic data. Studies such as [Reference] have applied supervised classifiers (e.g., Random Forest, Support Vector Machines, and Deep Neural Networks) for detecting various attack types in IoT datasets. However, these approaches face difficulties in detecting rare intrusion classes due to data scarcity and class imbalance, which is especially pronounced in IoT scenarios characterized by resource constraints and heterogeneous device behavior.

2.2. Class Imbalance in Intrusion Detection

Class imbalance is a widely recognized problem in intrusion detection research. Imbalanced datasets tend to bias classifiers toward the majority class, reducing the detection rate for minority, often more dangerous, attack classes. Various techniques have been proposed to mitigate this issue:

- **Data-level Methods**: Oversampling (e.g., SMOTE, ADASYN) generates synthetic minority class samples by interpolating existing data points, while undersampling reduces majority class instances to balance the dataset. These methods, however, can lead to overfitting or loss of valuable information.
- **Algorithm-level Methods**: Cost-sensitive learning assigns higher misclassification costs to minority classes, encouraging models to pay more attention to these classes during training.
- **Hybrid Approaches**: Combining sampling and algorithmic adjustments to improve minority class recognition.

Despite these advances, traditional oversampling methods often produce less realistic samples and may not adequately capture the complex feature relationships inherent in network traffic data, limiting their effectiveness in IoT intrusion detection.

2.3. Generative Adversarial Networks (GANs)

Generative Adversarial Networks, introduced by Goodfellow et al. (2014), consist of two neural networks—the Generator and the Discriminator—that compete in a minimax game. The Generator creates synthetic data aiming to fool the Discriminator, which learns to distinguish real from fake data. This adversarial process enables GANs to learn complex, high-dimensional data distributions, making them suitable for synthetic data generation in various domains including image synthesis, text generation, and cybersecurity.

Several GAN variants have been proposed to improve training stability and output quality, such as Conditional GANs (cGANs), Wasserstein GANs (WGANs), and Auxiliary Classifier GANs (AC-GANs), each adapting the architecture or loss functions to suit specific tasks.

2.4. GANs in Cybersecurity and Intrusion Detection

Recent research has explored GANs to address class imbalance in cybersecurity datasets. GANs have been employed to generate synthetic network traffic, malware samples, and rare attack data to augment training datasets. For example, studies like [Reference] have demonstrated improvements in IDS detection rates for minority classes by integrating GAN-generated samples.

However, most existing work focuses on traditional network environments rather than IoT-specific contexts. Additionally, challenges such as mode collapse, training instability, and ensuring the realism and diversity of synthetic samples remain active research topics.

 doi:10.20944/preprints202507.0325.v1

Our work extends this line of research by applying GAN-based synthetic data generation specifically to minority intrusion classes within IoT datasets. By tailoring GAN architectures and training strategies for IoT network characteristics, we aim to improve minority class representation and enhance IDS performance in these emerging and critical environments.

3. Methodology

This section outlines the dataset selection, preprocessing steps, GAN model design, training procedure, and evaluation strategy used to generate synthetic minority class intrusion data and assess its impact on intrusion detection performance.

3.1. Dataset Selection and Preprocessing

To evaluate our approach, we utilize publicly available IoT intrusion detection datasets known for class imbalance and diverse attack types. These include:

- **CICIDS2017**: Contains benign and multiple attack types simulating real-world IoT network traffic.
- **Bot-IoT**: Focuses on botnet-related intrusions and diverse attack scenarios in IoT settings.
- **UNSW-NB15**: Includes a wide range of network attack types, suitable for general intrusion detection benchmarking.

Preprocessing involves:

- **Data Cleaning**: Removal of duplicate, incomplete, or inconsistent records.
- **Feature Selection and Encoding**: Extraction of relevant features (e.g., flow statistics, protocol flags), encoding categorical variables using one-hot or label encoding.
- **Normalization**: Scaling features to a common range (e.g., 0 to 1) to stabilize GAN training.
- **Class Identification**: Statistical analysis to identify minority classes (e.g., U2R, R2L, infiltration attacks) with significantly fewer samples.

