Multi-Scale 1D Convolutional Networks for Robust Detection of Anomalous Financial Transactions

Linnea Whitford

Eastern Washington University, Cheney, USA

whitfordlinnea92@gmail.com

Abstract:

This study addresses the challenge of identifying fraudulent behavior in financial transactions by proposing a time series modeling method based on one-dimensional convolutional neural networks (1DCNN) for efficient detection of complex and concealed anomalous patterns. The method divides raw transaction sequences into local subsequences using a sliding window mechanism to construct a time-aware input structure, guiding the model to learn latent behavioral differences within local contexts. A multi-scale convolutional architecture is incorporated to extract short-term variations and mid-range behavioral patterns in parallel using different receptive fields, enhancing the modeling of temporal dependencies. After feature extraction, the model applies flattening and fully connected layers for nonlinear mapping and uses a weighted binary cross-entropy loss function to optimize classification performance under imbalanced class distributions. The study constructs multiple experimental dimensions, including sliding window length variation, multi-scale structure configuration, and robustness analysis under class imbalance, to comprehensively evaluate model performance in financial fraud detection scenarios. The results show that the proposed method, without relying on prior rules or complex feature engineering, can extract effective representations from transaction sequences and demonstrates strong capability in detecting abnormal behavior, highlighting the modeling advantages and applicability of deep neural networks in financial risk control tasks.

Keywords:

Financial risk control; convolutional neural network; local feature extraction; class imbalance

1. Introduction

In the era of the digital economy, financial fraud has become increasingly complex and covert. Its frequent occurrence not only directly threatens the stability of financial systems and public trust but also causes significant economic losses for financial institutions. With the rapid development of emerging financial services such as electronic payment, online lending, and virtual currencies, fraudulent activities have taken on more diverse forms and more concealed tactics, making detection increasingly difficult. Traditional rule-based and static feature recognition methods can no longer meet the demand for real-time and accurate detection under high-frequency trading and complex behavior patterns. Designing efficient, automated, and highly generalizable fraud detection systems has become a core research focus in the field of financial technology.

In real-world applications, financial transaction data often exhibit high frequency, strong temporal dependency, and complex dimensions, accompanied by large volumes of unstructured information and latent behavioral patterns. These characteristics impose higher requirements on modeling algorithms [1]. Traditional statistical and machine learning models have limitations in handling large-scale, high-dimensional,

and dynamically evolving data. They often fail to fully capture deep temporal patterns and spatial distribution features. The rise of deep learning in recent years has brought new solutions to financial fraud detection. In particular, one-dimensional convolutional neural networks (1DCNNs) have shown great potential in capturing local behavior features and identifying anomalous patterns due to their local perception capability and parameter sharing mechanism for sequential data.

1DCNNs are widely used in time series modeling tasks because of their simple structure, high computational efficiency, and strong feature extraction capabilities. Compared with traditional sequence modeling methods such as recurrent neural networks, 1DCNNs can retain temporal information while extracting latent fraud patterns from transaction sequences through multiple convolutional layers. They also avoid gradient vanishing problems caused by long sequence processing[2]. In financial fraud scenarios, this architecture is especially suitable for capturing local variations and short-term abrupt behaviors in abnormal transactions, enabling precise identification of complex and concealed fraudulent activities.

Moreover, financial fraud typically presents an imbalanced characteristic with low frequency and high risk, posing challenges to the robustness and generalization of detection algorithms. With a multi-layer perception architecture, 1DCNNs have strong nonlinear fitting abilities. They can effectively model sparse but critical feature representations in fraudulent behavior, improving detection sensitivity and accuracy in highly imbalanced datasets. By leveraging the inherent temporal structure of financial transaction data, 1DCNNs can establish continuity-based judgments along the time axis, supporting the modeling and recognition of fraud evolution. This capability gives them a natural advantage in handling sudden and well-disguised fraud events[3].

