

Research on Medical Data Privacy Protection and Synthetic Data Generation Based on Generative Adversarial Networks

Zhiqiong Zou

Jingchu University of Technology, Jingmen, Hubei 448000, China

Keywords: Generative Adversarial Networks (GANs), Medical Data, Privacy Protection

Abstract: With the rapid development of medical informatization and artificial intelligence technology, medical data, as a core resource, faces dual challenges of privacy protection and efficient utilization that urgently need to be addressed. Traditional privacy protection methods often sacrifice data utility and are difficult to meet the needs of complex medical scenarios. Generative Adversarial Networks (GANs), as a powerful generative model, can generate high-quality synthetic data while protecting privacy. Therefore, this article proposes a medical data privacy protection method based on Generative Adversarial Networks (GANs). By constructing an improved GANs model, it generates synthetic medical data that not only protects privacy but also has high practicality, effectively improving the practicality of synthetic data and providing a new solution for the secure sharing and application of medical data.

1. Introduction

Driven by the wave of medical informatization, medical data has become the core asset of the modern healthcare system. The sensitive content contained in it, such as patient diagnosis and treatment information, health indicators, etc., is not only an important foundation for clinical research and disease prediction, but also a key object for personal privacy protection. With the deep penetration of artificial intelligence technology in the medical field, how to achieve secure sharing and compliant utilization of medical data has become a core bottleneck restricting the development of smart healthcare. Traditional techniques such as data anonymization and pseudonymization can to some extent reduce the risk of privacy breaches, but often come at the cost of sacrificing data availability, making it difficult to meet the requirements for data authenticity and integrity in complex medical scenarios. In recent years, the rise of Generative Adversarial Networks (GANs) has provided a new paradigm for medical data privacy protection. This deep learning model, which achieves data synthesis through the game of generator and discriminator, can not only generate synthesized data with highly similar distribution to the original data, but also avoid sensitive information leakage by controlling the generation process. The privacy preserving Generative

Adversarial Network (pGAN) model proposed in existing research has been validated for its ability to balance privacy protection and data utility on multiple medical datasets by optimizing the network structure and introducing differential privacy mechanisms. Experiments have shown that the synthesized data generated by the model achieves ideal levels of privacy risk assessment indicators while maintaining the original statistical features, and the performance of machine learning models trained on synthesized data is close to that of the original dataset. Currently, research on medical data privacy protection is facing a dual challenge: it needs to deal with increasingly complex data abuse attack methods, while also meeting the urgent demand of medical AI for high-quality training data. This article is based on the GANs technology framework and systematically explores the collaborative mechanism between medical data privacy protection and synthetic data generation, aiming to build a new generation of data governance solution that can resist re-identification attacks and support precision medical model training. By improving the structural design of generative adversarial networks and optimizing privacy protection mechanisms, the method proposed in this paper effectively enhances the practicality of synthesized data while protecting patient privacy, providing a feasible solution for the secure sharing and application of medical data.

2. Construction of privacy protection generative adversarial network model

2.1. GANs principle

Generative Adversarial Networks (GANs) were proposed by Goodfellow et al. in 2014, and their core idea stems from zero sum games in game theory. The model consists of two major neural networks: Generator (G) and Discriminator (D). The goal of generator G is to generate synthetic data samples $G(z)$ from a random noise vector z (usually following a Gaussian or uniform distribution) that are sufficient to "deceive" the discriminator; Discriminator D needs to accurately distinguish whether the input sample comes from the real data distribution $p_{data}(x)$ or the generator constructed distribution $p_g(x)$. Both continuously optimize their own abilities in adversarial training, forming a dynamic balance. The value function $V(G, D)$ can be expressed as:

$$\min_G \max_D V(D, G) = E_{x \sim p_{data}(x)} [\log D(x)] + E_{z \sim p_z(z)} [\log(1 - D(G(z)))] \quad (1)$$

In the early stages of training, D can easily recognize real and synthetic samples. As the generation ability of G increases, the difficulty of distinguishing D also increases. In an ideal state, when p_g approaches p_{data} infinitely, D cannot distinguish the source (i.e. $D(x)=0.5$), and the synthesized data has highly consistent statistical properties with the original data. The data generation capability of GANs provides a theoretical foundation for reconstructing medical data while protecting privacy.