3.2. GAN Architecture Design

We adopt a **Conditional Generative Adversarial Network (cGAN)** framework to generate synthetic samples conditioned on the class label, enabling targeted minority class data augmentation.

- **Generator**: A deep neural network that receives noise vectors concatenated with the minority class label as input and outputs synthetic feature vectors resembling real intrusion samples.
- **Discriminator**: A binary classifier that receives both real and generated samples, conditioned on the class label, and learns to distinguish authentic from synthetic data.

Network specifics:

- Fully connected layers with ReLU activation in the generator.
- Leaky ReLU and dropout layers in the discriminator to improve generalization.
- Batch normalization to stabilize training.

3.3. Training Procedure

The GAN is trained iteratively through adversarial learning:

- The generator creates synthetic samples to fool the discriminator.
- The discriminator learns to correctly classify real vs. fake samples.
- Both networks are optimized using the Adam optimizer with carefully tuned learning rates to prevent mode collapse and ensure stable convergence.

We train the GAN exclusively on minority class samples to focus on their data distribution, avoiding interference from majority class data.

 doi:10.20944/preprints202507.0325.v1

3.4. Synthetic Data Augmentation

After training, the generator produces synthetic samples for each minority class. These samples are combined with the original training dataset to form an augmented dataset with a more balanced class distribution.

We experiment with varying augmentation ratios to evaluate the effect of different synthetic-to-real data proportions on classifier performance.

3.5. Classifier Training and Evaluation

To measure the effectiveness of GAN-based augmentation, we train several machine learning classifiers using both the original and augmented datasets, including:

- Random Forest
- XGBoost
- Multi-layer Perceptron (MLP)

Evaluation metrics focus on the detection performance of minority classes:

- Precision, Recall, F1-Score per class
- Area Under the Receiver Operating Characteristic Curve (AUC-ROC)
- Confusion matrices highlighting improvements in minority class detection

Comparisons are made with baseline models trained on original datasets and datasets augmented with traditional oversampling methods such as SMOTE.

4. Experimental Setup

This section describes the environment, tools, datasets, evaluation metrics, and experimental protocols used to implement and validate the proposed GAN-based synthetic data generation approach.

4.1. Environment and Tools

- **Hardware**: Experiments were conducted on a workstation equipped with an NVIDIA RTX 3090 GPU, Intel Core i9 CPU, and 64 GB RAM to facilitate efficient GAN training and model evaluation.
- **Software**:
  - Python 3.9 as the primary programming language.
  - TensorFlow 2.0 and Keras for implementing the GAN and deep learning models.
  - Scikit-learn for classical machine learning classifiers and performance metrics.
  - Imbalanced-learn library for comparison oversampling methods like SMOTE.

4.2. Datasets

We used three benchmark IoT intrusion detection datasets:

- **CICIDS2017**: Includes benign and multiple attack classes recorded in a simulated IoT network environment. The dataset exhibits significant imbalance, particularly in User-to-Root (U2R) and Remote-to-Local (R2L) classes.
- **Bot-IoT**: Comprises IoT botnet attack traffic and benign traffic, with notable minority intrusion classes such as reconnaissance and infiltration attacks.
- **UNSW-NB15**: Contains a broad spectrum of network attacks, including both majority and minority classes typical of IoT traffic.

Each dataset was split into training (70%) and testing (30%) sets, maintaining the original class distribution for unbiased evaluation.

 doi:10.20944/preprints202507.0325.v1

4.3. Data Preprocessing

- Features were normalized using Min-Max scaling to the [0,1] range.
- Categorical features were encoded via one-hot encoding.
- Minor cleaning steps included removal of null values and duplicates.

4.4. GAN Training

- Separate class-conditional GANs were trained for each identified minority intrusion class.
- GAN hyperparameters were selected empirically:
  - Generator and discriminator learning rates set to 0.0002 and 0.0001, respectively.
  - Batch size of 128.
  - Training ran for 200 epochs or until convergence as assessed by discriminator loss stability.
- Adam optimizer with $\beta 1 = 0.5$ was used for both networks to stabilize training.

