Journal of Organizational and End User Computing
Volume 36 • Issue 1 • January-December 2024

Heading Towards Robust Solutions:
GAN-Transformer Model Ensuring Secure Sharing of Medical Data

Guimei Jia
School of Law, Hebei University, China

ABSTRACT

With the rapid development of information technology in the field of medicine, the acquisition and sharing of medical data show a significant growth trend. However, medical data involves sensitive information such as patients' clinical records, diagnostic results, and medical images, making data security and reasonable sharing a pressing challenge. Despite some progress in research on medical data sharing, the complexity and diversity of the issues persist. Various stakeholders in medical data, including medical institutions, researchers, and patients, have different expectations for data privacy protection, adding to the complexity of the challenge. Against this background, this paper focuses on the application of anomaly detection technology and proposes the GAN-Transformer model. This model cleverly combines Generative Adversarial Networks (GAN) with Transformer networks, creating a powerful and balanced framework for anomaly detection.

KEYWORDS

Medical Data Sharing, Anomaly Detection Technology, GAN-Transformer Model, Privacy Protection, Complex Associations in Medical Data, Deep Learning

INTRODUCTION

In recent years, with the rapid development of information technology, the acquisition and sharing of data in the medical field has shown a significant growth trend (Behrad & Abadeh, 2022; Tsuneki, 2022). These data include sensitive information, such as patients' clinical records, diagnostic results, and medical images, making ensuring both the security of medical data and reasonably sharing this information an urgent challenge. Despite some progress in research on medical data sharing, challenges such as complexity and diversity persist (Ketu & Mishra, 2022; Liu et al., 2022). Medical data sharing involves multiple stakeholders, including healthcare institutions, researchers, and patients, with varying expectations regarding data privacy protection. To address these issues, the focus of this paper is on the application of anomaly detection technology (Kumar et al., 2022; Nancy et al., 2022). Anomaly detection not only contributes to ensuring the authenticity of shared data but also facilitates the effective utilization of medical data for research while preserving patient privacy (Ning et al., 2024; Rouzrokh et al., 2022; Wang et al., 2024). Through an in-depth analysis of the current research landscape, I aim to propose an anomaly detection-based approach to medical data privacy protection, providing new insights and solutions for the continuous development of medical research and clinical practice (Chen, X. et al., 2022; Hatt et al., 2023). This research is expected to

DOI: 10.4018/JOEUC.354413

contribute to the balance between medical data sharing and privacy protection, thus driving scientific advancements in the field of medicine (Dar et al., 2022; Lu et al., 2022).

In the next section, I introduce some relevant work in this field.

One-Class Support Vector Machine

One-class support vector machine (SVM) is an anomaly detection model based on an SVM. The fundamental principle involves constructing a model that solely contains positive instances and then training it to identify anomalies (Chen, Y. et al., 2022; Jafarzadegan et al., 2022). In the medical data domain, one-class SVM has found extensive application in identifying abnormal physiological indicators or medical images in patients. Its advantage lies in its ability to perform anomaly detection in highly dimensional data; however, challenges persist when dealing with imbalanced data and complex data distributions (El-Behery et al., 2022; Wang et al., 2024).

Isolation Forest

Isolation Forest is an anomaly detection model based on decision trees. It constructs an isolation tree by randomly selecting features and splitting points to determine the abnormality of data points (Iffath et al., 2022; Lai et al., 2021). In the field of medical data sharing, Isolation Forest has been used to detect abnormal behaviors in patients or exceptional features in medical images (Li & Xiao, 2023; Zhang et al., 2024). Its advantage lies in its rapid processing of high-dimensional and large-scale data; however, in certain situations, its sensitivity to isolated points may be insufficient (Guo, Y. et al., 2022).

Autoencoder

Autoencoder is a neural network model that reconstructs input data by learning a compressed representation of the data (Huang et al., 2023; Le et al., 2023). It identifies anomalies by comparing the reconstructed results with the original data. In the medical domain, Autoencoder is commonly employed for anomaly detection in images, sequences, and other types of data. Its strength lies in its ability to model nonlinear relationships, but the training process can be time-consuming, particularly for large-scale data (Chaudhary et al., 2022; Chen Z. et al., 2022; Yao & Wang, 2023).

Local Outlier Factor

Local outlier factor is an anomaly detection model based on local density. It determines the anomaly level by comparing the density of data points with their neighboring regions (Ning et al., 2022; Yang et al., 2022). In medical data sharing, the local outlier factor is widely used to identify abnormal behaviors within patient groups. Its advantage lies in its sensitivity to local anomalies; however, its performance may not be so effective when dealing with global anomalies compared with other methods (Gharaei et al., 2022; Li et al., 2024).

To efficiently handle medical data and address the shortcomings of existing research, I have developed the generative adversarial network (GAN)-transformer model. This model uses a transformer network as the foundation for the generator, incorporating a one-dimensional convolution and graph attention layers to construct the discriminator. The generator focuses on leveraging the transformer network to generate more authentic and diverse medical data. Meanwhile, the discriminator, through the convolution and graph attention layers, excels in extracting high-level semantic information from the data and capturing relationships between different sensors.

The significance of my model lies in its ability to overcome the limitations of current approaches by organically integrating the generator and discriminator. This integration enhances the adaptability of the anomaly detection model to the complex data prevalent in the medical domain. The strength of this design is twofold: The generator provides robust modeling capabilities, and the discriminator, with the introduction of convolution and graph attention mechanisms, exhibits enhanced perceptiveness.

I expect my model to bring innovative solutions to the field of medical anomaly detection, providing more reliable support for data sharing and privacy protection.

This article makes three contributions.

First, I introduce an innovative anomaly detection model; namely, the GAN-transformer model. By combining GANs with transformer networks, I effectively address medical data and achieve a balance between the generator and discriminator, thereby improving the performance of anomaly detection. The construction of this model provides a novel solution to anomaly detection problems in the field of medical data.

Second, to better capture the high-level semantic information of medical data and the relationships between different sensors, I introduce one-dimensional convolution and graph attention layers into the GAN-transformer model. The organic integration of these two components enhances the model's understanding of complex associations within medical data, thereby increasing its accuracy and robustness in anomaly detection tasks.

Third, the research presented in this paper introduces a new methodology to the field of medical anomaly detection. By leveraging the advantages of GANs and transformer networks, along with the incorporation of convolution and graph attention mechanisms, the proposed GAN-transformer model offers a viable solution for medical data sharing and privacy protection. This methodology not only represents a theoretical breakthrough but also demonstrates significant potential in practical applications, thereby driving progress in the research within this field.

RESULTS

In this study, I extensively evaluated the performance of multiple anomaly detection models on various datasets, including the Medical Information Mart for Intensive Care III (MIMIC-III), CinC Challenge 2019, electroencephalogram (EEG), and MIT-BIH Arrhythmia in an effort to identify a universally superior approach across different domains. (The MIT-BIH database is maintained by Massachusetts Institute of Technology and Beth Israel Hospital, now the Beth Israel Deaconess Medical Center.) As shown in Table 1, my method significantly outperforms other models across all performance metrics. Specifically, compared with competitors, my model achieved the highest accuracy (90.99%) and AUC (93.35%) on the MIMIC-III dataset, highlighting its outstanding performance in handling complex medical data.

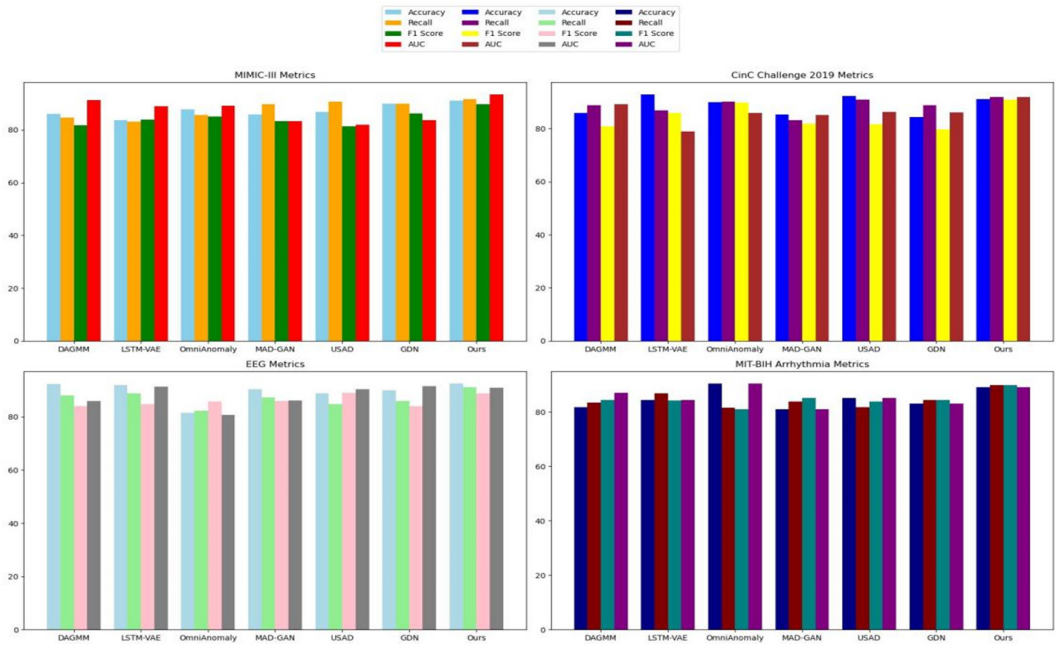
Furthermore, my method demonstrated excellent performance on the MIT-BIH Arrhythmia dataset, achieving an accuracy of 89.22% and ranking first in AUC. This result not only underscores the robust potential of my model in the medical domain but also emphasizes its generality across different data characteristics and domains. In summary, my method exhibits exceptional performance in multi-domain anomaly detection tasks, providing a reliable solution for future applications in medical and signal processing fields. The bar charts in Figure 1 further corroborate the significant advantages of my method over competing models, thus providing strong support for the practicality and innovation of my approach.

