



International Journal of Data Mining and Bioinformatics

ISSN online: 1748-5681 - ISSN print: 1748-5673

<https://www.inderscience.com/ijdmb>

Smart contract and distributed ledger based financial transaction settlement and tracking model design in digital economy

Wei Zhong

DOI: [10.1504/IJDMB.2026.10079091](https://doi.org/10.1504/IJDMB.2026.10079091)

Article History:

Received:	17 March 2026
Last revised:	20 April 2026
Accepted:	15 May 2026
Published online:	13 July 2026

Smart contract and distributed ledger based financial transaction settlement and tracking model design in digital economy

Wei Zhong

Ancheng Property & Casualty Insurance Co., Ltd.,
Chongqing, 400010, China
Email: lancer312@163.com

Abstract: With the rapid development of financial technology and the digital economy, fraud detection in financial transactions faces increasing challenges due to complex transaction networks, temporal dependencies, and nonlinear interactions. This study proposes an RL-LGNN framework that integrates long short-term memory (LSTM) networks, graph neural networks (GNN), and reinforcement learning (RL) for fraud detection in the financial transaction settlement process. LSTM is used to encode historical transactions as temporal sequences and extract time-dependent behavioural features. GNN then models inter-node transaction relationships and captures structural information from the transaction graph. On this basis, RL is introduced to dynamically optimise the detection strategy, thereby improving model adaptability and robustness. Experimental results on both public and real-world datasets show that the proposed framework outperforms conventional methods and achieves fraud detection accuracy above 90%. The proposed framework provides an effective solution for fraud detection in financial transaction settlement.

Keywords: financial transaction; fraud detection; graph neural network; GNN; reinforcement learning.

Reference to this paper should be made as follows: Zhong, W. (2026) 'Smart contract and distributed ledger based financial transaction settlement and tracking model design in digital economy', *Int. J. Data Mining and Bioinformatics*, Vol. 30, No. 7, pp.133–149.

Biographical notes: Wei Zhong serves as the Vice General Manager of the Fund Application Department at Ancheng Property & Casualty Insurance Co., Ltd., Chongqing, China. His research focuses on financial technology, broad-based allocation of insurance funds, and credit risk modelling. He is mainly engaged in quantitative asset selection, transaction implementation and risk management.

1 Introduction

With the rapid development of smart contracts and distributed ledger technology, financial systems in the digital economy have become increasingly transparent, secure, and automated. Smart contracts enable the automatic execution of predefined contractual terms through blockchain-based code, thereby reducing reliance on third-party intermediaries. This self-executing mechanism improves transaction efficiency and

enhances operational security. Distributed ledger technology further provides a decentralised framework for transaction record management, ensuring transparency and traceability throughout the transaction process (Xu et al., 2024). Unlike traditional centralised systems, distributed ledgers replicate records across multiple nodes, which reduces the risks of single-point failure and unauthorised data modification. However, as digital financial ecosystems continue to expand, transaction structures have become increasingly complex, particularly in cross-border payment systems and decentralised finance environments. In such settings, high-frequency and large-scale capital flows make real-time monitoring more difficult (Qiu et al., 2025). As a result, fraud identification and transaction tracking have become important issues in digital financial governance (Zhou et al., 2025). Fraudulent activities may not only threaten financial stability, but also weaken user confidence in smart contract systems and distributed ledger infrastructures (Chen and Han, 2021). Therefore, the development of an effective and robust model for fraud detection and transaction tracking is essential for improving transaction security and supporting the stable development of the digital economy.

Artificial intelligence (AI) has been widely applied in fraud detection because of its ability to process large-scale data, identify complex patterns, and detect anomalous behaviours (Rong et al., 2025). With the continued advancement of machine learning and deep learning methods, AI-based approaches have shown increasing value in financial fraud analysis (Zhang et al., 2020). Traditional machine learning methods, such as support vector machines and decision trees, are effective in conventional classification tasks, but they often perform poorly when transaction data exhibit strong temporal dependence and complex relational structures. Deep learning methods provide stronger representation capacity for such scenarios (Zhang et al., 2025). In particular, long short-term memory (LSTM) networks are suitable for modelling sequential transaction behaviours, including user transaction histories and account activity trajectories, because they can capture both short-term variations and long-term dependencies in time-series data (Johora et al., 2024). This capability makes LSTM useful for identifying abnormal transaction patterns that are difficult to detect through static analysis alone. In addition, graph neural networks (GNNs) are well suited to financial transaction networks represented in graph form. By modelling node interactions and neighbourhood relationships, GNNs can extract structural features relevant to fraud identification in complex transaction systems. Reinforcement learning (RL) also provides advantages for dynamic detection tasks in continuously changing transaction environments. Through iterative policy optimisation, RL can adaptively adjust detection strategies and improve model responsiveness under evolving transaction conditions (Tong and Shen, 2023).

This paper proposes an RL-LGNN framework for financial transaction fraud detection to address the complex spatio-temporal dependencies in transaction networks. In the digital economy and decentralised finance environments, transaction relationships have become increasingly complex, making it difficult for conventional static detection methods to capture dynamic behavioural patterns and inter-node dependencies. To address this issue, the proposed framework integrates LSTM, GNNs, and RL. Specifically, LSTM is used to model temporal dependencies in transaction sequences, GNNs are employed to represent structural relationships among transaction nodes, and RL is introduced to adaptively optimise the detection strategy. By jointly modelling temporal behaviours, relational dependencies, and adaptive decision-making, the proposed framework provides a unified approach for fraud detection in dynamic financial transaction systems. The main contributions of this study are summarised as follows.