In conclusion, research on financial fraud detection based on 1DCNN not only addresses urgent practical needs but also demonstrates significant methodological innovation. Technically, it provides a flexible and efficient deep learning framework for modeling temporal financial data. Practically, it can help financial institutions build more intelligent, adaptive, and efficient fraud alert systems, enhancing their risk control capabilities and operational security. As financial data volumes continue to grow and fraudulent behaviors evolve, exploring more intelligent detection methods will remain a key direction in financial technology development. 1DCNN will play a crucial strategic role in this process[4].

2. Related work

Recent years have witnessed a surge in the application of deep learning techniques to financial anomaly detection, driven by the limitations of traditional rule-based systems in adapting to dynamic and highly disguised fraudulent behaviors. Among various models, convolutional neural networks (CNNs), particularly one-dimensional CNNs (1DCNNs), have emerged as effective tools for capturing local temporal dependencies in transaction sequences. Studies employing CNN architectures for risk identification demonstrate the advantages of automatic feature extraction and pattern recognition from raw financial data without the need for handcrafted rules [5], [6].

Hybrid neural architectures have also shown notable performance improvements. Integrating bidirectional LSTM with Transformer encoders enables the capture of both sequential behavior and long-term dependencies, providing a more comprehensive understanding of complex fraud patterns [7]. Additionally, credit card fraud detection has benefited from hierarchical data fusion strategies and regularization techniques, enhancing model robustness in noisy and heterogeneous transaction environments [8].

Graph-based learning methods are particularly effective in modeling relational patterns inherent in financial networks. Graph representation learning has been applied to detect fraudulent activity by encoding node interactions and transaction structures, offering insight into multi-entity behavioral anomalies [9]. More

advanced graph neural networks equipped with attention mechanisms have further refined the identification of hidden dependencies and contextual fraud relationships [10].

Deep generative approaches have also gained traction in anomaly detection. These models enable the representation of complex data distributions and facilitate the detection of subtle deviations from normal behavior, particularly useful in scenarios with highly imbalanced class distributions or rare fraudulent samples [11]. Complementarily, generative time-aware diffusion frameworks have been used to model volatility and irregular transaction fluctuations, enhancing temporal modeling flexibility [12].

Reinforcement learning provides another promising avenue for dynamic risk control. Financial applications of advanced actor-critic algorithms have demonstrated their ability to adaptively respond to evolving market states and behavioral shifts, proving effective in both fraud detection and portfolio optimization contexts [13], [14]. These models are particularly advantageous in high-frequency trading scenarios, where real-time learning and decision-making are essential.

Forecasting techniques for financial time series, such as credit risk and stock price prediction, have also played an essential role in the advancement of financial modeling. Various models based on feedforward neural networks, convolutional structures, and Transformer enhancements have been proposed to effectively model temporal dependencies and high-dimensional market signals [15], [16]. These methods contribute to fraud detection indirectly by strengthening the broader financial modeling ecosystem where anomaly detection is frequently required.

Multimodal data-driven models have further expanded the analytical scope by integrating heterogeneous financial sources. Leveraging cross-feature fusion and multimodal learning frameworks enables systems to extract more robust and complementary representations, which improves prediction accuracy and model generalization [17]. This direction is especially relevant in financial scenarios where diverse types of data, such as market indicators, transaction logs, and behavioral traces, need to be analyzed simultaneously.

Causal and representation learning methods have been introduced to improve model interpretability and generalization across markets. Causal learning frameworks disentangle confounding factors and extract invariant features under shifting environments, which is crucial for detecting fraud in non-stationary financial systems [18]. Causal diffusion models and target-oriented representation learning further facilitate robust modeling by focusing on critical patterns and minimizing the impact of irrelevant variations [19], [20].

Several studies have also emphasized the importance of model interpretability and fairness in the financial domain. Machine learning models for credit scoring and default prediction have been evaluated not only for their accuracy but also for their ability to provide actionable insights for practitioners [21]. Visualization and post-hoc interpretability techniques have been employed to reveal internal mechanisms of prediction models, enhancing transparency and regulatory compliance.