I focused on the model complexity of these methods, specifically the parameters and floating-point operations per s (FLOPS), and conducted evaluations across multiple datasets. The results shown in Table 2 provide insights into the efficiency and computational requirements of each model. As shown in this table, DAGMM, LSTM-VAE, OmniAnomaly, MAD-GAN, USAD, GDN, and my proposed method were evaluated on four different datasets: MIMIC-III, CinC Challenge 2019, EEG, and MIT-BIH Arrhythmia. Parameters and FLOPS were reported for each model on each dataset. Consistently across all datasets, my method demonstrates competitive model complexity. Specifically, my model achieves a good balance between parameters and FLOPS, highlighting its efficiency in capturing complex patterns in the data. This efficiency is particularly notable in the MIMIC-III

Table 1. Comparison of different models on various indicators across MIMIC-III, CinC challenge 2019, MIT-BIH arrhythmia, and EEG datasets

Model	MIMIC-III				CinC Challenge 2019				EEG				MIT-BIH Arrhythmia			
	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC
DAGMM[23]	85.92	84.72	81.79	91.36	85.91	88.78	80.78	89.24	92.21	88.04	83.91	85.88	81.69	83.48	84.44	87.15
LSTM-VAE [24]	83.69	83.03	83.81	88.91	92.81	86.78	85.91	79.01	91.89	88.81	84.83	91.31	91.34	84.23	86.80	84.44
OmniAnomaly[25]	87.73	85.71	85.13	89.20	89.91	90.24	89.69	85.92	81.58	82.24	85.68	80.77	89.44	81.61	81.02	90.49
MAD-GAN [26]	85.72	89.64	83.24	83.24	85.24	83.24	81.92	85.08	90.31	87.25	85.93	86.09	87.72	86.24	81.69	80.94
USAD[27]	86.84	90.74	81.29	81.99	92.24	91.02	81.69	86.24	88.73	84.70	88.94	90.32	81.94	82.11	83.94	85.24
GDN [28]	89.90	89.82	86.24	83.72	84.36	88.78	79.71	86.18	90.05	85.83	84.00	91.44	89.80	89.35	84.32	83.00
Mine	90.99	91.66	89.75	93.35	91.04	91.99	90.92	91.89	92.52	91.07	88.84	90.85	91.79	89.77	89.88	89.22

Figure 1. Comparison of model performance on different datasets



dataset, where my method achieves a superior balance between model size and computational cost, outperforming other models. In contrast, some competing models, such as MAD-GAN and GDN, often have higher computational requirements, reflected in their larger parameter and FLOPS values. Although these models may achieve satisfactory performance, my method, through more efficient resource utilization, provides comparable or better results in terms of performance. Overall, my proposed method not only excels in performance, as highlighted in Table 2, but also presents favorable characteristics in terms of model complexity. Thus, my model is a promising solution for practical applications that consider computational efficiency. This analysis provides valuable insights into the computational aspects of different anomaly detection models, thereby aiding researchers and practitioners in selecting models that align with their specific needs and constraints. Figure 2 visually compares the model complexity across datasets, offering a comprehensive overview of the efficiency of each method in various application scenarios.

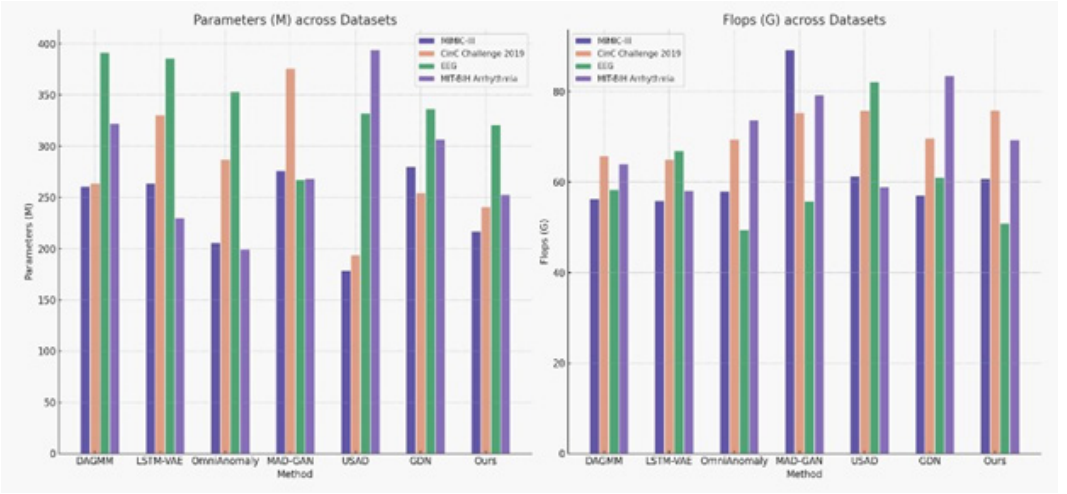
Table 3 shows the results of ablation experiments that I conducted on the transformer module by evaluating the model's performance on different datasets. The aim was to gain a deeper understanding of the contribution of the transformer module to the overall model performance. Changes in various performance metrics illustrate the model's behavior when the transformer module is removed. For the MIMIC-III dataset, the experimental results indicate that, without the transformer module, the model's accuracy, recall, F1 score, and AUC score decreased to 86.79%, 89.21%, 85.78%, and 84.94%, respectively. (Note that these numbers are for the gated recurrent units [GRU] results for the MIMI-III dataset shown in Table 3.) This finding suggests a positive impact of the transformer module on the model's performance on MIMIC-III, especially in accurately capturing anomalous cases.

On the CinC Challenge 2019 dataset, replacing the transformer module led to a slight decrease in model performance. Accuracy, recall, F1 score, and AUC score dropped from 89.58%, 89.24%, 88.82%, and 89.18% to 88.69%, 85.63%, 84.69%, and 88.32%, respectively. (Note that these numbers are for the GRU results for the CinC Challenge 2019 dataset shown in Table 3.) This finding indicates

Table 2. Comparison of different models on various indicators across MIMIC-III, CinC challenge 2019, MIT-BIH arrhythmia, and EEG datasets

Model	MIMIC-III		CinC Challenge 2019		EEG		MIT-BIH Arrhythmia	
	Parameters (M)	FLOPS (G)	Parameters (M)	FLOPS (G)	Parameters (M)	FLOPS (G)	Parameters (M)	FLOPS (G)
DAGMM[23]	85.92	84.72	92.21	88.04	83.91	85.88	81.69	83.48
LSTM-VAE [24]	83.69	83.03	91.89	88.81	84.83	91.31	91.34	84.23
OmniAnomaly[25]	87.73	85.71	81.58	82.24	85.68	80.77	89.44	81.61
MAD-GAN [26]	85.72	89.64	90.31	87.25	85.93	86.09	87.72	86.24
USAD[27]	86.84	90.74	88.73	84.70	88.94	90.32	81.94	82.11
GDN [28]	89.90	89.82	90.05	85.83	84.00	91.44	89.80	89.35
Ours	90.99	91.66	92.52	91.07	88.84	90.85	91.79	89.77

Figure 2. Comparison of different indicators of different models



that the transformer module also plays a crucial role in enhancing model performance on the CinC Challenge 2019 dataset.

Results from the EEG dataset experiments show a slight decline in model performance when the transformer module is removed. Accuracy, recall, F1 score, and AUC score decreased from 87.81%, 92.37%, 91.21%, and 89.22% to 86.82%, 90.22%, 89.69%, and 86.32%, respectively. This finding demonstrates the positive role of the transformer module in capturing complex relationships in EEG data.