2.2. Privacy Protection Generative Adversarial Network Model Framework

In the field of medical data privacy protection, the DP MedGAN model proposed in this paper constructs an improved generative adversarial network framework that integrates differential privacy mechanisms. As shown in Figure 1, the architecture is centered around a conditional generative adversarial network. By introducing patient non-sensitive attributes as conditional vectors and combining them with random noise input, the generator is guided to synthesize medical data samples with specific clinical features. The generator adopts a deep structure combining fully connected layers and deconvolution layers, and specially designs a multimodal input fusion module to concatenate and map condition vectors and noise vectors in the input layer, and achieve high-dimensional spatial representation learning through a shared weight fully connected layer. In

response to the frequent occurrence of sparse diagnostic codes in electronic health records, the output layer uses Sigmoid activation function instead of traditional Softmax, effectively supporting the synthesis requirements of multi disease co-occurrence scenarios.

The core of the model consists of three components: a conditional generator (G), a multi-layer perceptual discriminator (D), and a privacy protection layer. The generator receives the noise vector z and the patient's non sensitive condition vector c (such as age group, disease category), and synthesizes samples that meet specific clinical characteristics through conditional input guidance. The discriminator adopts a deep convolutional structure to learn complex local dependencies in medical data, such as the dynamic correlation of temporal vital signs. The privacy protection layer acts on the gradient update stage of the discriminator, achieving strict (ϵ, δ) - differential privacy assurance by injecting controllable Gaussian noise. The privacy utility balance mechanism is the core innovation of this framework. In the standard adversarial training loop, the generator attempts to generate realistic synthetic samples to deceive the discriminator, while the discriminator extracts features through convolutional layers to distinguish between real data and synthetic data. The key improvement is to perform L2 norm pruning on each sample gradient calculated by the discriminator before updating its parameters (to limit the risk of sensitive information leakage), and then add noise that satisfies Gaussian distribution $N(0, \delta^2 C^2 I)$ to the batch gradient mean. This design ensures that model parameter updates do not rely on any specific individual records, blocking privacy leakage paths from the source of synthetic data generation. In addition, the framework integrates an adaptive normalization module to uniformly process mixed types of features in medical data, such as continuous physiological indicators, discrete diagnostic codes, and categorical medication records. By dynamically adjusting the feature scale and distribution, this module significantly improves the modeling ability of generated data for complex medical data structures.

