Scholar Publishing Group
International Journal of Neural Network
https://doi.org/10.38007/NN.2025.040101
ISSN 2790-2692 Vol. 4, Issue 1: 1-11

Research on Computer Network Information Security and Protection under the Background of Big Data

Yantao Tao [1,a*]
[1]*School of Artificial Intelligence, Jingchu University of Technology, Jingmen 448000, Hubei, China*
[a]*taoyantao@jcut.edu.cn*
[*]*Corresponding author*

Keywords: Big data security, track privacy protection, differential privacy technology, 5G edge computing, deep learning model

Abstract: In the context of big data, trajectory data, as an important resource in areas such as location services, urban planning, and business analysis, continues to expand its collection and application scope. However, sensitive information such as user behavior characteristics and social relationships contained in it can easily be uniquely identified through a few location points, leading to privacy leakage risks. Existing protection technologies (such as encryption and anonymization) have problems of being cracked or data distortion, while the integration of differential privacy, 5G edge computing and artificial intelligence provides a new path to balance privacy and availability. This research focuses on the privacy protection of trajectory data throughout its life cycle, and proposes two innovative mechanisms: first, the trajectory differential privacy protection mechanism (5GMEC-DP) based on 5G mobile edge computing improves the Geo Indistinguishability method through the client coordinate differential privacy algorithm and the MEC server truncation mechanism. When the privacy budget $\varepsilon=0.001$ and $\varepsilon=0.0005$, the average availability (AQ) of trajectory coordinates decreases by 64% and 81% respectively compared with the traditional methods, and the overall database availability loss (HD) decreases by 64% and 82%; Secondly, based on the LSTM-GAN trajectory data differential privacy publishing mechanism (LGAN-DP), combined with deep learning models to generate synthetic trajectories and apply differential privacy processing result sets, its HD index is improved by 40% to 50% compared to existing methods, and its time complexity is lower. In addition, a trajectory privacy protection and publishing system has been developed that integrates modules such as visualization, encryption, and caching. Currently, the system focuses on location encryption and trajectory publishing, and plans to expand modules such as peripheral recommendation and travel prediction in the future. Through the integration of 5G edge computing and deep learning model, this research provides an efficient and scalable technical solution for track data privacy protection, which significantly improves the balance between privacy and availability compared with traditional methods.

1. Introduction

Driven by big data and mobile internet technology, trajectory data, as an important resource in areas such as location services, urban planning, and business analysis, continues to expand its collection and application scope. However, sensitive information such as user behavior characteristics and social relationships contained in trajectory data can easily identify individual identities through a few unique location points, leading to privacy leakage risks. Existing protection technologies such as encryption, anonymization, and desensitization can provide basic protection, but there are problems such as cracking, data distortion, or decreased availability. In recent years, new technologies such as differential privacy, homomorphic encryption and confusion have made it possible to balance privacy and availability. The integration of 5G edge computing and artificial intelligence has further promoted the innovation of trajectory protection mechanism. The current research faces three core challenges: how to maintain data availability under high privacy protection intensity, how to adapt to the personalized needs of diverse application scenarios, and how to meet the compliance requirements of cross regional privacy regulations. In this context, this paper focuses on the privacy protection of trajectory data throughout its life cycle, and proposes two innovative mechanisms: first, build a trajectory acquisition model based on the characteristics of 5G mobile edge computing, combine the coordinate difference privacy algorithm and the edge server truncation mechanism, improve the traditional Geo indistinguishability method, and realize the collaborative optimization of high-intensity privacy protection and data availability; Secondly, design a trajectory data differential privacy publishing framework based on LSTM-GAN, generate synthetic trajectories through deep learning models, and use aggregate numerical denoising techniques to achieve privacy data publishing. Furthermore, this article integrates the aforementioned technologies to develop a trajectory privacy protection and publishing system that includes modules such as visualization, encryption, and caching, forming a complete solution from data collection to publishing.