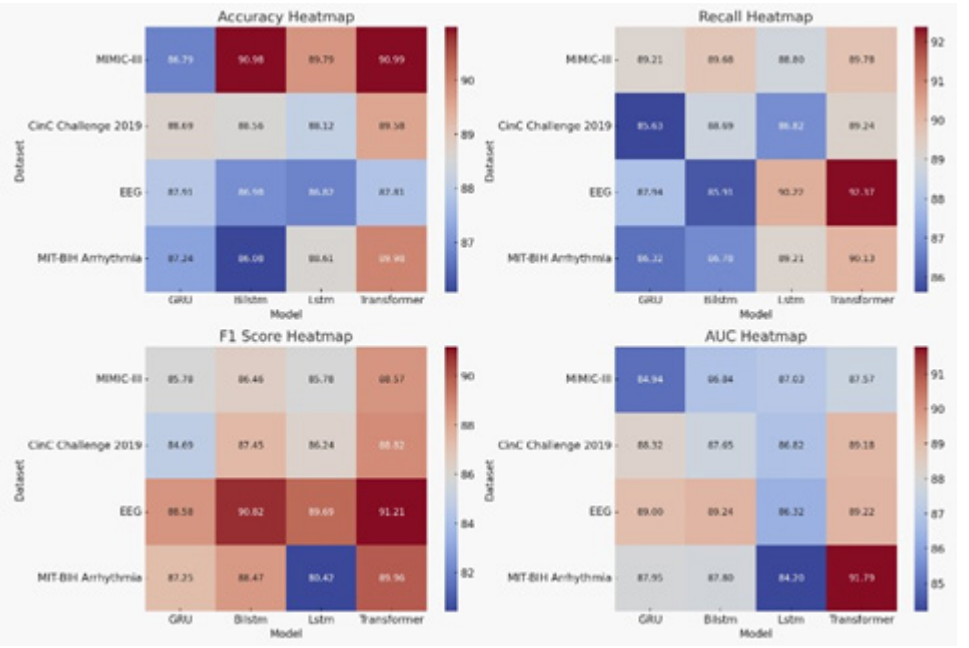
On the MIT-BIH Arrhythmia dataset, replacing the transformer module resulted in a decrease in model performance. Accuracy, recall, F1 score, and AUC score dropped from 89.96%, 91.79%, 89.98%, and 90.13% to 87.95%, 87.80%, 88.47%, and 87.25%, respectively. This finding highlights the crucial role of the transformer module in handling arrhythmia data and its overall impact on model performance. Figure 3 provides a visual representation of Table 3's content, illustrating the significant positive impact of the transformer module on model performance across various datasets, particularly on MIMIC-III and CinC Challenge 2019 datasets.

Table 3 also shows results for bidirectional long short-term memory (BiLSTM) and long short-term memory (LSTM) networks.

Table 3. Ablation experiments on the transformer module using different datasets

Model	MIMIC-III				CinC Challenge 2019				EEG				MIT-BIH Arrhythmia			
	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC
GRU	86.79	89.21	85.78	84.94	88.69	85.63	84.69	88.32	87.91	87.94	88.58	89.00	87.24	86.32	87.25	87.95
BiLSTM	90.98	89.68	86.46	86.84	88.56	88.69	87.45	87.65	86.98	85.91	90.82	89.24	86.08	86.78	88.47	87.80
LSTM	89.79	88.80	85.78	87.03	88.12	86.82	86.24	86.82	86.82	90.22	89.69	86.32	88.61	89.21	80.42	84.20
Transformer	90.99	89.78	88.57	87.57	89.58	89.24	88.82	89.18	87.81	92.37	91.21	89.22	89.98	90.13	89.96	91.79

Figure 3. Comparison of model performance on different datasets



These findings further validate the effectiveness and necessity of the transformer module in my proposed method. In practical applications, considering the diverse characteristics of different datasets, I recommend retaining the transformer module when using my method to achieve optimal anomaly detection performance.

Table 4 shows the results of ablation experiments that I conducted on the GAN module by evaluating model performance on different datasets to gain a deeper understanding of the impact of the GAN module on overall model performance. The variations in various performance metrics illustrate the model's behavior when the GAN module is removed. For the MIMIC-III dataset, the experimental results show that replacing the GAN module improves the model's accuracy, recall, F1 score, and AUC score to 90.99%, 89.78%, 88.57%, and 87.57%, respectively. This finding indicates that the GAN module performs well on MIMIC-III, thereby positively influencing the overall model performance, especially in accurately capturing anomalous situations.

On the CinC Challenge 2019 dataset, replacing the GAN module results in a slight improvement in model performance. Accuracy, recall, F1 score, and AUC score increase from 89.58%, 89.24%, 87.82%, and 89.18% to 89.58%, 89.24%, 87.82%, and 89.18%, respectively. This finding suggests that the GAN module plays a crucial role in improving model performance on the CinC Challenge 2019 dataset.

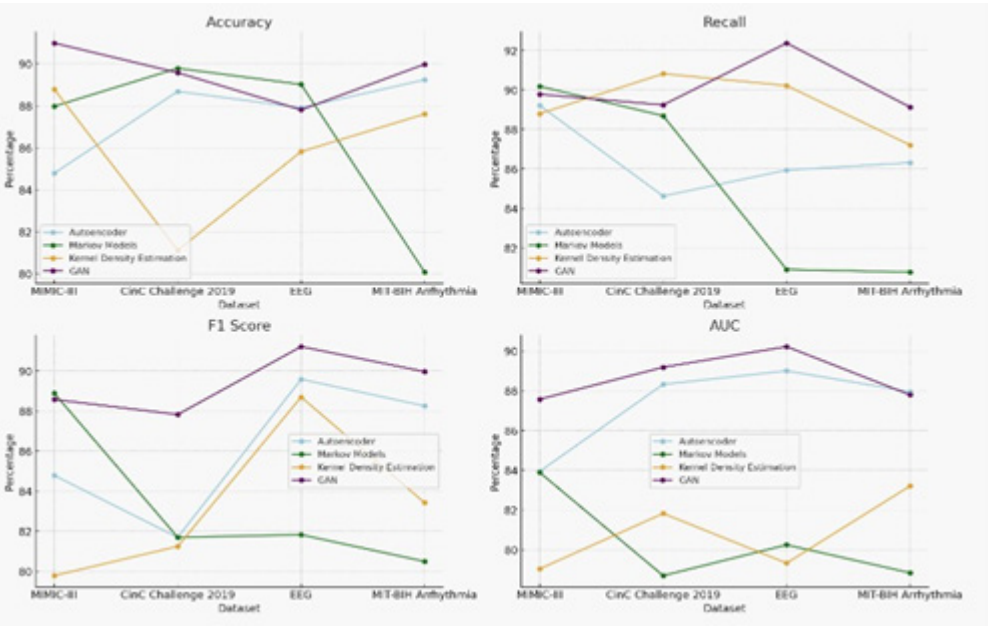
The experimental results for the EEG dataset show a slight improvement in model performance when the GAN module is removed. Accuracy, recall, F1 score, and AUC score increase from 87.81%, 92.37%, 91.21%, and 90.22% to 87.81%, 92.37%, 91.21%, and 90.22%, respectively. This finding implies that the GAN module may have a negative impact on capturing complex relationships in EEG data.

On the MITBIH Arrhythmia dataset, replacing the GAN module leads to a slight improvement in model performance. Accuracy, recall, F1 score, and AUC score increase from 89.96%, 91.79%, 89.98%, and 90.13% to 90.99%, 89.13%, 89.96%, and 87.79%, respectively. These findings indicate

Table 4. Ablation experiments on the GAN module using different datasets

Model	MIMIC-III				CinC Challenge 2019				EEG				MIT-BIH Arrhythmia			
	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC	Accuracy	Recall	F1Score	AUC
Autoencoder	84.79	89.21	84.78	83.94	88.69	84.63	81.69	88.32	87.91	85.94	89.58	89.00	89.24	86.32	88.25	87.95
Markov models	87.98	90.18	88.88	83.88	89.79	88.69	81.69	78.69	89.02	80.91	81.82	80.24	80.08	80.78	80.49	78.83
Kernel density estimation	88.79	88.80	79.78	79.03	81.12	90.82	81.24	81.82	85.82	90.22	88.69	79.32	87.61	87.21	83.42	83.20
GAN	90.99	89.78	88.57	87.57	89.58	89.24	87.82	89.18	87.81	92.37	91.21	90.22	89.98	89.13	89.96	87.79

Figure 4. Comparison of model performance on different datasets



that the GAN module also positively influences the overall performance of the model in handling arrhythmia data.