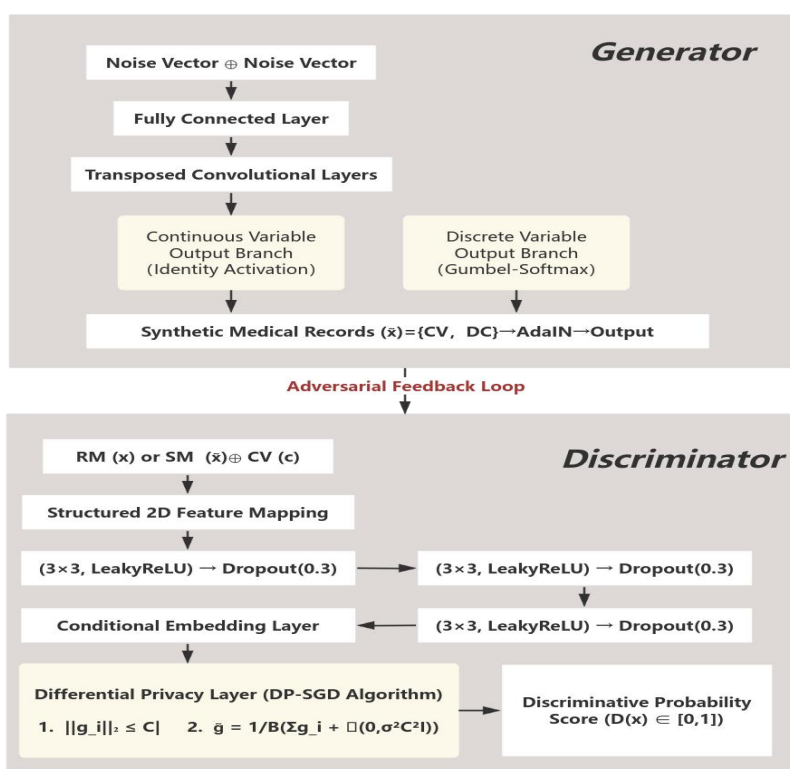


Figure 1. Model Architecture Schematic

2.3. Generator Design

As the core component of DP MedGAN, the design of the generator directly affects the quality and clinical rationality of synthesized data. In response to the multimodal and highly sparse characteristics of medical data, this work constructs a hybrid architecture based on deep fully connected and deconvolution layers (as shown in Figure 2). The input layer of the generator adopts a dual channel fusion mechanism: the Gaussian distributed noise vector $z \in \mathbb{R}^{128}$ is concatenated with the patient insensitive condition vector $c \in \mathbb{R}^k$ (encoding semantic information such as age segmentation and disease category) to form a joint input $[z][c] \in \mathbb{R}^{128+k}$. This vector is mapped to a high-dimensional hidden space through a fully connected layer with shared weights, and its transformation process is expressed as:

$$h_0 = \text{ReLU}(W_h \cdot [z][c] + b_h) \quad (2)$$

Where W_h is the weight matrix and b_h is the bias term. This design ensures that the generation process is controlled by the clinical context, ensuring that the pathological features of the output samples strictly match the conditional attributes.

To adapt to the complex structure of medical data, the hidden layer feature h_0 is gradually upsampled to the target dimension through two levels of deconvolution layers. The first deconvolution layer (kernel size 4×4 , step size 2) outputs the feature map h_1 , and the second layer (kernel size 3×3 , step size 1) generates h_2 . The key lies in the differentiated design of the mixed output layer: for continuous physiological indicators such as blood pressure and blood oxygen values, a linear activation function is used to directly return to the scalar; For discrete diagnostic codes (such as ICD-10) and categorical variables (medication type), Gumbel Softmax relaxation technique is introduced to achieve differentiable sampling. Specifically, for a discrete variable containing V categories, the output probability distribution is calculated as:

$$p_v = \frac{\exp((\log \pi_v + g_v)/\tau)}{\sum_{v=1}^V \exp((\log \pi_v + g_v)/\tau)} \quad (3)$$

Among them, $g_v \sim \text{Gumbel}(0,1)$ is the noise term, and τ is the annealing temperature parameter (reduced from 1.0 to 0.1 during training). This technology effectively avoids the problem of non differentiability in discrete sampling while approximating the true classification distribution.

Traditional Softmax cannot support the coexistence of multiple diseases due to normalization constraints, especially for the sparse multi label characteristics that frequently appear in electronic health records, such as patients with both hypertension and coronary heart disease. This design uses Sigmoid activation function instead of Softmax in the diagnostic code output layer. This mechanism allows each diagnostic code to be independently activated, generating binary labels by setting thresholds to accurately model common clinical comorbidities. Finally, the generator outputs a composite sample consisting of a triplet of continuous variables, discrete encoding, and multi label diagnostic information, fully covering the core elements of structured medical records.