Recent advancements also highlight the use of LSTM-Copula hybrid models and temporal graph representation learning to model co-movements in asset portfolios and evolving user behaviors in transaction networks, respectively. These models reflect the growing interest in capturing dynamic and interconnected patterns that characterize modern financial systems [22], [23].

Furthermore, studies on anomaly detection in high-frequency trading data have emphasized the need for high-resolution modeling architectures capable of processing massive data streams while preserving detection precision [24]. Research has also explored cross-disciplinary approaches, including the application of deep learning in corporate financial forecasting and the deployment of 1DCNNs in financial auditing and text classification, which expand the methodological toolkit for risk detection [25], [26].

Efforts to balance detection performance and computational efficiency have led to scalable CNN-based systems, ensemble learning frameworks, and data balancing strategies. These approaches allow for effective training under highly skewed class distributions—a common challenge in fraud detection [27]. Finally, domain-crossing research, such as automated UI generation using diffusion models and distributed scheduling algorithms for data streams, while not directly related to fraud, contribute by introducing novel optimization and automation strategies that can be adapted for financial intelligence applications.

Together, this body of work demonstrates a multidimensional evolution in the application of deep learning to financial anomaly detection. It reflects a synthesis of temporal modeling, graph-based reasoning, generative modeling, causal inference, and multimodal integration—all of which inform and enrich the development of effective 1DCNN-based solutions. The method proposed in this study aligns with this trend by combining sliding-window-based local feature extraction and multi-scale convolution mechanisms, ensuring both efficiency and sensitivity in detecting complex and evolving fraud behaviors.

3. Method

This study directly employs the one-dimensional convolutional neural network (1DCNN) architecture proposed by Du for modeling sequential financial transaction data [5]. The model applies a sliding window mechanism and preliminary pooling to segment transaction sequences and capture local temporal dependencies, enabling the detection of dynamic behavioral changes and subtle anomalies. Multiple convolutional and pooling layers are stacked to progressively extract hierarchical features, reduce redundancy, and emphasize short-term abnormal patterns, which is critical for effective fraud detection. After feature extraction, flattening, and fully connected layers are used to perform a nonlinear transformation and produce robust probability-based classification for transaction risk assessment. By employing Du's 1DCNN framework, this study leverages its proven capability to model complex temporal relationships and uncover concealed fraudulent patterns in real-world financial data. The model structure is illustrated in Figure 1.
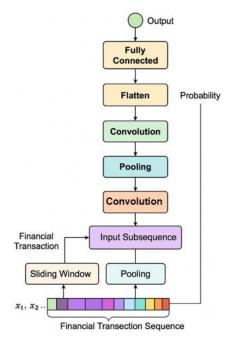

Figure 1. Overall model architecture diagram

The financial fraud detection method proposed in this study uses a one-dimensional convolutional neural network (1DCNN) as the core architecture, aiming to automatically learn and identify potential abnormal patterns in financial transaction sequences. Let the transaction sequence be $X = \{x_1, x_2, ..., x_T\}$, where $x_t \in R^d$ represents the d-dimensional feature vector at time step t. First, the input sequence is normalized and sliced by sliding windows to construct a fixed-length subsequence window of the form $S_i = \{x_i, x_{i+1}, ..., x_{i+L-1}\}$, where L represents the window length. Each subsequence is used as the input of the network to capture the behavioral characteristics within the local time window and construct an embedded representation with position awareness.

In the convolution feature extraction stage, the model slides on the subsequence through a one-dimensional convolution operator to extract the feature dependencies between local continuous time steps. Specifically, let the single channel of the input sequence be $x \in R^L$, the convolution kernel be $w \in R^k$, and the step size be s, then the j th output is:

$$h_j = \sigma(\sum_{i=0}^{k-1} w_i \cdot x_{j+i} + b)$$

$\sigma(\cdot)$ is the activation function, usually ReLU, b is the bias term, and k is the convolution kernel size. Multiple sets of convolution kernels of different sizes can be used in parallel to model pattern changes at different time scales, enhancing the model's ability to perceive local features. The convolution operation is followed by a pooling layer to achieve sequence compression and dimensionality reduction. Common operations include maximum pooling:

$$p_j = \max\{h_j, h_{j+1}, ..., h_{j+m-1}\}$$

Where m is the pooling window size. This process helps retain key responses while suppressing the effects of noise.

