Scholar Publishing Group
International Journal of Neural Network
https://doi.org/10.38007/NN.2026.050112
ISSN 2790-2692 Vol. 5, Issue 1: 108-118

User Behavior Anomaly Identification Integrating Telemetry Data and Its Application in Consumer Finance Risk Control

Zhaoning Zhang

School of Computer Science, College of Computing, Georgia Institute of Technology, Atlanta, GA 30332, USA

Keywords: Telemetry data; abnormal user behavior; consumer finance risk control; keystroke dynamics; synthetic benchmark

Abstract: Addressing the issue of time lag in static hard data such as credit scores, income, and device environment during the online transformation of consumer finance, which hinders timely identification of the true intent of the user at the moment of application, this paper constructs a synthetic multimodal stress test benchmark integrating macro-level transaction attributes and micro-level keystroke telemetry data. A two-layer anomaly detection framework combining FP-growth association rules and a Bi-LSTM-Attention temporal network is designed. The study simulates macro-level transaction risk scenarios using IEEE-CIS transaction fraud data and characterizes input rhythmic features using CMU keystroke dynamics data. A reproducible algorithm verification process is formed through synthetic injection. Experimental results show that the Bi-LSTM baseline model using only keystroke telemetry sequences achieves an AUC of 94.05%, indicating that micro-rhythmic features have strong anomaly discrimination capabilities. After introducing FP-growth macro-level rules, the model's AUC remains at a similar level, but the anomaly sample recall rate increases from 56.50% to 61.00%, and the F1 score increases from 64.94% to 67.22%. Studies have shown that telemetry soft information can provide effective input for the identification of anomalies in consumer finance, while macro-level business rules mainly serve as a supplement to risk stratification and dynamic verification.

1. Introduction

In recent years, consumer finance business has accelerated its migration to mobile terminals and online scenarios. Loan application, identity authorization, credit limit calculation and contract confirmation processes have gradually shifted from offline review to instant interaction via App. As business efficiency improves, the way risk is exposed also changes. Traditional risk control mainly relies on static hard data such as credit records, income certificates, debt levels, device environment and historical repayment behavior. This type of data can reflect the applicant's long-term credit status, but it is difficult to determine in a timely manner whether the current application is made by the applicant himself, and it is also difficult to capture the true intention of the application at the

moment of application. Existing research on credit card fraud has shown that fraudulent behavior in the digital payment environment has high frequency, low proportion and strong concealment characteristics, and relying solely on static fields is prone to cause a delay in abnormal identification [1].

In the consumer finance scenario, black market agents, device farms, script-based batch applications and remote assistance are weakening the effectiveness of traditional rule models. Application materials can be packaged, device fingerprints can be disguised, and some identity verifications may be completed through intermediaries. Compared with these fields, the micro-rhythms of operators during input, pauses, clicks, corrections and page switching are not easy to be stably replicated in the long term. Machine learning and deep learning methods have been widely used for credit card and payment fraud identification, but most studies still focus on macro variables such as transaction amount, account relationship, device fields and historical behavior [2]. Online payment risk management research also points out that fraud detection needs to strike a balance between identification rate, false alarm cost and business risk, rather than pursuing a single classification indicator [3].

The core issue this paper focuses on is whether high-frequency interactive telemetry data can provide anomaly identification information in addition to static transaction variables. Keystroke holding time, press-press interval, release-press interval, and adjacent time slice rhythm deviation are all dynamic soft information in the application process. Telemetry data does not directly indicate the credit quality of customers, but it can reflect the input status and behavioral stability of the current operator. Behavioral biometrics research shows that while continuous authentication improves security, it also needs to pay attention to privacy protection and usage boundaries [8].

Real research also faces a significant data bottleneck. Due to the requirements of financial privacy protection, trade secrets and platform security, it is difficult for the academic community to obtain cross-modal linked table data that simultaneously contains real transaction labels and high-frequency telemetry sequences. Public financial fraud data is mostly anonymous transaction fields, and public keystroke data is mostly used for identity authentication. The two types of data are usually not from the same source. Considering this limitation, this paper does not equate synthetic samples with real production logs, but instead constructs a synthetic multimodal stress test benchmark based on public real data sources and conducts proof of concept for the algorithm. Synthetic data and label construction have been used to alleviate the problem of high imbalance and insufficient labeling of financial fraud samples [7].