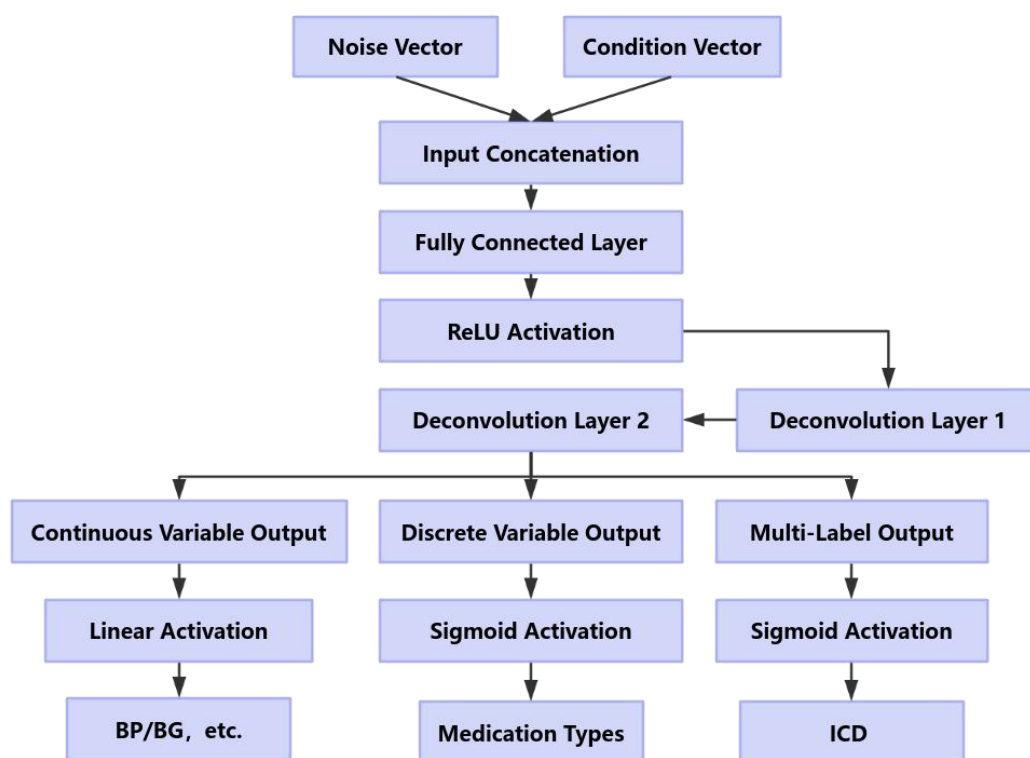


Figure 2. Generator Architecture Diagram

2.4. Discriminator configuration

Discriminator D has a dual responsibility in the DP MedGAN framework: it needs to accurately distinguish between real medical data and synthetic samples, while also providing a gradient perturbation interface for privacy protection mechanisms. This work designs a conditional discrimination architecture based on deep convolutional neural networks (CNN) to address the high-dimensional characteristics and temporal dependencies of medical records. The input layer first reshapes structured medical records (such as multi parameter monitoring data of patients within 24 hours) into a 32×32 two-dimensional feature map, and simulates the grid structure of image data by manually constructing spatial locality. For example, arranging heart rate, blood pressure, and blood oxygen values at adjacent time points as feature channels enables convolution operations to automatically capture dynamic correlations between physiological indicators (such as sudden drops in blood pressure often accompanied by an increase in heart rate).

The feature extraction module consists of three stacked convolutional layers, each layer using a 3×3 small-sized convolution kernel (step size 1) and a LeakyReLU activation function (negative slope $\alpha = 0.2$). The first layer outputs a 32×32 spectrogram with 64 channels, the second layer maintains spatial resolution through zero padding and expands to 128 channels, and the third layer downsamples to $16 \times 16 \times 256$ dimensions with a step size of 2. The key improvement lies in embedding Dropout layers (dropout rate $p=0.3$) in each convolutional layer, which significantly enhances the robustness of the model to medical data sparsity and outliers. To enhance the clinical rationality of generated samples, the discriminator introduces a conditional adversarial mechanism. Before fully connecting in the final layer, the patient's non sensitive attribute vector c (homologous to the generator input) is embedded into the feature space, and its joint representation is calculated