2. Correlation theory

In the field of big data and computer network information security protection, multiple studies have promoted innovative practices through interdisciplinary methods and technological integration. In terms of hybrid models and deep learning applications, Kaya et al. proposed the GCN-LSTM hybrid architecture, which utilizes the spatial feature extraction ability of graph convolutional networks (GCN) and the time series modeling advantages of long short-term memory networks (LSTM) to achieve efficient anomaly detection of dynamic network data. Its multi-dimensional feature fusion significantly improves real-time performance, but it relies on high-quality annotated data and has high computational complexity; Liu Zhe's research combines memristor neural networks with improved time convolutional networks (TCNN) to accelerate computer vulnerability feature extraction through hardware level parallel computing, significantly improving classification accuracy. However, the interpretability of the model still needs to be optimized. In the field of privacy protection and data security, Wang Xin and others used edge computing architecture to implement localized data processing for motion trajectory prediction tasks, and encrypted trajectory data in combination with differential privacy technology to ensure data availability while reducing the risk of privacy disclosure, but the balance between encryption intensity and service quality needs further exploration; Jin focuses on port data privacy management and proposes an information security framework based on access control and homomorphic encryption, which protects sensitive information through dynamic permission allocation. However, the system deployment cost is high and the network bandwidth requirements are strict. In terms of interdisciplinary data fusion, Li Dan et al. used interpretable machine learning models to integrate street view images with environmental factors, and revealed key influencing factors of urban vitality through SHAP value analysis, providing quantitative basis for urban planning. However, the model's generalization ability is limited by regional cultural differences; Xu Xiaoyan introduced network big data mining and federated learning techniques into the field of asset pricing to achieve cross institutional privacy collaboration, but the efficiency of model training is affected by communication delays. In addition, Quansheng et al.'s review of network virtualization and cloud services pointed out that the integration of Software Defined Networking (SDN) and Network Function Virtualization (NFV) can improve resource utilization, but it needs to address compatibility issues in heterogeneous environments; Mouanda emphasizes that information assurance enhances system resilience through risk assessment and strategy optimization, and its preventive security mechanism design embodies "invisible power", but the implementation effect depends on organizational culture support. These studies collectively promote the transformation of information security protection from passive response to active defense, but breakthroughs are still needed in areas such as model lightweighting, cross domain collaboration, and ethical compliance.

3. Research method

3.1. Overview of Deep Learning Technology and Its Privacy Protection Applications

Deep learning is an important branch of machine learning, which simulates the structure and function of human neural networks and uses multi-layer nonlinear transformations to learn high-level representations from data. It is widely used in fields such as image classification, speech recognition, and natural language processing. Its core component is a neural network, and common structures include feedforward neural networks (enhancing expressive power through hidden layers), convolutional neural networks (capturing spatial features using convolution and pooling operations, suitable for image processing), recurrent neural networks and long short-term memory networks (processing long-range dependencies of sequence data through gate mechanisms and memory units to improve speech and text modeling capabilities), and generative adversarial networks (generating high-quality samples through adversarial training of generators and discriminators). During the training process, the backpropagation algorithm is relied upon to calculate gradients and optimize parameters using the chain rule. In recent years, deep learning technology has also been applied in the field of privacy protection: in IoT speech recognition, the PSRBL framework combines secure activation functions with bidirectional long short-term memory networks to reduce model training and recognition time while protecting speech data privacy; In terms of trajectory privacy protection, the black box feature of deep learning is utilized to prevent model reverse cracking. For example, social network interest point recommendation methods embed quantization, long short-term attention mechanisms, and combine user historical behavior and social relationship information to ensure trajectory privacy while recommending locations. These technologies provide effective solutions for balancing data utilization and privacy protection, demonstrating broad application prospects.

3.2. Research progress on the application of differential privacy theory

Differential privacy traces its roots to Warner's Randomized Response mechanism in 1965 which used probabilistic true or false answers for privacy protection. In 2006 Dwork formalized differential privacy ensuring attackers cannot infer individual sensitive information from query results even with full background knowledge while preserving data’s statistical utility. This is achieved by adding carefully calibrated random noise from a probability distribution to original data preventing accurate individual value inference.Three core principles underpin its implementation: controllable privacy strength adjusting noise based on context composability ensuring multiple noise additions align with a single effect and data independence making noise unaffected by individual entries. Its rigorous mathematical foundation has enabled widespread adoption in Apple Google and Microsoft systems trajectory analysis and healthcare data protection.Key concepts include adjacent datasets differing by one record ε-differential privacy where smaller ε means stronger protection and global sensitivity measuring query result changes from data modifications. Two primary mechanisms exist: the Laplacian mechanism adds noise proportional to query sensitivity while the exponential mechanism selects outputs probabilistically for non-numerical data.Combination rules allow serial deployments summing privacy budgets or parallel deployments using the maximum individual budget balancing privacy and computational efficiency. Current research splits into data generation models using GANs or VAEs for synthetic medical or financial data and query-based methods like privacy-preserving k-means clustering.While challenges like the privacy-utility trade-off persist differential privacy drives innovation in data sharing ensuring security without sacrificing analytical value in the data-driven era.