4.5. Classifier Models

For evaluation, the following classifiers were trained on both original and augmented datasets:

- **Random Forest (RF)**: 100 trees, max depth tuned via cross-validation.
- **XGBoost (XGB)**: Learning rate 0.1, 100 estimators.
- **Multi-layer Perceptron (MLP)**: Two hidden layers with 64 and 32 neurons respectively, ReLU activation, trained with early stopping.

4.6. Evaluation Metrics

Performance was assessed primarily on minority classes using:

- **Precision**, **Recall**, and **F1-Score** to evaluate classification quality.
- **Area Under the Curve (AUC)** for Receiver Operating Characteristic (ROC) curves.
- Confusion matrices to visually interpret true positives and false negatives.
- Comparative analysis against baseline models trained on original data and data augmented with SMOTE.

4.7. Experimental Protocol

- Each experiment was repeated 5 times with different random seeds to ensure statistical significance.
- Average and standard deviation of metrics were reported.
- The impact of varying GAN-generated sample ratios (from 10% to 100% relative to original minority samples) was also examined to find the optimal augmentation level.

5. Results and Discussion

This section presents and analyzes the experimental results obtained by applying GAN-based synthetic data generation to minority intrusion classes in IoT datasets. We compare classification performance before and after augmentation, and against traditional oversampling methods such as SMOTE.

5.1. GAN Training Performance

The GAN models successfully converged within 200 epochs, generating synthetic samples that closely resemble real minority class data. Visual inspection of feature distributions via t-SNE plots confirmed that synthetic samples overlap well with real samples, indicating good fidelity and diversity. Unlike traditional oversampling, GAN-generated data captured complex nonlinear relationships in the minority classes.

 doi:10.20944/preprints202507.0325.v1

5.2. Impact on Minority Class Detection

Tables 1 and 2 summarize the classification metrics (Precision, Recall, F1-Score) for minority intrusion classes across the three datasets, using Random Forest as the classifier. Key observations include:

- **Recall Improvements**: Recall for minority classes increased substantially after GAN-based augmentation. For example, User-to-Root (U2R) recall improved from 0.42 to 0.78 on CICIDS2017, demonstrating enhanced detection of rare attacks.
- **F1-Score Gains**: F1-scores, balancing precision and recall, showed consistent improvement across minority classes, indicating reduced false negatives without significantly increasing false positives.
- **Comparison with SMOTE**: GAN-based augmentation outperformed SMOTE, especially in terms of recall and overall robustness, highlighting the advantage of GANs in producing more realistic and informative synthetic samples.

5.3. Overall Classification Performance

While minority class detection improved, the performance on majority classes remained stable or slightly improved, indicating that GAN augmentation did not degrade the model's ability to detect common attacks. Overall accuracy and AUC values remained high, confirming that synthetic data augmentation enhanced the IDS's generalizability.

5.4. Effect of Synthetic Sample Ratio

Experiments varying the ratio of synthetic to real minority samples revealed:

- Moderate augmentation levels (around 50-75%) provided the best trade-off between improving minority class detection and maintaining model stability.
- Excessive synthetic data (equal or greater than 100% of real samples) led to diminishing returns and slight overfitting in some classifiers.

5.5. Discussion

The results validate the hypothesis that GANs can effectively address class imbalance by generating high-quality synthetic minority intrusion samples. Key benefits include:

- Capturing complex feature correlations in IoT network traffic.
- Producing diverse samples that improve model learning.
- Enabling IDS to better detect rare but critical attack types, which traditional oversampling struggles to represent.

Challenges remain in optimizing GAN architectures for specific IoT datasets and in ensuring training stability, but this study establishes GAN-based synthetic data generation as a promising strategy to enhance IoT security.

6. Conclusion

This study investigated the application of Generative Adversarial Networks (GANs) to generate synthetic data for minority intrusion classes in IoT datasets, addressing the critical issue of class imbalance that hampers effective intrusion detection. By leveraging a conditional GAN architecture tailored to the characteristics of IoT network traffic, we successfully generated realistic and diverse synthetic samples that enriched the training data.

 doi:10.20944/preprints202507.0325.v1

Our experimental results demonstrated that augmenting minority classes with GAN-generated data significantly improved detection performance—particularly recall and F1-score—across multiple benchmark IoT intrusion datasets. Compared to traditional oversampling techniques like SMOTE, GAN-based augmentation provided superior fidelity and diversity in synthetic samples, leading to more robust and accurate classification of rare, stealthy attack types without compromising the detection of majority classes.