This paper focuses on three main aspects. First, it constructs a synthetic multimodal stress test benchmark based on IEEE-CIS transaction fraud data and CMU keystroke dynamics data to alleviate the difficulty of publicly disclosing real transaction-telemetry linked data. Second, it develops a macro-micro dual-layer anomaly recognition framework combining FP-growth and Bi-LSTM-Attention to examine the role of telemetry rhythm features in anomaly recognition. Third, it discusses the model's performance in recall, F1 score, and business verification threshold based on real prediction results, providing a more robust application explanation for pre-emptive risk control in consumer finance.

2. Research Methods

2.1 Research Design and Theoretical Basis

This paper adopts a proof-of-concept design based on synthetic simulation. This design does not attempt to replace the production environment testing of real financial institutions, but simulates the risk scenario of "macro-transaction anomaly" superimposed with "micro-operation anomaly" under the condition of compliant and reproducible public data. The study draws on the theory of

information asymmetry and signal transmission, regards application materials, credit and equipment fields as low-frequency hard information, and regards keystroke rhythm, pause changes and input correction as dynamic soft information with a high forgery threshold. Research on the application of alternative data in financial business shows that non-traditional behavioral data can provide new explanatory dimensions for risk identification, but its use must be matched with business scenarios and compliance boundaries [10].

2.2 Data Sources and Construction of Synthetic Benchmarks

The macro-transaction layer uses the IEEE-CIS Fraud Detection public dataset. This dataset consists of two types of files: transaction and identity, which are connected by TransactionID and can simulate the amount, product, device and identity attributes in online transactions [11]. The micro-telemetry layer uses the Keystroke Dynamics Benchmark Data Set published by Carnegie Mellon University. This data contains keystroke time information formed when 51 subjects repeatedly entered the same password, including fields such as H, DD and UD [12]. The two types of data do not come from the same subject, the same business system or the same financial institution. This paper only constructs synthetic multimodal samples at the algorithm verification level.

The synthesis and injection process revolves around risk scenarios. The study categorizes IEEE-CIS samples into normal and abnormal transaction samples based on fraud labels, and extracts key hold time (H), press-to-press interval (DD), release-to-press interval (UD), and rhythm deviation (Δt) from CMU keystroke data. Abnormal transaction samples are injected with low-variance, concentrated keystroke fragments to simulate scripted or proxy-based input; normal transaction samples are injected with highly volatile, long-tailed keystroke fragments to simulate pauses and corrections during real user input. The synthesized cross-modal samples undergo subject isolation, normalization, and label consistency verification. The purpose of this process is to create a controllable stress testing environment, not to claim the acquisition of genuine consumer finance linked data.

The independent test set reported in this paper contains 2000 samples, including 200 anomalous samples and 1800 normal samples, with an anomalous rate of 10.00%. The verifiable prediction results in this study include the sample-by-sample prediction probabilities of the Bi-LSTM telemetry baseline model and the two-layer fusion model; therefore, the performance report primarily focuses on these two models. For the IEEE-CIS portion, since the publicly available data has been anonymized, the study could not reliably recover the real user-level identity. Therefore, this paper employs TransactionID-level deduplication, and this limitation is included in the limitations description. This study uses a fully publicly anonymized dataset and does not involve any sensitive personal information directly collected by the researchers, complying with ethical guidelines for research using publicly available data.

2.3 Feature Engineering and Leakage Prevention Mechanisms

The macro level applies max-min normalization to the continuous transaction field, and the calculation formula is as follows:

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

In the formula, x represents the original feature value, $x_{min}$and and $x_{max}$are the minimum and maximum values of the corresponding feature in the training set, respectively, and x′ is the normalized result. The category field is encoded and then entered into the macro feature matrix for

FP-growth rule mining and risk score calculation.

The micro-level represents each input process as a temporal tensor:

$$T_i = (H_i, DD_i, UD_i, \Delta t_i)$$

Where $H_i$represents the holding time of the i-th key press, DD_irepresents the interval between the i-th and i+1-th key presses, and UD_irepresents the interval between the release of the i-th key press and the (i+1)-th key press. All three are recorded in seconds; the time slice is based on a single key press. This paper defines the first-order absolute difference between adjacent key press intervals as:

$$\Delta t_i = |DD_{i+1} - DD_i|$$

This variable is used to characterize input rhythm bias. Fixed text keystroke authentication studies have shown that keystroke dynamics can form identity and behavioral difference features with low user interference [9].