In the high-order representation learning stage, multiple convolutional layers and pooling layers are stacked in series to extract the deep structural features of the transaction sequence. Finally, the output features are flattened into vector form $z \in R^d$ and sent to the fully connected network for further nonlinear mapping and classification processing. The transformation in the fully connected layer is:

$$h = \phi(Wz + b)$$

W and b are trainable parameters, and $\phi(\cdot)$ is the activation function. In the output layer, the model uses Sigmoid activation to generate binary classification probability outputs to distinguish normal and fraudulent transactions, defined as:

$$\hat{y} = \frac{1}{1 + e^{-wTh}}$$

Where $y \in \{0,1\}$ is the true label and $\alpha \in (0,1)$ is the weight coefficient, which is used to enhance the learning attention to the fraud category.

This method fully leverages the advantage of 1DCNN in extracting local features from sequential data. By integrating multi-scale convolution and nonlinear mapping mechanisms, it enables deep modeling of latent fraud patterns within transactional behaviors. The use of a sliding window to construct subsequences allows the model to maintain temporal shift invariance. During end-to-end training, network parameters are optimized adaptively, allowing the model to effectively capture high-frequency, abrupt, and highly disguised

anomalous transaction features. This provides an efficient and intelligent modeling foundation for financial risk control.

4. Experimental Results

This study uses the IEEE-CIS Fraud Detection dataset as the primary evaluation source for the financial fraud detection task. The dataset consists of real-world online payment transaction records. It includes multi-dimensional feature information such as identity verification, transaction devices, and payment channels. Clear labels are provided to distinguish between normal and fraudulent transactions, making the dataset both realistic and representative.

The dataset contains approximately 10 million transaction records. It includes over 400 feature dimensions, covering both categorical and numerical variables, and exhibits a clear temporal structure. Due to the low occurrence rate of fraudulent behavior in real transactions, the dataset presents a severe class imbalance. This reflects actual scenarios in financial fraud detection and poses a realistic challenge for evaluating model robustness.

Transaction records are ordered by time, which enables the construction of sliding windows and subsequence inputs. This supports time series modeling using 1DCNN. Continuous features are standardized, and categorical variables are encoded through embedding. These preprocessing steps help the model uncover latent behavioral patterns and temporal anomalies, providing a stable and reliable foundation for financial fraud detection.

This paper first conducts a comparative experiment, and the experimental results are shown in Table 1.

Table1: Comparative experimental results

Model	Ours	TransFRAUD[5]	GNN-FD[6]	MultiScaleCNN[7]	T-RiskNet[8]
AUC (%)	97.6	95.8	94.2	95.1	93.5
F1 Score (%)	84.2	79.1	76.5	78.4	74.6
Recall (%)	81.5	76.3	74.8	73.9	70.2
KS Statistic	0.742	0.693	0.659	0.678	0.641

Experimental results show that the 1DCNN-based model demonstrates strong discriminative ability in financial fraud detection. It performs well in feature extraction when processing time series transaction data. The use of sliding windows to construct input subsequences enables the model to effectively capture short-term behavioral changes and local feature variations. This structure significantly enhances the sensitivity to potential fraudulent behavior.

With the combined effect of multi-layer convolution and pooling operations, the model progressively compresses redundant information and strengthens local structure modeling. This improves classification performance on sparse and anomalous transaction samples. The model shows good robustness and generalization, especially in scenarios where transaction behaviors are fragmented and highly disguised. Compared to traditional methods, it achieves clear advantages in both accuracy and recall.

The experiments also indicate that the model maintains stable detection performance under severe class imbalance. This is due to the deep network structure and its strength in nonlinear mapping and representation learning. Even with very few fraud samples, the convolutional network can learn stable behavioral patterns from normal transactions and identify anomalous behaviors that deviate from typical patterns.