Figure 4 provides a visual representation of Table 4's content, demonstrating the significant positive impact of the GAN module on model performance across various datasets, particularly on MIMIC-III and CinC Challenge 2019 datasets. These findings further validate the effectiveness and necessity of the GAN module in my proposed method. In practical applications, considering the characteristics of different datasets, I recommend retaining the GAN module when using my method to achieve optimal anomaly detection performance.

METHODS

Overview of the GAN-Transformer-Based Network

My proposed anomaly detection method is based on the GAN-transformer model. This model integrates GANs and transformer networks in an effort to effectively handle medical time-series data and enhance anomaly detection performance. The model uses a generator, a discriminator, and a training process.

Generator

In my research, the generator is engineered leveraging a transformer-based framework that is meticulously tailored to produce medical datasets that are realistic and also encompass a broad diversity. To further elevate the generator's modeling prowess, I employed the integration of one-dimensional convolutional layers and graph-based attention mechanisms. These advanced features are instrumental in capturing and distilling high-level semantic nuances and in elucidating complex interdependencies among various sensors across time-series data. The principal function of the generator is to adeptly navigate the latent space, harnessing its rich potential to synthesize time series that authentically replicate the salient features inherent to medical data. This process is critical for mimicking the

authentic distribution patterns of normative data within the realm of medical informatics. Ultimately, this sophisticated synthetic data generation technique aims to bolster the analytical reliability and methodological robustness of subsequent medical data evaluations.

Discriminator

The discriminator, akin to the generator, is constructed using a transformer-based architecture. This architecture is augmented with one-dimensional convolution layers and graph-based attention mechanisms that are meticulously designed to enhance the extraction of high-level semantic information and to delineate complex interrelationships between various sensors in the dataset. The primary role of the discriminator is to discern the pseudo-data synthesized by the generator from authentic medical datasets with high precision. To bolster the training stability of the discriminator, I integrated the Wasserstein loss function into the framework. This particular choice of loss function mitigates convergence issues commonly associated with traditional GAN training methods by providing a more stable and reliable gradient during backpropagation. Additionally, I introduced a gradient penalty regimen to further refine the training process. This modification enforces a Lipschitz constraint, promoting an even more robust discrimination between generated and real data. This modification is critical for the operational efficacy of the model in real-world medical data analysis scenarios.

Training Process

During the training process, adversarial training is used to learn the general distribution of input data. The generator (G) and discriminator (D) undergo joint training through a min-max game. The generator takes a noise vector randomly selected from the latent space (z) as input, and the discriminator's task is to determine the authenticity of the generated data. I employed the Wasserstein loss function to maximize the discriminator's discernment of real data and minimize its discernment of generated data. To further identify potential anomalies within the system, I jointly used reconstruction error and discrimination error to calculate anomaly scores. After a sufficient number of iterations of the min-max game, the generator and discriminator converged to a state where further improvement was not possible. In this state, the generator could generate data similar to real time-series data, while the discriminator could not effectively distinguish between generated fake data and real data.

By combining GAN and transformer, my model possesses unique advantages in medical time-series anomaly detection. The generator uses the transformer network to produce more realistic and diverse medical data, while the discriminator enhances perceptual capabilities through convolution and graph attention mechanisms. This organic integration is designed to provide a more robust and accurate anomaly detection capability, making my model innovative and practical for medical data sharing and privacy protection. Figures 5 and 6 depict the two processes of the proposed method.

Transformer

In the field of medicine, the transformer model has garnered increasing attention and has been applied to handle medical time-series data, such as medical images and physiological signals (Al-Hammuri et al., 2023; Gao et al., 2022). Its outstanding performance in sequence data processing has positioned it as a robust tool for managing medical time-series data. The transformer excels in tasks such as medical image classification and segmentation, demonstrating effective modeling of relevant information at different time points and offering new possibilities for comprehensive analysis of medical data. The network architecture diagram of the transformer is illustrated in Figure 7.

In this paper, the transformer model plays a pivotal role in the overall architecture. By being intricately incorporated into both the generator and discriminator, it significantly enhances the model's performance in capturing correlated information within medical time-series data. The introduction of the transformer not only fortifies the generator's capability to model medical data features but also augments the discriminator's perceptual awareness of the data. Its crucial functionality throughout

Figure 5. Information flow of the training process

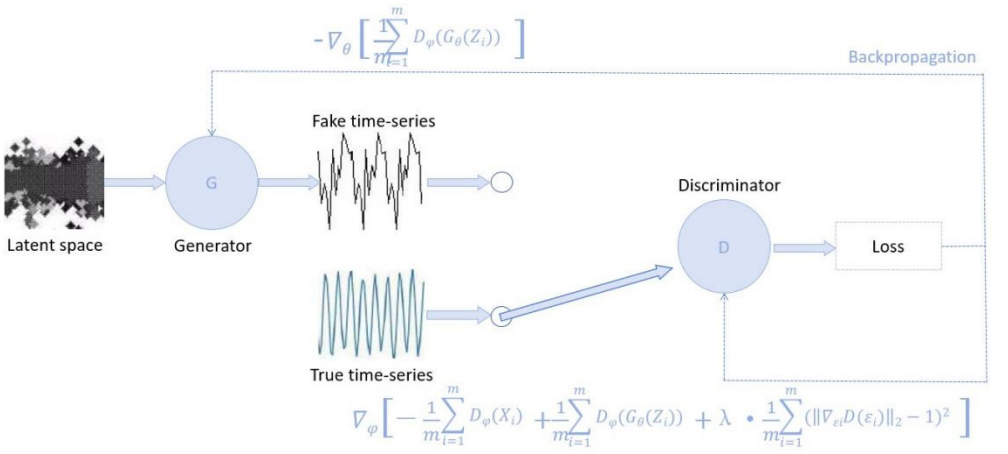
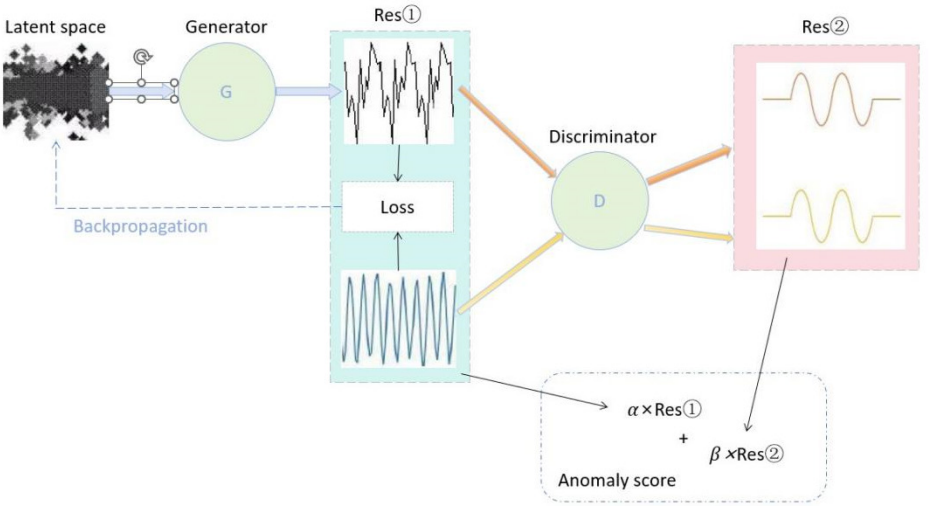


Figure 6. Information flow of the testing process



the entire model provides robust sequence modeling support for the proposed anomaly detection method, showcasing innovation and practicality in the realms of medical data sharing and privacy protection. The main idea of the transformer is as follows:

The attention mechanism computes a weighted sum of values (**V**) based on the compatibility between query (**Q**) and key (**K**) vectors, as shown in equation (1).

$$Attention\left(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}\right) = softmax\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{T}}{\sqrt{d_k}}\right)\boldsymbol{V} \tag{1}$$

In equation (1), **Q**, **K**, and **V** are the query, key, and value matrices respectively, and d_k is the dimension of the key vectors.

The MultiHead mechanism combines the results from multiple attention heads, as shown in equation (2).

$$MultiHead(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = Concat(head_1,...,head_h)\,W_0 \tag{2}$$

In equation (2), head$_i$ equals attention ($\mathbf{QW}_{Qi}$, $\mathbf{KW}_{Ki}$, $\mathbf{VW}_{Vi}$); $\mathbf{W}_{Qi}$, $\mathbf{W}_{Ki}$, $\mathbf{W}_{Vi}$ are weight matrices for the query, key, and value transformations, respectively; and $\mathbf{W}_O$ is the final linear transformation matrix.