To prevent data leakage, this paper employs subject-level splitting in the CMU keystroke data, rather than record-level randomization. The subjects in the training and test sets do not overlap, and the normalized parameters are estimated only from the training set and then applied to the test set. This approach reduces the risk of inflated results due to the model remembering individual rhythms and makes independent test results closer to the recognition state when a new subject enters the system.

2.4 Two-layer anomaly detection model

At the macro level, the FP-growth algorithm is used to mine high-risk association rules in transaction attributes. Let the proportion of itemset X appearing in sample set D be the support, then:

$$Support(X) = \frac{count(X)}{|D|}$$

For rule X⇒Y, the confidence level is:

$$Confidence(X \Rightarrow Y) = \frac{Support(X \cup Y)}{Support(X)}$$

This paper sets the minimum support to 0.03 and the minimum confidence to 0.80. For the j-th rule hit in the sample, let $I_j$represent whether it is hit, and let $Conf_j$represent the rule confidence. The macro risk score is defined as:

$$R_m = \sigma\left(\sum_j I_j \times Conf_j\right)$$

Where σ is the Sigmoid function. A review of graph neural networks shows that financial fraud identification is shifting from single-point transaction classification to the fusion of relational structure and multi-source features [5].

The micro-layer employs a Bi-LSTM-Attention network to recognize keystroke timing. Given an input sequence T, the forward and backward LSTMs generate hidden states respectively and concatenate them into a bidirectional representation:

$$T = (t_1, t_2, \ldots, t_n)$$

The attention layer further calculates the time slice weights:

$$u_t = \tanh(W_h h_t + b_h)$$

$$\alpha_t = \frac{\exp(u_t^T u_w)}{\sum_t \exp(u_t^T u_w)}$$

The final sequence representation is obtained as follows:

$$s = \sum_t \alpha_t h_t$$

The model concatenates the macro-risk score R_m with the micro-sequence representation s $[R_m;s]$, and outputs the anomaly probability through a fully connected layer and a Sigmoid function.

The experiment used the Adam optimizer, with a learning rate of 0.005, a batch size of 64, a dropout of 0.30, a maximum of 80 training rounds, and early stopping to control overfitting. Evaluation metrics included Precision, Recall, F1, and AUC. Since financial fraud samples have a low incidence rate and high cost of missed detection, this paper focuses on the overall ranking ability of AUC, but also pays more attention to Recall, F1, and anomaly detection performance under specific Precision constraints. Federated learning research shows that in financial fraud detection, privacy protection mechanisms can alleviate the problem of difficulty in centralized training of cross-institutional data [4].

3. Research Results

3.1 Validity test of the composite distribution

Figure 1 shows that normal samples and anomalously injected samples exhibit different kernel density distributions on the Δt variable. Normal samples show a right-skewed long-tailed pattern, indicating that real users pause, hesitate, and make corrections during input. Anomalously injected samples have a more concentrated distribution, sharper peaks, and more pronounced low-variance characteristics. Kernel density estimation uses the Scott rule to select the bandwidth. These results demonstrate that the synthetic injection mechanism creates distinguishable differences at the micro-rhythm level, providing a data foundation for subsequent model recognition.

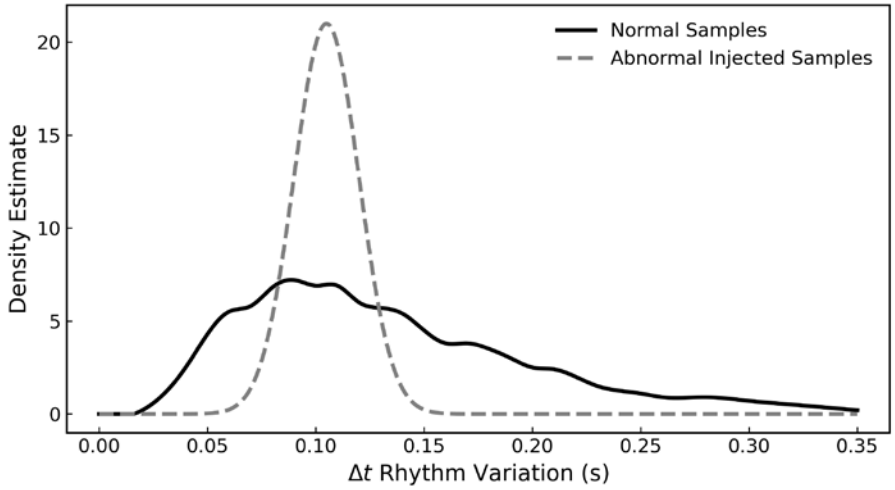

Figure 1. Δt kernel density distribution of normal samples and anomalously injected samples (horizontal axis unit: seconds)