3.3. Overview of edge computing and Track Privacy Protection Technology

By deploying computing and data processing functions to edge devices close to the data source, edge computing has built a multi-layer architecture including edge devices, edge gateways, cloud centers and data centers. Its core advantages lie in improving data processing efficiency, reducing transmission delays and enhancing security. As an important branch of edge computing, mobile edge computing (MEC) supports real-time processing of local complex tasks by sinking cloud computing resources to the edge of 5G networks, and combines with the high-speed and low latency characteristics of 5G to provide efficient data processing models for Internet of Things, smart cities and other scenarios. At the privacy protection level, edge computing faces challenges such as data transmission security, storage security, access control and malicious attacks. It needs to ensure the security of data throughout its life cycle through encryption, authentication, intrusion detection and other technologies. As an important application object of edge computing, track data privacy protection needs to take into account the protection of individual and overall sensitive information: on the one hand, track privacy covers both explicit (such as sensitive locations) and implicit (such as social relations, health status, etc. inferred from tracks) sensitive information; On the other hand, privacy protection technologies need to balance data availability and leakage risks, including methods based on encryption, anonymization, model generation, blockchain, and differential privacy. These technologies support the application value of trajectory big data in fields such as transportation planning and LBS services by reconstructing, obfuscating, or encrypting trajectory data while ensuring user privacy.

4. Results and discussion

4.1. Efficient Trajectory Data Publishing via Deep Learning and Differential Privacy

In the context of big data, the system architecture for trajectory privacy protection is mainly divided into two categories: distributed and centralized. The former relies on user side processing but is limited by communication bandwidth and terminal computing capabilities, while the latter improves security and service efficiency through trusted third-party servers. Existing methods are mostly based on k-anonymity, prefix tree structure, or differential privacy fuzzification, but they suffer from difficulties in data aggregation, reduced availability, or high computational complexity. To this end, this article proposes the LGAN-DP algorithm, combined with LSTM-GAN to generate synthetic trajectories, and implements privacy protection through a differential privacy publishing module. The system model of this algorithm includes trajectory encoding, generator, discriminator, loss function, and differential privacy processing module. It ensures that the data meets the definition of ε - differential privacy through k-means clustering and Laplace noise addition. The experiment is based on the Foursquare NYC dataset (193 users, 3079 trajectories, 66962 trajectory points), and uses Hua's and Li's mechanisms as benchmarks to verify performance from three aspects: privacy (mutual information MI), availability (HD metric), and algorithm complexity. The experimental environment used Intel i9 10900K CPU, 64GB memory, and NVIDIA RTX3090 GPU, with a model training memory occupation of about 3GB. The results showed that LGAN-DP was significantly better than the baseline method in terms of privacy: when ε =0.1, its average MI was reduced by 41.7% and 18.2% compared to Hua's and Li's mechanisms, respectively; When N=80 and ε =0.5, the MI statistical value of LGAN-DP (0.0662) decreased by 80.5% and 86.4% compared to Hua's (0.3399) and Li's (0.4854), respectively, as shown in Table 1. In terms of usability, the HD metric of LGAN-DP is reduced by an average of 45% compared to the baseline method, indicating that its generated synthetic trajectories effectively reduce the impact of noise on data utility while maintaining spatiotemporal features.

Table 1. Comparison of MI indicators under different privacy parameters

ε	N=20	N=40	N=60	N=80
0.1	0.699/0.656/ 0.515	0.553/0.709/0.433	0.288/0.239/0.253	0.083/0.079/0.083
0.3	0.771/0.713/ 0.393	0.568/0.723/0.381	0.306/0.352/0.092	0.232/0.174/0.024
0.5	0.783/0.766/ 0.282	0.753/0.783/0.322	0.633/0.432/0.335	0.066/0.485/0.340
1.0	0.764/0.810/ 0.286	0.672/0.716/0.325	0.741/0.662/0.338	0.012/0.443/0.342

Algorithm complexity analysis shows that the time complexity of LGAN-DP is O (m * h) (where m is the number of samples and h is the hidden layer dimension), significantly lower than the O (t * k * m ^{2}) of the baseline method. In addition, LGAN-DP does not require retraining the model during dataset updates, only changing the input data, while the baseline method requires reconstruction of clusters, resulting in additional time overhead. Overall, LGAN-DP achieves a better balance between privacy protection strength, data availability, and computational efficiency through the collaborative optimization of deep learning and differential privacy, providing an innovative solution for secure release of trajectory data.