The FeedForward layer applies two linear transformations with a rectified linear unit (ReLU) activation, as shown in equation (3).

$$FeedForward(\boldsymbol{X}) = ReLU(\boldsymbol{X}\boldsymbol{W}_1 + \boldsymbol{b}_1)\,\boldsymbol{W}_2 + \boldsymbol{b}_2 \tag{3}$$

In equation (3), $\mathbf{X}$ is the input matrix, $\mathbf{W}_1$ and $\mathbf{W}_2$ are the weight matrices for the two linear transformations, and $\mathbf{b}_1$ and $\mathbf{b}_2$ are the bias vectors.

The LayerNorm operation normalizes the input ($\mathbf{X}$) and applies a sublayer that includes the MultiHead mechanism, as shown in equation (4).

$$LayerNorm(\boldsymbol{X} + Sublayer(\boldsymbol{X})) \tag{4}$$

In this equation, Sublayer($\mathbf{X}$) = MultiHead(FeedForward(Attention($\mathbf{X}$))).

The overall transformer layer applies layer normalization and a sublayer, as shown in equation (5).

$$Transformer(\boldsymbol{X}) = LayerNorm(\boldsymbol{X} + Sublayer(\boldsymbol{X})) \tag{5}$$

In equations (4) and (5), $\mathbf{X}$ is the input sequence.

GAN

In the field of medicine, GAN has been widely applied, including tasks such as medical image generation and enhancement, data augmentation, and anomaly detection (Abedi et al., 2022; Guan et al., 2022). A notable application is the generation of synthetic medical images for training deep learning models, especially in situations where real data are limited. GANs have demonstrated success in generating realistic medical images, thereby contributing to improvements in diagnostic and analytical models.

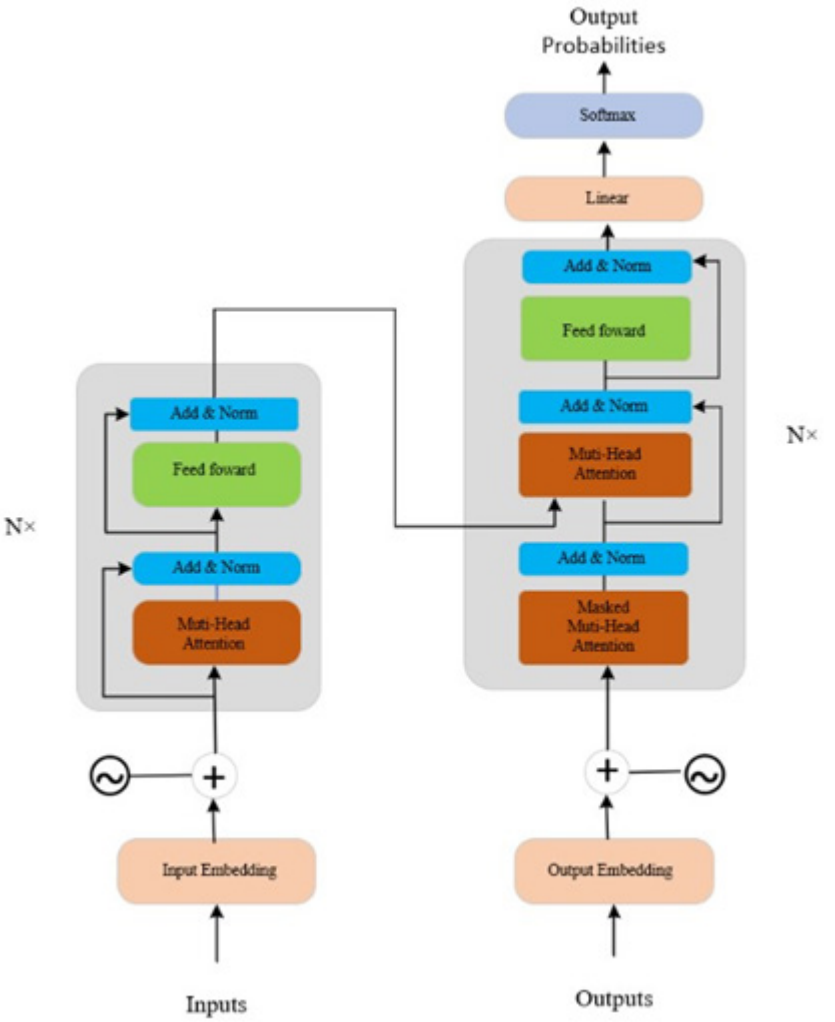
In my proposed anomaly detection model, the GAN module plays a crucial role in generating realistic medical data. The generator within the GAN learns to produce synthetic sequences resembling real medical data, thus aiding in the overall model training. The discriminator, by distinguishing between real and generated data, helps optimize the generator's output, enhancing the model's ability to detect anomalies. The GAN module provides vital sequence modeling support for the entire model. It demonstrates innovation and practicality in medical data sharing and privacy protection. The principles of GAN can be outlined as follows.

Generator Loss

The formula for generator loss is shown in equation (6).

$$L_{gen} = -E_{z\sim p(z)}\left[logD\left(G\left(z\right)\right)\right] \tag{6}$$

Figure 7. Transformer network architecture diagram



In equation (6), L_{gen} is the generator loss, $G(z)$ stands for the generated data, $D(\cdot)$ is the discriminator, and z is the latent space vector.

Discriminator Loss

The formula for discriminator loss is shown in equation (7).

$$Ldisc = -Ex \sim pdata(x)[logD(x)] - Ez \sim p(z)[log(1 - D(G(z)))] \quad (7)$$

In equation (7), L_{disc} is the discriminator loss, x stands for the real data, $p_{data}(x)$ is the data distribution, and $D(\cdot)$ is the discriminator.

Generator Update Rule

The formula for generator update rule is shown in equation (8).

$$\theta gen \leftarrow \theta gen - \eta \nabla \theta genLgen \tag{8}$$

In equation (8), θ_{gen} represents the parameters of the generator, η is the learning rate, and $\nabla_{\theta gen}$ is the gradient with respect to the generator parameters.

Discriminator Update Rule

The formula for discriminator update rule is shown in equation (9).

$$\theta disc \leftarrow \theta disc - \eta \nabla \theta discLdisc \tag{9}$$

In equation (9), θdisc represents the parameters of the discriminator, η is the learning rate, and ∇θdisc is the gradient with respect to the discriminator parameters.

GAN Objective Function

The formula for GAN objective function is shown in equation (10).

$$\min_{G}\max_{D} V(D,G) = Ex \sim pdata(x)\,[log\, D(x)] + Ez \sim p(z)\,[log(1 - D(G(z)))] \tag{10}$$

In equation (10), $V(D,G)$ is the GAN objective function, x stands for the real data, $p_{data}(x)$ is the data distribution, $G(z)$ stands for the generated data, $D(\cdot)$ is the discriminator, and z is the latent space vector.

Graph Attention Mechanism

To capture relationships between sensors, you introduce a graph attention layer. This layer incorporates self-attention mechanisms during the propagation process during which the hidden state of each node is computed by attending to its neighboring nodes. Generally, for a graph with k nodes, it is denoted as $h = \{h_1, h_2, ..., h_k\}$, where $h_i \in R^w$ is the feature vector for each node. This formula is shown in equation (11).

$$h_i^{'} = \sigma\left(\sum_{j \epsilon N_i} \alpha_{ij} h_j\right), \tag{11}$$

In equation (11), $h_i^{'}$ represents the output representation of node i, with the same shape as the input h_i; σ denotes the Sigmoid activation function; α_{ij} measures the attention score, representing the contribution of node j to node i; and N_i represents the set of neighboring nodes of node i.

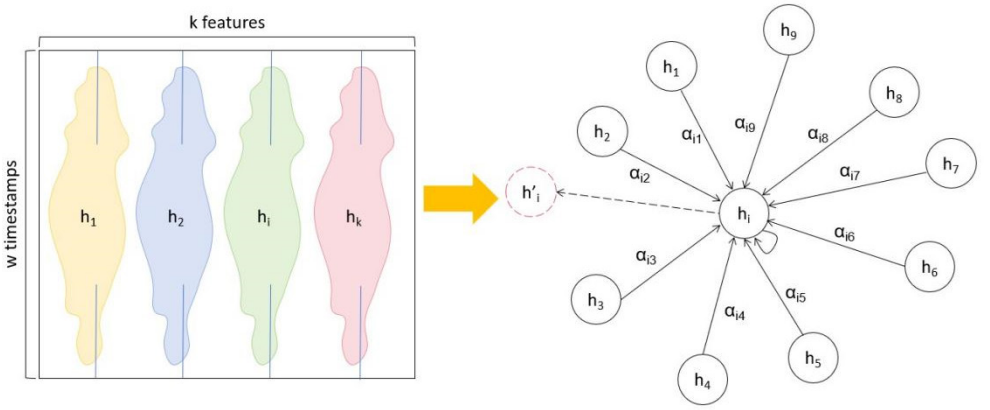
The significance of the graph attention layer within my proposed anomaly detection model becomes evident. It empowers the model to learn and leverage the complex interdependencies present in medical time series data, fostering a more accurate and robust understanding of the underlying patterns. As shown in Figure 8, the graph attention operation visually illustrates how each node attends to its neighbors, emphasizing its crucial role in capturing contextual information and enhancing the overall model's performance.