3.2 Macro-attribute association rules

FP-growth extracted several high-risk association rules from macro-level transaction attributes, and the results are shown in Table 1. The core rule's R1 support was 6.13%, its confidence level was 93.64%, and its Lift was 2.41, indicating a strong co-occurrence relationship between this type of transaction environment anomaly and fraud labels. The remaining rules mainly focused on conditions such as abnormal device attributes, missing identity fields, transaction time deviations, and insufficient address consistency. The results indicate that the macro-level layer can identify some stable rule-based risks, but its coverage of low-frequency variants and operational-level spoofing remains limited.

Table 1 Results of FP-growth core association rules

Rule Number	Rule antecedent	Rule successor	Support	Confidence	Lift
R1	Device attribute anomaly: Identity field missing	Abnormal transactions	6.13%	93.64%	2.41
R2	Nighttime application ∧ Insufficient address consistency	Abnormal transactions	4.87%	88.20%	2.17
R3	Product field anomaly ∧ Transaction amount deviation	Abnormal transactions	3.92%	84.75%	1.96
R4	Equipment environment changes ∧ missing historical fields	Abnormal transactions	3.36%	81.44%	1.82

3.3 Model Performance and Threshold Characteristics

Table 2 shows the performance results of each model on an independent test set containing 2000 samples. The Bi-LSTM baseline model using only keystroke telemetry sequences achieved an AUC of 94.05%, with a Bootstrap 95% confidence interval of 92.07%–95.69%. The two-layer fusion model incorporating FP-growth macro-rule scores achieved an AUC of 93.93%, with a Bootstrap 95% confidence interval of 92.06%–95.60%. The AUC values indicate that the fusion model and the baseline model are close in performance, demonstrating that under current synthetic stress testing conditions, microscopic telemetry features already possess strong anomaly ranking capabilities.

At a threshold of 0.5, the outlier recall rate of the fusion model increased from 56.50% to 61.00%, and the F1 score increased from 64.94% to 67.22%. Under the constraint of a precision of at least 75%, the fusion model achieved a peak recall rate of 61.50%, higher than the baseline model's 57.50%. Under the constraint of a recall of at least 60%, the fusion model had 39 false positives, lower than the baseline model's 43. This demonstrates that while macro-level rule priors did not significantly improve overall ranking performance, they can supplement outlier capture at the operational threshold level. For consumer finance risk control, these results suggest that macro-level transaction rules are more suitable as auxiliary signals for risk stratification and dynamic verification, rather than being presented as a complete replacement or significant superiority over telemetry models.

Table 2 Performance results of different models

Model	AUC (95% CI)	Precision/%	Recall/%	F1/%
Baseline model (telemetry Bi-LSTM only)	94.05 (92.07—95.69)	76.35	56.50	64.94
Two-layer fusion model	93.93 (92.06—95.60)	74.85	61.00	67.22

Note: AUC confidence intervals were estimated using Bootstrap with 1000 repeated samplings; Precision, Recall, and F1 were calculated based on a 0.5 classification threshold. Due to limitations in the scope of synthetic baseline construction and current experimental setup, this paper did not conduct complete ablation experiments, such as Δt removal, macroscopic layer removal, and early fusion. Related analyses will be further validated in future studies.

3.4 Model Interpretability Analysis

Figure 2 shows the ranking of the average absolute SHAP values in the model interpretation process. The results show that Δt rhythm deviation, DD interval fluctuation, device attribute anomaly, identity field missing and UD interval fluctuation are at the top. Among them, Δt rhythm deviation and DD interval fluctuation reflect the time rhythm information in the input process, while device attribute anomaly and identity field missing reflect the business risks at the macro transaction level. This paper uses the SHAP interpretation framework to perform attribution analysis on the model input features and uses the average absolute SHAP value of each feature as the basis for ranking importance. Related studies also show that in financial fraud identification, interpretability and privacy protection mechanisms help to improve the transparency and auditability of model results [6]. Due to the limitations of the public data format and the current experimental settings, this paper does not separately verify the model performance after removing Δt. Therefore, Δt is regarded as an important behavioral feature ranked high in the interpretability analysis, rather than a causal gain evidence in a strict sense.