4.2. Design of privacy protection and publishing system for trajectory big data

In the big data environment, trajectory data has become an important support for daily services due to its wide application value, and users can easily obtain information about surrounding points of interest. However, the release of unprocessed trajectory data poses a serious risk of privacy leakage, leading to highly sensitive users and enterprises refusing to share data, thereby limiting the deep application of trajectory big data. To address this challenge, it is necessary to build a publishing system that balances privacy protection and data utility. The system requirements focus on three core capabilities: firstly, it is necessary to implement differential privacy encryption between location information and trajectory datasets, and provide quantitative evaluation of encryption errors; Secondly, it supports visual comparison of data before and after encryption, including map display of personal location coordinates, generalized trajectory routes, and encryption error ranges; Finally, integrate the route planning function based on spatiotemporal information to ensure user interaction experience. The system adopts a modular architecture design, as shown in Figure 1

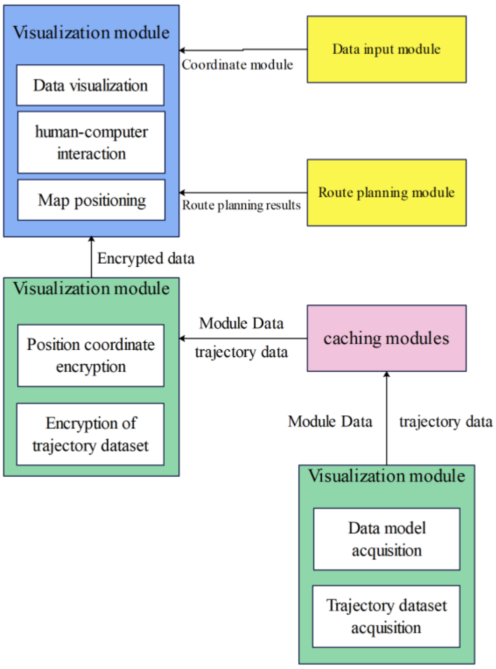

Figure 1. Module Relationship Diagram

It includes six key modules: the data acquisition module connects to the Python application through a database, extracts trajectory datasets, and stores them as H5 files; Cache module optimizes system performance by reducing duplicate calculations through parameter caching; The trajectory data encryption module serves as the core and uses differential privacy technology to encrypt the position coordinates and trajectory set; The data input module receives user location information and supports encryption or route planning operations; The route planning module generates path results based on SLDeep technology; The visualization module integrates map APIs to dynamically display trajectory data, encryption errors, and planned routes. This design deeply integrates privacy protection mechanisms with visual interaction technology, ensuring data security while providing users with an efficient and transparent trajectory data service solution. The entity classes include Trajectory (encapsulating the unique trajectory identifier tid and cluster center path sequence detailedPath), Coordinate, and KCentries (integrating timestamp timestamp, cluster number cenNumber, and coordinate object Coordinate), all of which ensure data encapsulation through private properties and public access methods, supporting the unique localization of generalized cluster center coordinates through timestamps and cluster numbers. The service class focuses on business logic implementation: the Administration class manages user authentication and data access permissions, provides password setting setPassword and front-end display interface, and encapsulates encrypted coordinate, trajectory, and cluster data in JSON format for visualization module calls; The Publishers class is responsible for publishing generalized trajectory datasets, maintaining trajectory lists pathsList and real/noisy counts, and supporting dynamic updates of published content; The CoordinateEncrypt class serves as the privacy protection core, generating encrypted coordinates requestCoordinate based on the differential privacy parameter epsilon for the original coordinates, and calculating the encryption error distance errDistance. The privacy protection strength is quantified through the error evaluation interface. This design decouples entity classes from business logic, combines access control and encryption algorithms, and supports flexible data interaction and visualization services while ensuring the privacy of trajectory data. It provides a modular and scalable implementation framework for computer network information security protection in big data environments.