as:

$$h_{joint} = LeakyReLU(W_f \cdot Flatten(h_3) + W_c \cdot c) \quad (4)$$

Among them, h_3 is the final convolutional output, and W_f and W_c are the projection matrices. This mechanism forces the discriminator to simultaneously evaluate the "authenticity" and "contextual consistency" of the sample, such as detecting unreasonable levels of myocardial enzyme profiles in elderly patients in the generated data. Finally, the discrimination probability $D(x | c)$ is output through the Sigmoid function.

2.5. Privacy protection mechanism

The privacy protection core of DP MedGAN lies in the differential privacy (DP) modification of the discriminator training process, using the DP-SGD (Differentiated Private Stochastic Gradient Descent) algorithm framework proposed by Abadi et al. This mechanism injects controlled noise into the discriminator gradient to ensure that model parameter updates do not leak any individual record information. The implementation process is shown in Figure 4. In each training iteration, the first step is to calculate the loss gradient $\nabla \theta_D$ of the discriminator on the current batch of samples (including real data and generated samples). In response to the strong sensitivity of medical data, strict sample by sample gradient pruning is implemented: L2 norm constraints are applied to the gradient g_i of each sample

$$g_i \leftarrow g_i / \max\left(1, \frac{\|g_i\|_2}{C}\right) \quad (5)$$

The clipping threshold $C=1.0$ is set based on the weight Lipschitz constant after spectral normalization. This operation limits the upper bound of the gradient norm to C , preventing individual samples from excessively affecting the model and laying a sensitivity foundation for subsequent noise injection. The trimmed batch gradient enters the noise injection module. Mean the gradients of B samples within the batch and add noise that satisfies Gaussian distribution $N(0, \sigma^2 C^2 I)$:

$$\tilde{g} = \frac{1}{B} \left(\sum_{i=1}^B g_i + N(0, \sigma^2 C^2 I) \right) \quad (6)$$

The noise scale σ is a key parameter that balances privacy and utility. This design satisfies the (ϵ, δ) - differential privacy definition: for any adjacent dataset (with only one sample difference), the variational distance of the discriminator parameter update distribution is strictly constrained, and attackers cannot infer whether a specific individual exists by observing the model.

The precise accounting of privacy budget adopts Moment Accountant technology. Assuming the privacy loss for the t -th round of training is ϵ_t , the logarithm of the moment generation function is obtained by tracking the noise gradient distribution

$$\partial(\lambda) = \log E \left[\exp(\lambda M(D)) \middle| M(D') \right] \quad (7)$$

$$\text{Total Privacy Loss} = \min_{\lambda} \left[\frac{\partial(\lambda)}{\lambda} + \frac{\log(1/\delta)}{\lambda} \right] \quad (8)$$

3. Experiment and Results

The experiment used MIMIC-III and eICU intensive care datasets to extract temporal vital signs, laboratory examination indicators, diagnostic codes, and medication records from 10000 and 5000 patients, respectively. Using traditional k -anonymity ($k=5$), standard DP-GAN, and PATE-GAN as baseline models, privacy risk (membership inference attack success rate, maximum average

difference MMD) and data utility (statistical similarity: Jensen Shannon divergence, Wasserstein distance) were analyzed; Two dimensional evaluation of downstream task performance: AUC and F1 values for predicting mortality/readmission rates. Unified model configuration settings: DP MedGAN privacy budget $\epsilon=1.0$ ($\delta=10^{-5}$), noise scale $\sigma=1.5$, batch size $B=64$, training epochs $T=100$. All experiments were implemented on the NVIDIA Tesla V100 GPU using PyTorch 1.10.