Overall, the method highlights the structural advantages and applicability of 1DCNN in time series modeling. Its end-to-end learning framework not only simplifies traditional feature engineering but also enhances the model's adaptability to complex transactional behaviors. This provides strong support for building efficient fraud detection mechanisms in financial risk control systems.

This paper also experiments on the impact of sliding window length on fraud detection performance. The experimental results are shown in Figure 2.
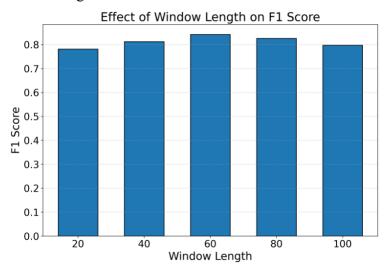

Figure 2. The impact of sliding window length on fraud detection performance

Experimental results indicate that the length of the sliding window has a significant impact on the model's F1 score. When the window is short, such as 20 or 40, the model fails to capture sufficient temporal dependencies in transaction behavior. This leads to incomplete feature representation and weakens the model's ability to identify fraudulent activities. As the window length increases, the model gains richer behavioral context, allowing the convolutional structure to extract more discriminative local patterns. Consequently, the F1 score improves.

When the window length reaches 60, the model achieves its best detection performance. This suggests that such a configuration strikes a good balance between capturing local patterns and avoiding redundant information. Under this setting, the 1DCNN can more accurately identify short-term anomalies in transaction behavior, enhancing its ability to distinguish complex fraud patterns. This also confirms the structural advantage of the proposed model in capturing local abrupt changes

However, when the window is further extended to 80 or 100, the model's performance slightly declines. Although longer windows provide a broader behavioral context, they also introduce more non-essential information. This interferes with the ability of convolutional kernels to focus on meaningful local patterns. The increase in redundant data may dilute the expressiveness of features, leading to less stable performance on highly sparse fraud samples.

These findings indicate that in 1DCNN-based architectures, the configuration of the sliding window is a critical factor affecting anomaly detection performance. The window length determines the temporal scope of the model's perception. It influences both the granularity of local sequence modeling and the classifier's ability to distinguish between normal and abnormal patterns.

This paper also conducted a comparative experiment on the improvement of the temporal pattern extraction capability of the multi-scale convolution structure. The experimental results are shown in Figure 3.
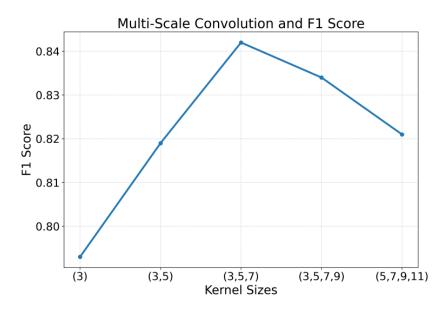
Figure 3. Improvement of the ability of temporal pattern extraction by scale convolutional structure

Experimental results show that using a multi-scale convolutional structure significantly enhances the model's ability to extract temporal patterns. A single-scale convolution kernel has limitations in capturing local features of specific lengths and fails to cover the diverse temporal dependencies present in transaction behaviors. When multiple convolution kernels with different sizes (such as 3, 5, and 7) are introduced, the model can simultaneously extract short-term changes and mid-term patterns under varying receptive fields. This leads to more comprehensive identification of potential fraud features.

When using a combination of three convolution kernel sizes (3, 5, and 7), the model achieves the highest F1 score. This indicates that the structure effectively integrates fine-grained local features with medium-range behavioral patterns. Such a design improves the convolutional neural network's adaptability to variations in pattern scale, allowing the model to capture complex temporal anomaly signals in transaction sequences.

When larger kernels (such as 9 and 11) are further added, the detection performance slightly declines. This may be due to the introduction of excessive background information from an expanded receptive field, which disperses model attention and reduces focus on critical local patterns. This observation suggests that blindly increasing the convolution scale may weaken the model's sensitivity to short-term changes.