4.3. Comparative analysis of evaluation effects

In the context of big data, the track big data privacy protection and publishing system has built a complete privacy security solution by integrating 5GMEC-DP, a differential privacy protection mechanism of 5G mobile edge computing, and LGAN-DP, a track data publishing mechanism based on LSTM-GAN. Introduction to the integrated functions and route planning entrance on the system homepage. Users can independently select their departure and destination through the input box, and combine SLDeep technology with Baidu Maps API to achieve optimal path planning based on time dimension. It also supports map zooming to view route details. The location information encryption function interface allows users to input latitude and longitude coordinates. The system generates encrypted coordinates that comply with the ε - privacy budget based on differential privacy algorithms. Each encryption result is randomized to enhance security, and the position offset error before and after encryption is visualized through color codes. The generalized trajectory dataset publishing module provides three-level interaction: users can retrieve the generalized cluster center coordinates corresponding to specific trajectory numbers and timestamps through the cluster center query button, and the query results are presented in latitude and longitude values; Clicking on the trajectory line will bring up a pop-up window displaying a complete map visualization of the generalized trajectory, including timestamp sequences and coordinate point distributions, achieving an intuitive mapping from abstract data to spatial paths. The system integrates deep learning models and privacy protection algorithms through web application technology, generating generalized trajectory data that meets the definition of differential privacy in the backend database. The frontend adopts a responsive design to support multi-dimensional data interaction, which not only ensures the privacy of trajectory data, but also improves data availability through visualization and route planning services, providing a practical technical framework and example for computer network information security protection in big data environments.

5. Conclusion

In the context of big data, the privacy protection of trajectory data needs to balance privacy and availability. Although existing technologies such as Geo Indifferentiability algorithm can provide location privacy protection, it is prone to data distortion under high privacy intensity (such as significant decrease in AQ and HD indicators); Traditional trajectory publishing methods suffer from low accuracy, insufficient efficiency, or inadequate privacy protection. This paper proposes two innovative mechanisms: first, the trajectory differential privacy protection mechanism (5GMEC-DP) based on 5G mobile edge computing, which limits the noise level of Geo Indistinguishability through the client longitude and latitude coordinate differential privacy algorithm and MEC server truncation mechanism. Experiments show that when ε =0.001 and ε =0.0005, the trajectory coordinate AQ decreases by 64% and 81% respectively compared with the traditional methods, and the overall database HD decreases by 64% and 82%, significantly improving the data availability under high privacy intensity; Secondly, based on LSTM-GAN trajectory data differential privacy publishing mechanism (LGAN-DP), combined with long short-term memory network and generative adversarial network to generate synthesized trajectories, the similarity is optimized through trajectory loss function, and the differential privacy processing result set is applied. The experiment shows that its HD index is improved by 40%~50% compared to existing methods, and the time complexity is lower, effectively balancing privacy protection and data publishing efficiency. Furthermore, this article integrates the aforementioned technologies to construct a trajectory privacy protection and publishing system, covering functions such as visualization, encryption, and caching. However, the current focus is on location encryption and trajectory publishing, with plans to expand modules such as peripheral recommendation and travel prediction in the future, evolving towards a more comprehensive trajectory data application management system. Compared with traditional schemes that rely on single encryption or anonymization, this research provides a more efficient and scalable technical path for the privacy protection of track data throughout its life cycle through the integration of 5G edge computing and deep learning.

References

[1] Chen, X. (2025). Research on the Application of Multilingual Natural Language Processing Technology in Smart Home Systems. Journal of Computer, Signal, and System Research, 2(5), 8-14.

[2] Yue X, Research on User Feedbak and Improvemet Mechanisms in Enterprise Social Media Pplication [J]. International Journal of Finance and Investment, 2025, 2(2): 25-28.

[3] Pan Y. Research on Cloud Storage Data Access Control Based on the CP-ABE Algorithm[J]. Pinnacle Academic Press Proceedings Series, 2025, 2: 122-129.

[4] Xiu L. Analyses of Online Learning Behaviour Based on Linear Regression Algorithm[C]//2025 IEEE International Conference on Electronics, Energy Systems and Power Engineering (EESPE). IEEE, 2025: 1333-1338.

[5] Pan Y. Research on the Design of a Real-Time E-Commerce Recommendation System Based on Spark in the Context of Big Data[C]//2025 IEEE International Conference on Electronics, Energy Systems and Power Engineering (EESPE). IEEE, 2025: 1028-1033.