Table 1. MIA Success Rate Comparison

Model	MIMIC-III Dataset	eICU Dataset
Raw Data	68.2	71.5
k-Anonymity	52.1	48.3
DP-GAN	33.7	36.9
PATE-GAN	28.4	30.1
DP-MedGAN	22.6	25.3

Table 1. Downstream Prediction Task Performance

Model Dataset	Mortality Prediction	Readmission Prediction
Raw Data	0.843	0.621
k-Anonymity	0.782	0.553
DP-GAN	0.881	0.587
PATE-GAN	0.798	0.571
DP-MedGAN	0.832	0.608

The MIA attack success rate of DP MedGAN on two datasets was significantly lower than the baseline (decrease>5%), indicating that its generated samples had the weakest correlation with the original individuals. Its MMD value suggests that it still maintains good overall distribution similarity under strong privacy constraints. The prediction model trained using DP MedGAN synthesized data showed that its mortality prediction AUC (0.832) and readmission rate F1 value (0.608) were closest to the original data performance (difference<3%), significantly better than other privacy protection methods.

4. Conclusion

With the increasing demand for high-quality data in medical AI and the increasingly strict privacy regulations, Generative Adversarial Networks (GANs) have become a key technology for solving the data sharing dilemma due to their ability to synthesize high fidelity medical data while protecting privacy. The DP MedGAN model proposed in this article achieves collaborative optimization of privacy security and data practicality by integrating conditional generation mechanism and differential privacy protection. This model not only effectively resists member inference attacks, but also generates synthetic data that is significantly better than traditional anonymization and benchmark generation models in terms of statistical distribution similarity and downstream clinical task performance. Its adaptive architecture design is compatible with multimodal medical data such as continuous physiological indicators and discrete diagnostic coding, providing a feasible path for cross institutional secure data collaboration and further promoting the construction of a privacy protected medical intelligent ecosystem.

Funding

This Paper (partly) supported by the Open Research; Fund of Key Laboratory of Nonlinear Analysis & Applications (Central China Normal University), Ministry of Education, P. R. China, NAA2025ORG011.