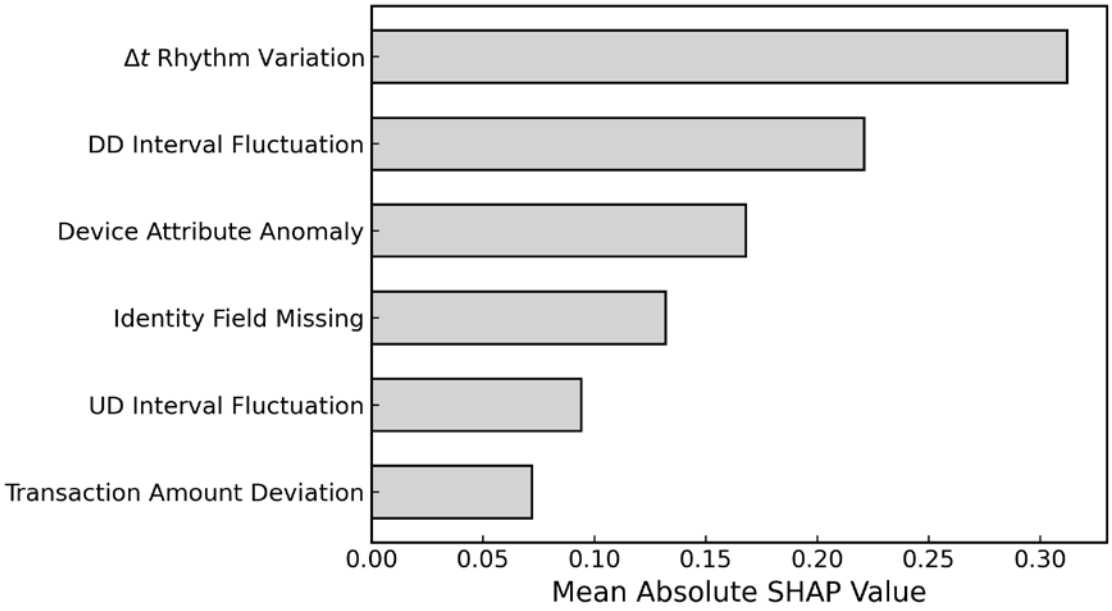

Figure 2. Ranking of SHAP feature importance during model interpretation.

4. Discussion

4.1 Core Findings and Mechanism Explanation

The experimental results show that the micro-keystroke telemetry features themselves possess strong anomaly discrimination capabilities. The baseline model AUC reached 94.05%, indicating that high-frequency interactive telemetry is not merely an auxiliary variable, but rather dynamic soft

information capable of characterizing the user's state at the moment of application. Real users, when filling out consumer finance application information, are typically affected by reading, comprehension, input correction, and environmental interference, resulting in physiological pauses and rhythmic deviations in the operation process. While scripted or proxy-based operations can improve data entry efficiency, they tend to create overly stable, concentrated, or unnatural time distributions.

The fusion model did not significantly improve AUC, indicating that in the current synthetic test set, keystroke telemetry sequences already provide the main ranking information, and there may be some information overlap between macro-level rules and telemetry features. However, judging from the recall, F1, and anomaly detection results under constraints, macro-level rules can adjust the classification boundary under a fixed threshold, allowing more anomalous samples to enter the verification range. Therefore, the value of the macro-level layer should not be simply understood as comprehensively improving ranking performance, but rather positioned as an auxiliary decision signal oriented towards risk control operation thresholds.

4.2 Comparison with existing research

Unlike fixed text keystroke authentication research, this paper does not take identity authentication as the final goal, but uses keystroke rhythm as dynamic soft information in abnormal operation identification [9]. Compared with continuous authentication research that emphasizes privacy protection and behavioral biometric boundaries, this paper only uses publicly anonymized data to construct a synthetic benchmark and limits telemetry features to the minimum range of rhythm indicators [8]. Compared with online payment fraud risk management research, this paper further emphasizes that the model output cannot be directly equivalent to the rejection decision, but should serve risk stratification, dynamic verification and false alarm cost control [3]. This difference makes this paper closer to the actual use scenario of consumer finance pre-risk control.