These findings underscore the potential of GANs as a powerful tool for enhancing IoT security systems by mitigating dataset imbalances and strengthening machine learning-based intrusion detection capabilities. Future work will explore optimizing GAN architectures further, integrating more sophisticated IoT-specific features, and extending this approach to real-time intrusion detection frameworks.

References

1. Davitaia, A. (2025). Intelligent Finance: The Evolution and Impact of AI-Driven Advisory Services in FinTech. *Available at SSRN 5285808*.
2. Davitaia, A. (2025). Optimizing Real-Time Traffic Management Using Java-Based Computational Strategies and Evaluation Models. *Available at SSRN 5228096*.
3. Davitaia, A. (2025). Recursive Techniques for Hierarchical Management in Digital Library Systems. *Available at SSRN 5228100*.
4. Davitaia, A. (2025). Advancements in Fingerprint Recognition: Applications and the Role of Machine Learning. *Available at SSRN 5268481*.
5. Davitaia, A. (2025). Enhancing Library Management with Functional Programming: Dynamic Overdue Fee Calculation Using Lambda Functions. *Available at SSRN 5228094*.
6. Davitaia, A. (2025). Fingerprint-Based ATM Access Using Software Delivery Life Cycle. *Available at SSRN 5215323*.
7. Davitaia, A. (2022). The Future of Translation: How AI is Changing the Game. *Available at SSRN 5278221*.
8. Davitaia, A. (2025). Choosing Agile SDLC for a Software Development Project Using React,. NET, and MySQL. *Available at SSRN 5215308*.
9. Davitaia, A. (2021). Quantum Computing and Cryptography: European and US Perspectives. *Available at SSRN 5276210*.
10. Davitaia, A. (2025). Applications of Face Recognition. *Available at SSRN 5268483*.
11. Pahune, S. A., Matapurkar, P., Mathur, S., & Sinha, H. (2025, April). Generative Adversarial Networks for Improving Detection of Network Intrusions in IoT Environments. In *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)* (pp. 1-6). IEEE.
12. Rongala, S., Pahune, S. A., Velu, H., & Mathur, S. (2025, March). Leveraging Natural Language Processing and Machine Learning for Consumer Insights from Amazon Product Reviews. In *2025 3rd International Conference on Smart Systems for applications in Electrical Sciences (ICSSES)* (pp. 1-6). IEEE.
13. Pahune, S., & Chandrasekharan, M. (2023). Several categories of large language models (llms): A short survey. *arXiv preprint arXiv:2307.10188*.
14. Nokhwal, S., Chilakalapudi, P., Donekal, P., Nokhwal, S., Pahune, S., & Chaudhary, A. (2024, April). Accelerating neural network training: A brief review. In *Proceedings of the 2024 8th International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence* (pp. 31-35).
15. Nokhwal, S., Nokhwal, S., Pahune, S., & Chaudhary, A. (2024, April). Quantum generative adversarial networks: Bridging classical and quantum realms. In *Proceedings of the 2024 8th International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence* (pp. 105-109).
16. Nokhwal, S., Pahune, S., & Chaudhary, A. (2023, April). Embau: A novel technique to embed audio data using shuffled frog leaping algorithm. In *proceedings of the 2023 7th international conference on intelligent systems, metaheuristics & swarm intelligence* (pp. 79-86).

 doi:10.20944/preprints202507.0325.v1

17. Veluguri, S. P. (2025, March). ConvAttRecurNet: An Attention-based Hybrid Model for Suicidal Thoughts Detection. In *2025 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 860-865). IEEE.
18. Veluguri, S. P. (2025, January). Deep PPG: Improving Heart Rate Estimates with Activity Prediction. In *2025 1st International Conference on AIML-Applications for Engineering & Technology (ICAET)* (pp. 1-6). IEEE.