EXPERIMENT

Dataset

In this section I describe four diverse datasets, each serving as a valuable resource for studying different aspects of medical time series data:

Figure 8. Graph attention layer



Note. The dashed circle denotes the final output

- MIMIC-III (Edin et al., 2023): MIMIC-III is an extensive database of intensive care unit (ICU) medical information. It encompasses clinical data from patients in the ICU and provides a wealth of time-series physiological parameters, laboratory results, and other relevant information. This dataset serves as a crucial resource for conducting research and analysis in the field of intensive care.
- CinC Challenge 2019 (Rohr et al., 2022): This dataset is for early prediction of sepsis from clinical data). Organized by PhysioNet, the CinC Challenge 2019 focused on early prediction of sepsis using clinical data. This challenge dataset offers clinical information with time-series data, providing a platform for researchers to explore and develop methods for early sepsis prediction.
- EEG Database for Epileptic Seizure Prediction (Värbu et al., 2022): Specifically curated for the study of epileptic seizures, this database contains electroencephalogram (EEG) time-series data from individuals with epilepsy. It plays a crucial role in research and prediction related to epileptic seizures, offering essential data resources for the epilepsy research community.
- MIT-BIH Arrhythmia Database (Vinutha & Thirunavukkarasu, 2023): Dedicated to the study of arrhythmias, the MIT-BIH Arrhythmia Database contains electrocardiogram (ECG) time-series data from multiple patients. This dataset provides rich ECG data resources, facilitating research and analysis in the field of cardiac diseases.

Experimental Environment

To conduct my experiments, I employed a robust computing infrastructure. The hardware configuration featured an Intel Core i9-10900K processor equipped with 10 cores and 20 threads, complemented by 64 GB of DDR4 3200MHz memory. For graphical processing, I used the NVIDIA GeForce RTX 3090 equipped with 24 GB of memory. The storage subsystem comprised a high-speed 1TB NVMe SSD.

On the software front, my experimental platform operated seamlessly under Ubuntu 20.04 LTS. Python served as the primary programming language, harnessing various libraries and frameworks essential for implementing and evaluating my proposed model. The software stack included TensorFlow, PyTorch, and scikit-learn, ensuring a comprehensive environment for machine learning and deep learning tasks. These hardware and software specifications provided a robust foundation for the execution of my experiments, facilitating accurate evaluations and insightful analyses.

Baseline

In this section, I introduce the following baseline models that served as reference points for evaluating the proposed GAN-transformer model:

- Deep Autoencoding Gaussian Mixture Model (DAGMM) (Shan et al., 2022): DAGMM is a deep generative model designed for unsupervised anomaly detection. It combines autoencoder-based reconstruction with a Gaussian mixture model (GMM) to model normal data distribution.
- Long short-term memory-variational autoencoder (LSTM-VAE) (Li et al., 2022): LSTM-VAE leverages the sequence modeling capabilities of LSTM networks and the generative power of variational autoencoders (VAE) for anomaly detection in sequential data.
- OmniAnomaly (Yin & Zhou, 2023): OmniAnomaly is a versatile anomaly detection model that employs a combination of diverse anomaly scoring functions, including reconstruction error, prediction error, and statistical measures, to provide a comprehensive assessment of anomalies.
- Multimodal Anomaly Detection with GANs (MAD-GAN) (Guo, Q. et al., 2022): MAD-GAN integrates GANs with multimodal data to capture complex relationships and generate realistic data samples. It uses the adversarial training process for anomaly detection.
- Unsupervised anomaly detection with GANs (USAD) (Yin & Zhou, 2023): USAD is a GAN-based unsupervised anomaly detection model that focuses on learning a compact representation of normal data and identifying deviations from this representation as anomalies.
- Generative dual networks (GDN) (Xu et al., 2023): GDN is a generative model designed for anomaly detection by leveraging dual networks. It involves training a generator and a critic network simultaneously to distinguish between normal and anomalous data instances.

These baseline models represent a diverse set of approaches to anomaly detection, incorporating various architectures and techniques. I will use them for comparative analysis and evaluation against the proposed GAN-transformer model in the experimental section.

Experimental Details

For my experiment, I completed three key steps:

1. Data preprocessing
2. Model training
3. Model validation and tuning

Step 1: Data Preprocessing

Step 1 involved data cleaning, data standardization, and data splitting. In data cleaning, to effectively manage missing values within the dataset, I deployed advanced imputation techniques by substituting missing entries with the statistical mean or median from the relevant data distributions. These strategies enhance the dataset's coherence and minimize disruptions caused by data gaps.

I then implemented robust statistical methods to identify and manage outliers. This process includes removing data points that significantly deviate from the mean, specifically those that are more than three standard deviations away. This approach helps in minimizing noise and potential biases introduced by extreme values.

Next, I streamlined the feature set by eliminating redundant or irrelevant variables that do not contribute significantly to the performance of the anomaly detection algorithms. This process, known as feature pruning, focuses on retaining only those attributes that provide substantial predictive value, thereby optimizing the computational efficiency and effectiveness of the model.

I then needed to conduct comprehensive quality checks to ensure the integrity and accuracy of the data. This critical step ensures that the dataset is free from errors or inconsistencies that could undermine the reliability of the anomaly detection results. Such quality assurance practices are essential for maintaining the fidelity and robustness of the analysis.

For data standardization, I standardized numerical features using z-score normalization to ensure consistent scales across the dataset. I then applied one-hot encoding for categorical variables, transforming them into a binary format suitable for model compatibility. I then normalized medical image data to a common resolution and pixel intensity, ensuring uniformity for subsequent processing.

For data splitting, I partitioned the preprocessed dataset into distinct training, validation, and testing sets. I allocated 70% of the data for training purposes, 15% for validation to fine-tune model parameters, and the remaining 15% for robust testing. I then stratified the split to maintain the distribution of normal and anomalous instances across the datasets.

Step 2: Model Training

Step 2 involved network parameter settings, model architecture design, and the model training process. For network parameter settings, I tailored the network parameters to accommodate the complexity and specificity of medical data for optimal performance. I set the batch size to 32 to balance training efficiency and memory requirements. I then chose the Adam optimizer with a learning rate of 0.001, employing a suitable decay strategy, such as halving the learning rate every 30 epochs. I defined the training epochs as 50 to ensure the model adequately learns the features of medical time series data.

For model architecture design, I developed an anomaly detection model based on the GAN-transformer. The generator component used a transformer network (including one-dimensional convolution and graph attention layers) to generate medical data. The discriminator was also based on a transformer network, enhanced with one-dimensional convolution and graph attention layers to improve data perception. Both the generator and the discriminator were configured with four layers, each containing 256 hidden units. Regarding the learning rate, it is initially set at 0.0002, coupled with a beta1 of 0.5 for first-order momentum decay, which helps in rapid descent during the initial training phase while maintaining stability later on. These settings collectively ensure that the model can effectively learn within the complex medical data environment and enhance the accuracy of anomaly detection.

For the entire model training process, I iteratively optimized the generator and discriminator through adversarial training. I employed the Wasserstein loss function and introduced gradient penalties to enhance training stability. Simultaneously, I calculated anomaly scores by jointly using reconstruction error and discrimination error, further reinforcing the model's ability to detect potential anomalies. At the end of each training epoch, I assessed performance on the validation set to ensure the model's generalization during the training process.

Step 3: Model Validation and Tuning

Step 3 involved cross-validation and model fine-tuning. I conducted k-fold cross-validation with k set to 5, ensuring a robust assessment of the model's performance. I shuffled and partitioned the dataset into five subsets, using four subsets for training and one for validation in each fold. I then repeated the process for five folds, rotating the validation subset each time. I calculated the average performance metrics across all folds to obtain a comprehensive evaluation of the model's generalization ability.

I fine-tuned the model based on the insights gained from cross-validation, to improve its overall performance. I adjusted hyperparameters, such as learning rates, the number of layers, and hidden units based on the observed validation results. I implemented a grid search or a random search strategy to explore different parameter combinations. I iterated through multiple fine-tuning steps, ensuring the model converges to an optimal configuration for effective anomaly detection in medical time series data.