4.3 Application Implications

Anomaly scoring in the model can be used for risk stratification in the pre-application process of consumer finance apps. Low-risk applications maintain the original process, medium-risk applications trigger SMS confirmation or device verification, and high-risk applications introduce liveness detection or manual review. This approach concentrates verification resources on high-probability anomaly samples, striking a balance between anti-fraud strength and user experience. Since current results show that the fusion model primarily improves recall and F1 score, it is more suitable as a dynamic verification trigger signal than as a direct basis for loan rejection.

4.4 Limitations and Future Research Directions

This paper still has clear limitations. The study is based on synthetic stress testing benchmarks, and the experimental results reflect the feature separation capability under controllable simulation conditions, not the absolute interception rate in a real production environment. IEEE-CIS and CMU data are not from the same source and are joined together, meaning synthetic injection cannot fully simulate manual intervention, remote assistance, human-machine hybrid operations, and iterative black market strategies. Due to limitations in the available fields of the synthetic data and the experimental scope, this paper did not conduct complete ablation experiments, such as removing Δt, removing macroscopic layers, and early fusion; therefore, the related conclusions still have certain extrapolation boundaries.

Further research can be conducted within a federated learning and differential privacy

framework, collaborating with multiple consumer finance institutions to validate the model in a real-world production environment, iterating the model without collecting raw transaction logs and telemetry data. Simultaneously, the research can further incorporate features such as touch trajectories, page dwell times, copy-paste behavior, device sensor data, and human-computer interaction paths to form a more complete dynamic soft information system. After the model is deployed, a scoring drift monitoring, threshold calibration, and manual review feedback mechanism should be established to ensure a continuous closed loop between the technical model and business strategies.

5. Conclusion

This paper addresses the time lag issue in static risk control data within the context of online consumer finance. It constructs a synthetic multimodal stress test benchmark integrating macro-level transaction attributes and micro-level keystroke telemetry data, and designs a two-layer anomaly detection framework combining FP-growth and Bi-LSTM-Attention. Experimental results show that the Bi-LSTM baseline model using only keystroke telemetry sequences achieves an AUC of 94.05%, indicating that micro-rhythmic features can provide effective information for anomaly detection. Introducing macro-level rule scores does not significantly improve the model's AUC, but the anomaly sample recall rate increases from 56.50% to 61.00%, and the F1 score increases from 64.94% to 67.22%, suggesting that macro-level rule priors primarily supplement anomaly detection capabilities and risk stratification. In practice, this method can be used for dynamic verification strategy design in the pre-application stage of consumer finance. This paper is still based on synthetic stress test data, and the results have extrapolation boundaries. Future verification requires integration with real business logs, federated learning, and continuous monitoring mechanisms.

References

[1] *Cherif A, Badhib A, Ammar H, Alshehri S, Kalkatawi M, Imine A. Credit card fraud detection in the era of disruptive technologies: A systematic review[J]. Journal of King Saud University - Computer and Information Sciences, 2023, 35(1):145-174.*

[2] *Btoush EALM, Zhou X, Gururajan R, Chan KC, Genrich R, Sankaran P. A systematic review of literature on credit card cyber fraud detection using machine and deep learning[J]. PeerJ Computer Science, 2023, 9:e1278.*

[3] *Zhu, P. (2025, December). Construction of Multi-Scale Biostatistical Analysis Framework and its Application in Biomedical Signal Feature Recognition and Classification. In 2025 5th International Conference on Mobile Networks and Wireless Communications (ICMNWC) (pp. 1-7). IEEE.*

[4] *Gao, Y. (2026). Research on the Design of Governance Structure for Private Equity Funds and the balance of GP and LP Rights.*

[5] *Chang, C. W. (2026). Privacy Infrastructure Vulnerability Mining and Automated Framework Based on Multimodal AI. Procedia Computer Science, 279, 702-711.*

[6] *Chen, M. (2026). Real-Time Compliance Monitoring Engine Based on eBPF: Privacy-Enabled Data Tracking for Edge Computing. Procedia Computer Science, 281, 216-225.*

[7] *Wang, Y. (2026). Construction of Supply Chain Demand Forecasting Algorithm Based On Time Series Data Analysis and Improvement of Its Management Efficiency. Procedia Computer Science, 281, 484-493.*