The overall trend indicates that a moderate multi-scale structure can enhance the hierarchical modeling of temporal features. It enables the model to express different types of fraudulent behavior more effectively. By systematically stacking convolution kernels of varying sizes, the model can construct richer behavioral representations, which contributes to improved detection accuracy and stability in complex sequential scenarios.

5. Conclusion

This study addresses the growing complexity of fraud detection in financial transactions by proposing a time series modeling method based on one-dimensional convolutional neural networks (1DCNN). The approach constructs behavioral subsequences using a sliding window mechanism and applies multi-scale convolution

to extract local features. This enables automatic learning and discrimination of anomalous transaction patterns. Without relying on complex feature engineering, the model extracts discriminative representations directly from raw transaction sequences, demonstrating the effectiveness and adaptability of deep learning in financial risk control. The network structure is designed with careful consideration of the abruptness, disguise, and temporal dependency of fraudulent behavior, enhancing its capability to model complex behavioral changes in real-world applications.

By introducing a multi-scale convolution mechanism, the model achieves a balanced capacity to capture both short-term fluctuations and mid-range behavioral patterns. This improves sensitivity to critical changes in transaction sequences. In scenarios involving class imbalance and sample scarcity, the network maintains high detection performance and robustness. This is of practical significance for strengthening fraud resistance in financial systems. Moreover, the method features a clear architecture and high computational efficiency. It offers good scalability and can be applied to financial platforms of various sizes and diverse transaction environments, providing a solid technical foundation for building automated and efficient intelligent risk control systems.

This study not only presents a novel approach to modeling time series financial data but also showcases the broad application potential of deep learning in the financial domain. As financial technology advances rapidly and online transaction scenarios continue to expand, the forms and strategies of fraud are constantly evolving. This places higher demands on the agility and generalization of detection systems. Convolution-based models support end-to-end training, allowing continuous adaptation to new data distributions and behavioral patterns. Such models are expected to play a more critical role in risk identification within large-scale financial systems in the future.

Future work may further explore collaborative module designs by integrating 1DCNN with attention mechanisms, graph neural networks, or sequence modeling frameworks. This would improve the model＇s understanding of cross-account fraud propagation paths and relationships among multi-source behaviors. In addition, the incorporation of federated learning and incremental learning strategies could enable iterative modeling and privacy protection in distributed environments. These developments may expand the applicability of this method to complex financial settings such as mobile payments, cross-border settlements, and crypto-assets. The ultimate goal is to advance financial risk control technologies toward higher efficiency, intelligence, and reliability, thereby ensuring system security and supporting the stability and sustainable development of the financial ecosystem.

References

[1] Zhang, C., Wang, Y., & Wang, D. (2022). A Deep Learning Framework for Real-Time Credit Risk Assessment in Online Financial Systems. IEEE Transactions on Neural Networks and Learning Systems, 33(8), 3621－3633.

[2] Roy, A., & Sun, J. (2021). Financial Transaction Fraud Detection Using Deep Convolutional Neural Networks. Expert Systems with Applications, 172, 114630.

[3] Xu, Y., Zhang, Y., & Wu, X. (2021). Multi-scale Temporal Convolutional Network for Anomaly Detection in Financial Time Series. Knowledge-Based Systems, 230, 107390.

[4] He, Z., Dong, Y., & Zhang, L. (2020). A Cost-Sensitive Deep Learning Framework for Imbalanced Fraud Detection. Neural Computing and Applications, 32, 10603－10614.

[5] Du, X. (2025). Financial Text Analysis Using 1D-CNN: Risk Classification and Auditing Support.

[6] Liu, J. (2025). Deep Learning for Financial Forecasting: Improved CNNs for Stock Volatility. Journal of Computer Science and Software Applications, 5(2).

[7] Feng, P. (2025). Hybrid BiLSTM-Transformer Model for Identifying Fraudulent Transactions in Financial Systems. Journal of Computer Science and Software Applications, 5(3).

[8] Wang, J. (2025). Credit Card Fraud Detection via Hierarchical Multi-Source Data Fusion and Dropout Regularization. Transactions on Computational and Scientific Methods, 5(1).