[6] Yan J. Research on Application of Big Data Mining and Analysis in Image Processing[J]. Pinnacle Academic Press Proceedings Series, 2025, 2: 130-136.

[7] Xiu L. Research on the Design of Modern Distance Education System Based on Agent Technology[J]. Pinnacle Academic Press Proceedings Series, 2025, 2: 160-169.

[8] Hui, X. (2025). Research on Improving the Matching Efficiency between Cancer Patients and Clinical Trials Based on Machine Learning Algorithms. Journal of Medicine and Life Sciences, 1(3), 74-80.

[9] Chen A. Research on the Demand Hierarchy of E-Commerce Products Based on Text Mining and the IPA-KANO Model[J]. Pinnacle Academic Press Proceedings Series, 2025, 2: 153-159.

[10] Guo, Xingwen. “Study on the New Path of Chinese Commercial Banks' Globalization Development.” International Journal of Global Economics and Management (2024): 5(1),152-157.

[11] Fu, Yilin. "Design and Empirical Analysis of Financial Quantitative Trading Model based on VMD-DCNN-SGRU Architecture and Integrated System." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-7. IEEE, 2025.

[12] Xu, Yue. “Research on Software Development Amd Design of Computer Network Automatic Detection and Control System.” Scientific Journal of Technology (2025): 7(3),77-83

[13] Zhou, Yixin. "Design and Implementation of Online Log Anomaly Detection Model based on Text CM and Hierarchical Attention Mechanism." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-6. IEEE, 2025.

[14] Jiang, Yixian. "Research on Random Sampling Data Diffusion Technique in the Construction of Digital Object System Test Dataset." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-6. IEEE, 2025.

[15] Tu, Xinran. "Feature Selection and Classification of Electronic Product Fault Short Text by Integrating TF-IDF and Wor D2vec." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-6. IEEE, 2025.

[16] Ma, Zhuoer. "Research and Development of Financial Contract Text Information Extraction System based on M-BiLSTM and Our-M Models." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-7. IEEE, 2025.

[17] Yuan S. Design and Optimization of Network Security Situation Awareness Algorithm for Generative Adversarial Networks Targeting Attack Data and Traffic [C]//2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE, 2025: 1-6.

[18] Wei Z. Construction of Supply Chain Finance Game Model Based on Blockchain Technology and Nash Equilibrium Analysis[J]. Procedia Computer Science, 2025, 262: 901-908.

[19] Lai L. Research and Design of Data Security Risk Assessment Model Based on Fusion of Deep Learning and Analytic Hierarchy Process (AHP)[J]. Procedia Computer Science, 2025, 262: 747-756.

[20] Jiang Y. Research on the Optimization of Digital Object System by Integrating Metadata Standard and Machine Learning Algorithm[J]. Procedia Computer Science, 2025, 262: 849-858.

[21] An C. Research on High Frequency Financial Transaction Data Modeling and Cloud Computing Implementation Based on SSA-GA-BP Model[J]. Procedia Computer Science, 2025, 262: 859-867.

[22] Zhang X. Optimization and Implementation of Time Series Dimensionality Reduction Anti-fraud Model Integrating PCA and LSTM under the Federated Learning Framework[J]. Procedia Computer Science, 2025, 262: 992-1001.

[23] Wang C. Research on Modeling and Forecasting High-Frequency Financial Data Based on Histogram Time Series[J]. Procedia Computer Science, 2025, 262: 894-900.

[24] Huang, Jiangnan. "Online Platform user Behavior Prediction and Decision Optimization based on Deep Reinforcement Learning." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-6. IEEE, 2025.

[25] Wei X. Research on Preprocessing Techniques for Software Defect Prediction Dataset Based on Hybrid Category Balance and Synthetic Sampling Algorithm[J]. Procedia Computer Science, 2025, 262: 840-848.

[26] Pan H. Design and Implementation of a Cloud Computing Privacy-Preserving Machine Learning Model for Multi-Key Fully Homomorphic Encryption[J]. Procedia Computer Science, 2025, 262: 887-893.

[27] Cai Y. Design and Implementation of a Cross Platform i0s Application Development Framework Based on YAI Configuration Files[J]. Procedia Computer Science, 2025, 262: 939-947.

[28] Pan Y. Research on Enterprise Data Security Protection Technology on Cloud Platforms[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 30-36.