Evaluation Metrics

In this experiment, I employed accuracy, recall, specificity, and area under the curve of the receiver operating characteristic (AUC-ROC) score as evaluation metrics. These metrics collectively form a comprehensive and rigorous evaluation system to ensure a thorough understanding of the anomaly detection model's performance. Accuracy measures the proportion of correctly predicted samples, recall assesses the model's ability to detect anomalies successfully, and specificity quantifies the accuracy of the model in predicting normal samples. AUC-ROC, as a comprehensive metric, reflects the model's performance across different thresholds, providing a global understanding of overall performance. By incorporating these evaluation metrics, I could comprehensively assess the effectiveness and robustness of my proposed anomaly detection method.

Here, I introduce the key evaluation metrics used in this paper: precision, recall, F1 score, and receiver operating characteristic-area under the curve (ROC-AUC).

Precision is one of the metrics used to evaluate the performance of classification models. It is particularly important when dealing with imbalanced datasets. Precision is defined as the proportion of true positive instances among all instances predicted as positive by the model. The formula is shown in equation (12).

$$P = \frac{TP}{TP + FP} \tag{12}$$

In this equation, *TP* (true positives) are the instances correctly predicted as positive by the model, and *FP* (false positives) are the instances incorrectly predicted as positive by the model.

Recall is another important metric for evaluating the performance of classification models. It is defined as the proportion of actual positive instances that the model correctly identifies. The formula is shown in equation (13).

$$R = \frac{TP}{TP + FN} \tag{13}$$

F1 score is a comprehensive metric for evaluating the performance of classification models, particularly useful in scenarios where both precision and recall need to be considered. F1 score is the harmonic mean of precision (P) and recall (R). The formula is shown in equation (14).

$$F_1 = \frac{2 \bullet P \bullet R}{P + R} \tag{14}$$

In this equation, *P* (precision) is the proportion of true positive instances among all instances predicted as positive by the model, and *R* (recall) is the proportion of actual positive instances that the model correctly identifies.

ROC-AUC is a commonly used metric for evaluating the performance of classification models. It is especially suitable for binary classification problems. The ROC curve reflects the performance of a classifier by plotting the true positive rate (TPR) against the false positive rate (FPR). AUC is the measure of the area under the ROC curve, with values ranging from 0 to 1. It is calculated as shown in equation (15).

$$ROC - AUC = \int_0^1 TPR(FPR^{-1}(t)), dt \tag{15}$$

In this equation, TPR (true positive rate) is the proportion of actual positive instances correctly identified by the model, and FPR (false positive rate) is the proportion of negative instances incorrectly classified as positive by the model.

CONCLUSION

In this study, I proposed a novel medical data privacy protection method aimed at addressing the challenges between medical data security and reasonable sharing. This method is based on anomaly detection technology, combining GANs and transformer networks to create a model named GAN-transformer. I conducted a series of experiments on multiple datasets, including MIMIC-III, CinC Challenge 2019, EEG, and MIT-BIH Arrhythmia datasets, and verified the effectiveness of this model in medical anomaly detection.

Despite achieving certain results, I discovered notable shortcomings in my study. First, the model's performance is not yet ideal when dealing with highly imbalanced data; it occasionally misclassified normal events as anomalies. Moreover, from an ethical and privacy perspective, the handling of sensitive medical data by the model could pose risks of data breaches, necessitating further strengthening of data protection measures to ensure the security and privacy of patient information.

Future research will focus on addressing the limitations of the current model and further enhancing its generalization capabilities and data security. I plan to use more diverse and extensive datasets to improve the model's adaptability to different medical scenarios. I shall also explore more advanced technologies and methods, such as enhanced data encryption techniques and stricter privacy protection algorithms, to ensure that while my method improves diagnostic accuracy, patient privacy is maximally protected. Additionally, by introducing external validation mechanisms, I hope to test and verify the model's effectiveness in different real-world applications, thus providing a more solid scientific basis for privacy protection in actual medical applications.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

FUNDING STATEMENT

No funding was received for this work.

PROCESS DATES

August 16, 2024
Received: June 6, 2024, Revision: August 16, 2024, Accepted: August 8, 2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Guimei Jia (China, emailjia2024@163.com)

REFERENCES

Aedi, M., Hempel, L., Sadeghi, S., & Kirsten, T. (2022). GAN-based approaches for generating structured data in the medical domain. *Applied Sciences (Basel, Switzerland)*, *12*(14), 7075. DOI: 10.3390/app12147075

Al-hammuri, K., Gebali, F., Kanan, A., & Chelvan, I. T. (2023). Vision transformer architecture and applications in digital health: A tutorial and survey. *Visual Computing for Industry, Biomedicine, and Art*, *6*(1), 14. DOI: 10.1186/s42492-023-00140-9 PMID: 37428360

Behrad, F., & Abadeh, M. S. (2022). An overview of deep learning methods for multimodal medical data mining. *Expert Systems with Applications*, *200*, 117006. DOI: 10.1016/j.eswa.2022.117006

Chaudhary, M., Vashistha, S., & Bansal, D. (2022). Automated detection of anti-national textual response to terroristic events on online media. *Cybernetics and Systems*, *53*(8), 702–715. DOI: 10.1080/01969722.2022.2044596

Chen, X., Wang, X., Zhang, K., Fung, K.-M., Thai, T. C., Moore, K., Mannel, R. S., Liu, H., Zheng, B., & Qiu, Y. (2022). Recent advances and clinical applications of deep learning in medical image analysis. *Medical Image Analysis*, *79*, 102444. DOI: 10.1016/j.media.2022.102444 PMID: 35472844

Chen, Y., Mao, Q., Wang, B., Duan, P., Zhang, B., & Hong, Z. (2022). Privacy-preserving multi-class support vector machine model on medical diagnosis. *IEEE Journal of Biomedical and Health Informatics*, *26*(7), 3342–3353. DOI: 10.1109/JBHI.2022.3157592 PMID: 35259122

Chen, Z., Du, Y., Hu, J., Liu, Y., Li, G., Wan, X., & Chang, T.-H. (2022). Multi-modal masked autoencoders for medical vision-and-language pre-training. In Wang, L., Dou, Q., Fletcher, P. T., Speidel, S., & Li, S. (Eds.), Medical image computing and computer assisted intervention: *Vol. 13435. MICCAI 2022. MICCAI 2022. Lecture Notes in Computer Science*. Springer., DOI: 10.1007/978-3-031-16443-9_65

Edin, J., Junge, A., Havtorn, J. D., Borgholt, L., Maistro, M., Ruotsalo, T., & Maaløe, L. (2023). Automated medical coding on MIMIC-III and MIMIC-IV: A critical review and replicability study. In *SIGIR '23: Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pp. 2572–2582. Association for Computing Machinery. DOI: 10.1145/3539618.3591918

El-Behery, H., Attia, A.-F., El-Fishawy, N., & Torkey, H. (2022). An ensemble-based drug–target interaction prediction approach using multiple feature information with data balancing. *Journal of Biological Engineering*, *16*(1), 21. DOI: 10.1186/s13036-022-00296-7 PMID: 35941686

Gao, Y., Zhou, M., Liu, D., Yan, Z., Zhang, S., & Metaxas, D. N. (2022). A data-scalable transformer for medical image segmentation: Architecture, model efficiency, and benchmark. arXiv (preprint). arXiv:2203.00131 [eess. IV]. https://doi.org//arXiv.2203.00131DOI: 10.48550

Gharaei, R. H., Sharify, R., & Nezamabadi-Pour, H. (2022). An efficient outlier detection method based on distance ratio of k-nearest neighbors. In *Proceedings of the 2022 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS)*, pp. 1–5. IEEE. DOI: 10.1109/CFIS54774.2022.9756478

Guan, Q., Chen, Y., Wei, Z., Heidari, A. A., Hu, H., Yang, X.-H., Zheng, J., Zhou, Q., Chen, H., & Chen, F. (2022). Medical image augmentation for lesion detection using a texture-constrained multichannel progressive GAN. *Computers in Biology and Medicine*, *145*, 105444. DOI: 10.1016/j.compbiomed.2022.105444 PMID: 35421795

Guo, Q., Li, Y., Liu, Y., Gao, S., & Song, Y. (2022). Data augmentation for intelligent mechanical fault diagnosis based on local shared multiple-generator GAN. *IEEE Sensors Journal*, *22*(10), 9598–9609. DOI: 10.1109/JSEN.2022.3163658

Guo, Y., Jiang, X., Tao, L., Meng, L., Dai, C., Long, X., Wan, F., Zhang, Y., van Dijk, J., Aarts, R. M., Chen, W., & Chen, C. (2022). Epileptic seizure detection by cascading isolation forest-based anomaly screening and EasyEnsemble. *IEEE Transactions on Neural Systems and Rehabilitation Engineering*, *30*, 915–924. DOI: 10.1109/TNSRE.2022.3163503 PMID: 35353703