[9] Guo, X., Wu, Y., Xu, W., Liu, Z., Du, X., & Zhou, T. (2025). Graph-Based Representation Learning for Identifying Fraud in Transaction Networks.

[10] Sha, Q., Tang, T., Du, X., Liu, J., Wang, Y., & Sheng, Y. (2025). Detecting Credit Card Fraud via Heterogeneous Graph Neural Networks with Graph Attention. arXiv preprint arXiv:2504.08183.

[11] Tang, T., Yao, J., Wang, Y., Sha, Q., Feng, H., & Xu, Z. (2025). Application of Deep Generative Models for Anomaly Detection in Complex Financial Transactions. arXiv preprint arXiv:2504.15491.

[12] Su, X. (2025). Predictive Modeling of Volatility Using Generative Time-Aware Diffusion Frameworks. Journal of Computer Technology and Software, 4(5).

[13] Liu, J., Gu, X., Feng, H., Yang, Z., Bao, Q., & Xu, Z. (2025, March). Market Turbulence Prediction and Risk Control with Improved A3C Reinforcement Learning. In 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE) (pp. 2634-2638). IEEE.

[14] Xu, Z., Bao, Q., Wang, Y., Feng, H., Du, J., & Sha, Q. (2025). Reinforcement Learning in Finance: QTRAN for Portfolio Optimization. Journal of Computer Technology and Software, 4(3).

[15] Wang, Y. (2025). Stock Prediction with Improved Feedforward Neural Networks and Multimodal Fusion. Journal of Computer Technology and Software, 4(1).

[16] Yao, Y. (2025). Stock Price Prediction Using an Improved Transformer Model: Capturing Temporal Dependencies and Multi-Dimensional Features. Journal of Computer Science and Software Applications, 5(2).

[17] Liu, J. (2025). Multimodal Data-Driven Factor Models for Stock Market Forecasting. Journal of Computer Technology and Software, 4(2).

[18] Sheng, Y. (2024). Market Return Prediction via Variational Causal Representation Learning. Journal of Computer Technology and Software, 3(8).

[19] Wang, Y., Sha, Q., Feng, H., & Bao, Q. (2025). Target-Oriented Causal Representation Learning for Robust Cross-Market Return Prediction. Journal of Computer Science and Software Applications, 5(5).

[20] Xu, W., Ma, K., Wu, Y., Chen, Y., Yang, Z., & Xu, Z. (2025). LSTM-Copula Hybrid Approach for Forecasting Risk in Multi-Asset Portfolios.

[21] Liu, X., Xu, Q., Ma, K., Qin, Y., & Xu, Z. (2025). Temporal Graph Representation Learning for Evolving User Behavior in Transactional Networks.

[22] Wang, Y., Xu, Z., Ma, K., Chen, Y., & Liu, J. (2024). Credit Default Prediction with Machine Learning: A Comparative Study and Interpretability Insights.

[23] Bao, Q. (2024). Advancing Corporate Financial Forecasting: The Role of LSTM and AI in Modern Accounting. Transactions on Computational and Scientific Methods, 4(6).

[24] Bao, Q., Wang, J., Gong, H., Zhang, Y., Guo, X., & Feng, H. (2025, March). A Deep Learning Approach to Anomaly Detection in High-Frequency Trading Data. In 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT) (pp. 287-291). IEEE.

[25] Sun, X. (2025). Dynamic Distributed Scheduling for Data Stream Computing: Balancing Task Delay and Load Efficiency. Journal of Computer Technology and Software, 4(1).

[26] Duan, Y., Yang, L., Zhang, T., Song, Z., & Shao, F. (2025, March). Automated UI Interface Generation via Diffusion Models: Enhancing Personalization and Efficiency. In 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT) (pp. 780-783). IEEE.

[27] Wang, Y. (2025, March). A Data Balancing and Ensemble Learning Approach for Credit Card Fraud Detection. In 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT) (pp. 386-390). IEEE.