References

- [1] Hui X. *Medical Entity Recognition Based on Bidirectional LSTM-CRF and Natural Language Processing Technology and Its Application in Intelligent Consultation*[J]. 2025, 6(1),1-8
- [2] Bukun Ren, *Efficient Multimodal Visual Segmentation Model Based on Phased Fusion of Differential Modalities*, *International Journal of Big Data Intelligent Technology*, 2025, 6(1), 109-117
- [3] Jun Ye, *Multimodal Medical Data Intelligent Classification Method and System Implementation Based on Improved SVM and Similarity Learning Algorithm*, *International Journal of World Medicine*, 2025, 6(1),19-27
- [4] Yang, D., & Liu, X. (2025). *Research on Large-Scale Data Processing and Dynamic Content Optimization Algorithm Based On Reinforcement Learning*. *Procedia Computer Science*, 261, 458-466.
- [5] Zhang M. *Research on Optimization of Automatic Medical Image Recognition System Based on Deep Learning*[J]. *Journal of Computer, Signal, and System Research*, 2025, 2(4): 18-23.
- [6] Chen, H., Yang, Y., & Shao, C. (2021). *Multi-task learning for data-efficient spatiotemporal modeling of tool surface progression in ultrasonic metal welding*. *Journal of Manufacturing Systems*, 58, 306-315.
- [7] Cao, Y., Cao, P., Chen, H., Kochendorfer, K. M., Trotter, A. B., Galanter, W. L., ... & Iyer, R. K. (2022). *Predicting ICU admissions for hospitalized COVID-19 patients with a factor graph-based model*. In *Multimodal AI in healthcare: A paradigm shift in health intelligence* (pp. 245-256). Cham: Springer International Publishing.
- [8] Chen, H., Wang, Z., & Han, A. (2024). *Guiding Ultrasound Breast Tumor Classification with Human-Specified Regions of Interest: A Differentiable Class Activation Map Approach*. In *2024 IEEE Ultrasonics, Ferroelectrics, and Frequency Control Joint Symposium (UFFC-JS)* (pp. 1-4). IEEE.
- [9] Varatharajah, Y., Chen, H., Trotter, A., & Iyer, R. K. (2020). *A Dynamic Human-in-the-loop Recommender System for Evidence-based Clinical Staging of COVID-19*. In *HealthRecSys@RecSys* (pp. 21-22).
- [10] Chen, H., Varatharajah, Y., de Ramirez, S. S., Arnold, P., Frankenberger, C., Hota, B., & Iyer, R. (2020). *A retrospective longitudinal study of COVID-19 as seen by a large urban hospital in Chicago*. *medRxiv*, 2020-11.
- [11] Chen, H., Zhu, Y., Zuo, J., Kabir, M. R., & Han, A. (2024). *TranSpeed: Transformer-based Generative Adversarial Network for Speed-of-sound Reconstruction in Pulse-echo Mode*. In *2024 IEEE Ultrasonics, Ferroelectrics, and Frequency Control Joint Symposium (UFFC-JS)* (pp. 1-4). IEEE.
- [12] Chen, H., Zuo, J., Zhu, Y., Kabir, M. R., & Han, A. (2024). *Generalizable Deep Learning for Pulse-echo Speed of Sound Imaging via Time-shift Maps*. In *2024 IEEE Ultrasonics, Ferroelectrics, and Frequency Control Joint Symposium (UFFC-JS)* (pp. 1-4). IEEE.
- [13] Chen, H., Zuo, J., Zhu, Y., Kabir, M. R., & Han, A. (2024). *Polar-Space Frequency-Domain Filtering for Improved Pulse-echo Speed of Sound Imaging with Convex Probes*. In *2024 IEEE Ultrasonics, Ferroelectrics, and Frequency Control Joint Symposium (UFFC-JS)* (pp. 1-4). IEEE.
- [14] Chen, H., Varatharajah, Y., de Ramirez, S. S., Arnold, P., Frankenberger, C., Hota, B., & Iyer, R. (2020). *A retrospective longitudinal study of COVID-19 as seen by a large urban hospital in Chicago*. *medRxiv*, 2020-11.
- [15] Liu B. *Data Analysis and Model Construction for Crew Fatigue Monitoring Based on Machine Learning Algorithms*[J]. *optimization*, 2024, 8(5): 48-52.