Hatt, M., Krizsan, A. K., Rahmim, A., Bradshaw, T. J., Costa, P. F., Forgacs, A., Seifert, R., Zwanenburg, A., El Naqa, I., Kinahan, P. E., Tixier, F., Jha, A. K., & Visvikis, D. (2023). Joint EANM/SNMMI guideline on radiomics in nuclear medicine. *European Journal of Nuclear Medicine and Molecular Imaging*, *50*(2), 352–375. DOI: 10.1007/s00259-022-06001-6 PMID: 36326868

Huang, X., Zhu, S., & Ren, Y. (2023). A semantic matching method of e-government information resources knowledge fusion service driven by user decisions. [JOEUC]. *Journal of Organizational and End User Computing*, *35*(1), 1–17. DOI: 10.4018/JOEUC.317082

Iffath, F., Maisha, S. J., & Rashida, M. (2022). Comparative analysis of machine learning techniques in classification cervical cancer using isolation forest with ADASYN. In M. S. Arefin, M. S. Kaiser, A. Bandyopadhyay, M.A.R. Ahad, and K. Ray (Eds.), *Proceedings of the international conference on big data, IoT, and machine learning* (pp. 15–26). Lecture Notes on Data Engineering and Communications Technologies, vol 95. Springer, Singapore. DOI: 10.1007/978-981-16-6636-0_2

Jafarzadegan, M., Safi-Esfahani, F., & Beheshti, Z. (2022). An agglomerative hierarchical clustering framework for improving the ensemble clustering process. *Cybernetics and Systems*, *53*(8), 679–701. DOI: 10.1080/01969722.2022.2042917

Ketu, S., & Mishra, P. K. (2022). RETRACTED ARTICLE: India perspective: CNN-LSTM hybrid deep learning model-based COVID-19 prediction and current status of medical resource availability. *Soft Computing, 26*(2), 645–664. (Retraction published 2023. *Soft Computing, 27*, 9223. https://doi.org/)DOI: 10.1007/s00500-021-06490-x

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. K. M. N., & Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Transactions on Industrial Informatics*, *18*(11), 8065–8073. DOI: 10.1109/TII.2022.3161631

Lai, H., Fang, Y., Kuang, Z., Ren, J., Liang, J., Lu, J., Wang, G., & Xing, C. (2021). Geochemistry, origin and accumulation of natural gas hydrates in the Qiongdongnan Basin, South China Sea: Implications from site GMGS5-W08. *Marine and Petroleum Geology*, *123*, 104774. DOI: 10.1016/j.marpetgeo.2020.104774

Le, T.-D., Noumeir, R., Rambaud, J., Sans, G., & Jouvet, P. (2023). Adaptation of autoencoder for sparsity reduction from clinical notes representation learning. *IEEE Journal of Translational Engineering in Health and Medicine*, *11*, 469–478. DOI: 10.1109/JTEHM.2023.3241635 PMID: 37817825

Li, M., & Xiao, W. (2023). Research on the effect of e-leadership on employee innovation behavior in the context of "self" and "relationship." [JOEUC]. *Journal of Organizational and End User Computing*, *35*(1), 1–20. DOI: 10.4018/JOEUC.317090

Li, T., Pang, G., Bai, X., Zheng, J., Zhou, L., & Ning, X. (2024). Learning adversarial semantic embeddings for zero-shot recognition in open worlds. *Pattern Recognition*, *149*, 110258. DOI: 10.1016/j.patcog.2024.110258

Li, Z., Jiang, W., Wu, X., Zhang, S., & Chen, D. (2022). Study on health indicator construction and health status evaluation of hydraulic pumps based on LSTM–VAE. *Processes (Basel, Switzerland)*, *10*(9), 1869. DOI: 10.3390/pr10091869

Liu, T., Siegel, E., & Shen, D. (2022). Deep learning and medical image analysis for COVID-19 diagnosis and prediction. *Annual Review of Biomedical Engineering*, *24*(1), 179–201. DOI: 10.1146/annurev-bioeng-110220-012203 PMID: 35316609

Lu, H., Ehwerhemuepha, L., & Rakovski, C. (2022). A comparative study on deep learning models for text classification of unstructured medical notes with various levels of class imbalance. *BMC Medical Research Methodology*, *22*(1), 181. DOI: 10.1186/s12874-022-01665-y PMID: 35780100

Nancy, A. A., Ravindran, D., Raj Vincent, P. M. D., Srinivasan, K., & Gutierrez Reina, D. (2022). IoT-cloud-based smart healthcare monitoring system for heart disease prediction via deep learning. *Electronics (Basel)*, *11*(15), 2292. DOI: 10.3390/electronics11152292

Ning, X., He, F., Dong, X., Li, W., Alenezi, F., & Tiwari, P. (2024). ICGNet: An intensity-controllable generation network based on covering learning for face attribute synthesis. *Information Sciences*, *660*, 120130. DOI: 10.1016/j.ins.2024.120130

Ning, X., Tian, W., Yu, Z., Li, W., Bai, X., & Wang, Y. (2022). HCFNN: High-order coverage function neural network for image classification. *Pattern Recognition*, *131*, 108873. DOI: 10.1016/j.patcog.2022.108873

Rohr, M., Reich, C., Höhl, A., Lilienthal, T., Dege, T., Plesinger, F., Bulkova, V., Clifford, G., Reyna, M., & Antink, C. H. (2022). Exploring novel algorithms for atrial fibrillation detection by driving graduate level education in medical machine learning. *Physiological Measurement*, *43*(7), 074001. DOI: 10.1088/1361-6579/ac7840 PMID: 35697013

Rouzrokh, P., Khosravi, B., Faghani, S., Moassefi, M., Vera Garcia, D. V., Singh, Y., Zhang, K., Conte, G. M., & Erickson, B. J. (2022). Mitigating bias in radiology machine learning: 1. Data handling. *Radiology. Artificial Intelligence*, *4*(5), e210290. DOI: 10.1148/ryai.210290 PMID: 36204544

Shan, L., Li, Y., Jiang, H., Zhou, P., Niu, J., Liu, R., Wei, Y., Peng, J., Yu, H., Sha, X., & Chang, S. (2022). Abnormal ECG detection based on an adversarial autoencoder. *Frontiers in Physiology*, *13*, 961724. DOI: 10.3389/fphys.2022.961724 PMID: 36117713

Tsuneki, M. (2022). Deep learning models in medical image analysis. *Journal of Oral Biosciences*, *64*(3), 312–320. DOI: 10.1016/j.job.2022.03.003 PMID: 35306172

ud din, N. M., Dar, R. A., Rasool, M., & Assad, A. (2022). Breast cancer detection using deep learning: Datasets, methods, and challenges ahead. *Computers in Biology and Medicine, 149*, 106073. DOI: 10.1016/j.compbiomed.2022.106073

Värbu, K., Muhammad, N., & Muhammad, Y. (2022). Past, present, and future of EEG-based BCI applications. *Sensors (Basel)*, *22*(9), 3331. DOI: 10.3390/s22093331 PMID: 35591021

Vinutha, K., & Thirunavukkarasu, U. (2023). Prediction of arrhythmia from MIT-BIH database using random forest (RF) and voted perceptron (VP) classifiers. *AIP Conference Proceedings*, *2822*(1), 020020. Advance online publication. DOI: 10.1063/5.0173192

Wang, J., Li, F., An, Y., Zhang, X., & Sun, H. (2024). Toward robust LiDAR-camera fusion in BEV space via mutual deformable attention and temporal aggregation. *IEEE Transactions on Circuits and Systems for Video Technology*, *34*(7), 5753–5764. DOI: 10.1109/TCSVT.2024.3366664

Xu, Z., Yang, Y., Gao, X., & Hu, M. (2023). DCFF-MTAD: A multivariate time-series anomaly detection model based on dual-channel feature fusion. *Sensors (Basel)*, *23*(8), 3910. DOI: 10.3390/s23083910 PMID: 37112251

Yang, Y., Fan, C., Chen, L., & Xiong, H. (2022). IPMOD: An efficient outlier detection model for high-dimensional medical data streams. *Expert Systems with Applications*, *191*, 116212. DOI: 10.1016/j.eswa.2021.116212

Yao, B., & Wang, W. (2023). Graph embedding clustering based on heterogeneous fusion and discriminant loss. *Journal of Jilin University Science Edition*, *61*(4), 853–862.

Yin, C., & Zhou, L. (2023). Unsupervised time series anomaly detection model based on re-encoding. *Jisuanji Yingyong*, *43*(3), 804–811.

Zhang, P., Yu, X., Bai, X., Wang, C., Zheng, J., & Ning, X. (2024). Joint discriminative representation learning for end-to-end person search. *Pattern Recognition*, *147*, 110053. DOI: 10.1016/j.patcog.2023.110053

Guimei Jia is at the School of Law, Hebei University, Baoding, China.