[29] Yan J. Analysis and Application of Spark Fast Data Recommendation Algorithm Based on Hadoop Platform[C]//2025 Asia-Europe Conference on Cybersecurity, Internet of Things and Soft Computing (CITSC). IEEE, 2025: 872-876.

[30] Hao, Linfeng. "Research on Automatic Driving Road Object Detection Algorithm Integrating Multi Scale Detection and Boundary Box Regression Optimization." In 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-6. IEEE, 2025.

[31] Guo Y. Research on Investment Bank Risk Monitoring and Early Warning Model Combining Factor Analysis and Artificial Neural Network[J]. Procedia Computer Science, 2025, 262: 878-886.

[32] 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).

[33] 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.

[34] 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.

[35] 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.

[36] Liu Y. The Latest Application and Security Analysis of Cryptography in Cloud Storage Data Audit[J]. Procedia Computer Science, 2025, 259: 984-990.

[37] Zhang M. Design of Object Segmentation and Feature Extraction Based On Deep Learning for AFM Image Processing and Analysis System[J]. Procedia Computer Science, 2025, 262: 982-991.

[38] 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.

[39] Cui N. Research and Application of Traffic Simulation Optimization Algorithm Based on Improved Road Network Topology Structure[C]//The International Conference on Cyber Security Intelligence and Analytics. Springer, Cham, 2025: 156-163.

[40] Zhang J. Design and Implementation of a Fuzzy Testing Framework for Hyper-V Virtualization Engine Based on Nested Virtualization and Coverage Orientation[C]//The International Conference on Cyber Security Intelligence and Analytics. Springer, Cham, 2025: 176-183.

[41] 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.

[42] Shen, D. (2025). AI-Driven Clinical Decision Support Optimizes Treatment Accuracy for Mental Illness. Journal of Medicine and Life Sciences, 1(3), 81-87.

[43] Yang D, Liu X. Collaborative Algorithm for User Trust and Data Security Based on Blockchain and Machine Learning[J]. Procedia Computer Science, 2025, 262: 757-765.

[44] Shi, Chongwei. “ Genetic DNA Testing: Current Applications and Future Prospects. ” Frontiers in Business, Economics and Management (2024): 17(1),10-13

[45] Ren B. Research Progress of Content Generation Model Based on EEG Signals[J]. Journal of Computer, Signal, and System Research, 2025, 2(4): 97-103.

[46] Liu Y. The Impact of Financial Data Automation on the Improvement of Internal Control Quality in Enterprises[J]. European Journal of Business, Economics & Management, 2025, 1(2): 25-31.

[47] Hua X. Optimizing Game Conversion Rates and Market Response Strategies Based on Data Analysis[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 37-43.

[48] Zhou Y. Research on the Innovative Application of Fintech and AI in Energy Investment[J]. European Journal of Business, Economics & Management, 2025, 1(2): 76-82.

[49] Huang J. Resource Demand Prediction and Optimization Based on Time Series Analysis in Cloud Computing Platform[J]. Journal of Computer, Signal, and System Research, 2025, 2(5): 1-7.

[50] Sheng C. Research on AI-Driven Financial Audit Efficiency Improvement and Financial Report Accuracy[J]. European Journal of Business, Economics & Management, 2025, 1(2): 55-61.

[51] Feng, Shanshan, Ke Ma, and Gongpin Cheng. "Risk evolution along the oil and gas industry chain: Insights from text mining analysis." Finance Research Letters 75 (2025): 106813.

[52] Zhang Q. Research on AI-Driven Advertising Optimization and Automated Decision System[J]. European Journal of Business, Economics & Management, 2025, 1(2): 62-68.

[53] Xu D. Design and Implementation of AI-Based Multi-Modal Video Content Processing[J]. European Journal of AI, Computing & Informatics, 2025, 1(2): 44-50.

[54] Li W. Audit Automation Process and Realization Path Analysis Based on Financial Technology[J]. European Journal of Business, Economics & Management, 2025, 1(2): 69-75.

[55] Liu X. The Role of Generative AI in the Evolution of Digital Advertising Products[J]. Journal of Media, Journalism & Communication Studies, 2025, 1(1): 48-55.

[56] Liu F. Research on Supply Chain Integration and Cost Optimization Strategies for Cross-Border E-Commerce Platforms[J]. European Journal of Business, Economics & Management, 2025, 1(2): 83-89.