- [16] Fan Y. *Financial Volatility Prediction Model Based On Denoising Autoencoder and Unstable Attention Mechanism*[J]. *Procedia Computer Science*, 2025, 261: 45-52.
- [17] Liu Y. *The Latest Application and Security Analysis of Cryptography in Cloud Storage Data Audit*[J]. *Procedia Computer Science*, 2025, 259: 984-990.
- [18] Ding M. *Quantitative Analysis of the Quantitative Impact of Optimizing User Engagement through Content Design*[J]. *Journal of Media, Journalism & Communication Studies*, 2025, 1(1): 36-41.
- [19] Ma, K., & Shen, J. (2024). *Interpretable Machine Learning Enhances Disease Prognosis: Applications on COVID-19 and Onward*. *arXiv preprint arXiv:2405.11672*.
- [20] Ma, K., Zhang, N., Mei, X., Feng, C., Hou, W., & Ye, Z. (2024, October). *Research on Optimization of Shared Bicycle Scheduling Based on Genetic Algorithm and LSTM*. In *2024 IEEE 6th International Conference on Civil Aviation Safety and Information Technology (ICCASIT)* (pp. 936-940). IEEE.
- [21] Zhang Y. *Research on Optimization and Security Management of Database Access Technology in the Era of Big Data*[J]. *Academic Journal of Computing & Information Science*, 2025, 8(1): 8-12
- [22] Yuan S. *Research on Anomaly Detection and Privacy Protection of Network Security Data Based on Machine Learning*[J]. *Procedia Computer Science*, 2025, 261: 227-236.
- [23] Wu, Hongjun. "Optimization of Malicious Code Detection Model for Web3. 0 Binary Files Based on Convolutional Neural Network and Graph Convolutional Neural Network." (2025). *International Journal of Multimedia Computing*, 6(1), 29-43
- [24] Li, J. (2025). *Research On Optimization Model of High Availability and Flexibility of Blockchain System Based on Microservice Architecture*. *Procedia Computer Science*, 261, 207-216.
- [25] Zhou Y. *Optimization of Multi dimensional Time Series Data Anomaly Detection Model Based on Graph Deviation Network and Convolutional Neural Network*[J]. *Procedia Computer Science*, 2025, 261: 199-206.
- [26] Tu, X. (2025). *The Application and Prospect of Machine Learning in Improving Production Efficiency*. *Artificial Intelligence and Digital Technology*, 2(1), 27-33.
- [27] Zhou Y. *Gateway Architecture and Security Design*[J]. *Journal of Computer, Signal, and System Research*, 2025, 2(4): 83-89.
- [28] Wang B. *Application of Efficient Load Test Strategies in Infrastructure*[J]. *Journal of Computer, Signal, and System Research*, 2025, 2(4): 69-75.
- [29] Jiang Y. *Automation and Life Cycle Management Optimization of Large-Scale Machine Learning Platforms*[J]. *Artificial Intelligence and Digital Technology*, 2025, 2(1): 20-26.
- [30] Fan, Sunjia, et al. "Defense methods against multi-language and multi-intent LLM attacks." *International Conference on Algorithms, High Performance Computing, and Artificial Intelligence (AHPCAI 2024)*. Vol. 13403. SPIE, 2024.
- [31] Huang J. *Digital Technologies Enabling Rural Revitalization: The Practice of AI and BIM in the Adaptive Reuse of Historic Buildings*[J]. *International Journal of Architectural Engineering and Design*, 2025, 2(1): 1-8.
- [32] Li B. *The Promoting Role of Data Analysis Technology in Sustainable Energy*[J]. *European Journal of Engineering and Technologies*, 2025, 1(1): 32-38.
- [33] Shi, Chongwei. "Genetic DNA Testing: Current Applications and Future Prospects." *Frontiers in Business, Economics and Management* (2024): 17(1),10-13
- [34] Li B. *Promoting the Effectiveness of Climate Policy through Data Analysis*[J]. *Journal of Education, Humanities, and Social Research*, 2025, 2(2): 118-124.

- [35] Yan, J. (2025). *AI-driven Streaming Customer Churn Prediction and Management Research. Mathematical Modeling and Algorithm Application*, 3(3), 1-4.
- [36] Wu L. *Data-Driven Process Improvement Methods and Results Sharmg[J]. European Journal of Business, Economics & Management*, 2025, 1(1): 111-117.
- [37] Zhang J. *Analysis of Dynamic Capacity Management Technology in Cloud Computing Infrastructure[J]. Journal of Computer, Signal, and System Research*, 2025, 2(4): 76-82.
- [38] Gu, Yiting (2025). "Practical Approaches to Developing High-performance Web Applications Based on React" *Frontiers in Science and Engineering*, 5(2), 99-105.
- [39] Zhang M. *Optimization of Medical Device Software Lifecycle Management Based on DevOps[J]. Journal of Medicine and Life Sciences*, 2025, 1(3): 8-13.
- [40] Zhao F. *Development Design and Signal Processing Algorithm Optimization of Traditional Chinese Medicine Pulse Acquisition System Based on CP301 Sensor[J]. Advances in Computer, Signals and Systems (2024)*, 8 (6): 106, 111.
- [41] Fan Y. *Automatic Optimization of Trading Strategies Based on Reinforcement Learning[C]//2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT). IEEE, 2025: 59-64.*