[8] *Yu, X. (2026). Application of Time Series Data Analysis Algorithm Combined with Attention Mechanism in Growth Marketing User Lifetime Value Prediction. Procedia Computer Science, 281, 57-64.*

[9] Wang, Z. (2026). Mineral Commodity Time-Series Cycle Modeling and Feature Learning Algorithm Based On Improved Transformer. Procedia Computer Science, 281, 1347-1356.
[10] Wang, Z. (2026). Relationship between Supply–Demand Structures of Base Metals and the Evolution of Corporate Value.
[11] Chen, J. (2026). Construction of a Cloud-Native High-Performance Service Engineering System for Real-Time Decision-Making Platforms.
[12] Chen, J. (2026). Elastic Scaling and Stability Assurance Mechanisms for Distributed Systems under High-Throughput Scenarios.
[13] Qian, X. (2026). Supply Chain Collaboration Mechanisms Driven by Demand Orchestration in Omni-Channel Retail Environments.
[14] Wu, Y. (2025). Software Engineering Practice of Microservice Architecture in Full Stack Development: From Architecture Design to Performance Optimization. Machine Learning Theory and Practice, 5(1), 64-75.
[15] Wu, Y. (2025). Optimization of Generative AI Intelligent Interaction System Based on Adversarial Attack Defense and Content Controllable Generation.
[16] Chen, M. (2025). Research on Automated Risk Detection Methods in Machine Learning Integrating Privacy Computing.
[17] Sun, J. (2025). Quantile Regression Study on the Impact of Investor Sentiment on Financial Credit from the Perspective of Behavioral Finance.
[18] Wang, Y. (2025). Application of Data Completion and Full Lifecycle Cost Optimization Integrating Artificial Intelligence in Supply Chain.
[19] Wu, Y. (2025). Software Engineering Practice of Microservice Architecture in Full Stack Development: From Architecture Design to Performance Optimization. Machine Learning Theory and Practice, 5(1), 64-75.
[20] Su, J. (2026). Research on Android Real-time Communication System Architecture and High-reliability Assurance Pathways Integrating AI-based Anomaly Detection Mechanisms. Engineering Advances, 6(2).
[21] Liang, Q. (2026). Research on the Renovation Design Path for Enhancing the Efficiency of Mixed-Use Office and Retail Spaces. European Journal of AI, Computing & Informatics, 2(2), 163-170.
[22] Wang, N. (2026). Research on Evaluation and Optimization Models of Enterprise Resource Allocation Efficiency from a Data-driven Perspective. Advances in Computer and Communication, 7(1).
[23] Gao, Y. (2026). Application of Delaware Corporate Law in Cross-Border M&A: Business Structures, Contractual Risk, and Case-Based Lessons. Economics and Management Innovation, 3(2), 128-136.
[24] Huang, J. (2026). From Policy Authorization to Practical Execution: A Decision-Support Framework for Implementing Housing Supply Strategies in the United States. Strategic Management Insights, 3(1), 24-31.
[25] Gao, Y. (2026). The Role and Practice of Delaware Law in Global Cross-border M&A Transactions. International Journal of Law, Policy & Society, 2(1), 38-46.
[26] Liang, Q. (2026). Reconstruction of Commercial Building Space Reuse Mode Driven by Composite Business Types. International Journal of Engineering Advances, 3(1), 107-113.
[27] Zhang, K. (2025, December). Research on Cross-Selling Precision Marketing Strategy Based On Xgboost Model and SHAP Explanatory Framework. In 2025 IEEE 1st International Conference on Recent Trends in Computing and Smart Mobility (RCSM) (pp. 1-7). IEEE.

[28] Liang, Q. (2026). How Architectural Design and Utility Infrastructure Impacts AI Supporting Campus and Drive Future Innovation, Operational Efficiency and Sustainable Advancement in Utility-Critical Environment. European Journal of Engineering and Technologies, 2(2), 71-77.

[29] Zhang, Q. (2025, July). Research on Improving the Effectiveness of Programmatic Advertising Using Multi-armed Bandit Algorithms. In International Conference on Frontier Computing (pp. 543-552). Singapore: Springer Nature Singapore.

[30] Wang, Y. (2025, July). Research on Federated Learning Algorithm Design and Privacy Protection Mechanism of Sports Rehabilitation Data Based on Multimodal Fusion. In International Conference on Frontier Computing (pp. 563-574). Singapore: Springer Nature Singapore.