- 1 A coupled sequential-structural representation framework for fraud detection is proposed, in which node-level transaction evolution is encoded using LSTM, and the resulting temporal embeddings are incorporated into GNN learning. Unlike a simple feature concatenation or cascading pipeline, this design allows the transaction graph representation to be conditioned on both behavioural dynamics and inter-account relationships.
- 2 A RL-based adaptive policy layer is introduced on top of the LSTM-GNN backbone. Instead of treating fraud detection as a purely static classification task, the RL agent operates on the joint temporal-structural representation as the environment state and learns a dynamic decision policy based on feedback from fraud detection outcomes. This coupling enables the model to adapt to evolving transaction patterns and enhances robustness in non-stationary financial environments.
- 3 The proposed framework is empirically evaluated on both public and proprietary datasets, demonstrating consistent performance improvements over several competitive baselines. Further analysis indicates that these gains arise not only from the combination of multiple components, but also from the interaction between sequential modelling, graph representation learning, and adaptive policy optimisation.

Unlike conventional modular pipelines, the proposed framework is designed as a coupled temporal-structural-policy learning architecture, where representation learning and adaptive decision-making are jointly connected for fraud detection in evolving transaction networks.

2 Related works

2.1 Financial applications of deep learning methods

Deep learning, a class of neural network-based methods, has become an important non-parametric approach in fields such as signal processing and pattern recognition because of its strong capability to model complex nonlinear relationships among variables. Unlike traditional econometric approaches, deep learning methods do not rely on pre-specified equations or assumed functional forms, which provides greater flexibility in modelling the dynamic and heterogeneous characteristics of financial markets. Consequently, these methods have shown considerable potential in financial time-series forecasting compared with conventional parametric models, such as the autoregressive integrated moving average (ARIMA) model, generalised autoregressive conditional heteroskedasticity (GARCH) model, ordinary least squares (OLS), and difference-in-differences (DID) methods (Ozbayoglu et al., 2020). Olorunnimbe and Viktor (2023) systematically reviewed the application of deep learning to stock market prediction, with particular attention to the LSTM network and recurrent neural network (RNN). Their review highlighted the importance of data preprocessing and backtesting, while also emphasising the challenges associated with large-scale financial data. Naritomi and Adachi (2020) investigated the use of generative adversarial networks (GANs) for financial data augmentation and showed that synthetically generated data can enhance the performance of risk prediction and fraud detection models, thereby

improving the effectiveness of financial stress testing. Théate and Ernst (2021) assessed the application of deep learning in algorithmic trading, particularly deep reinforcement learning (DRL)-based trading systems. Their study indicated that although DRL exhibits strong adaptability in real-time trading environments by learning market dynamics and generating autonomous trading decisions, its practical deployment remains constrained by challenges related to risk control and regulatory compliance. Gülmez (2023) examined the use of LSTM models in algorithmic trading for financial price movement prediction and demonstrated that LSTM performs well in complex time-series forecasting, especially in capturing nonlinear market dependencies. Zhang et al. (2022a) further explored the application of RL to portfolio optimisation. Using real market data, they showed that DRL models can dynamically adjust asset allocation in response to changing market conditions, thereby improving returns while reducing portfolio risk.

2.2 *Fraud identification during the settlement of transactions*

Fu et al. (2016) applied convolutional neural networks (CNNs) to credit card fraud detection and reported superior predictive performance. In addition, because certain types of credit card transaction data exhibit temporal dependencies, RNNs, which are designed to capture sequential correlations, are well suited to financial time-series analysis. Zou et al. (2009) observed that the architecture of RNNs is more appropriate for financial time-series prediction than that of shallow neural networks, indicating their potential utility in forecasting transaction-related fraud patterns. Zhang et al. (2018) developed a CNN-based model for online fraud detection and improved detection performance by reordering the original features through a feature ordering strategy. Their results showed that the proposed model increased the recall rate by 2% relative to other CNN-based methods, while maintaining a recall level of approximately 94%. Heryadi and Warnars (2017) employed LSTM to predict credit card transaction data processed by CNNs, confirming that LSTM can effectively capture temporal patterns in transaction sequences and thereby improve recognition accuracy. Li et al. (2020) proposed a novel loss function, termed full-centre loss, which simultaneously considers distance and angular bias between features. Their empirical results indicated that this loss function outperformed conventional alternatives and improved overall model performance. Fiore et al. (2019) used a GAN to synthesise minority-class samples and construct an augmented training set. The results demonstrated that classifiers trained on the augmented dataset achieved substantially higher accuracy than those trained on the original data alone. Since deep learning models are commonly optimised through gradient-based backpropagation algorithms, a number of studies have focused on improving optimisation strategies to address the challenges of credit card fraud detection. Bello et al. (2023) further investigated the application of deep learning to fraud detection in financial transactions, with particular emphasis on data imbalance and feature extraction, and demonstrated the effectiveness of such models in real-time transaction monitoring.

The above studies indicate that, with the continued development of computing technologies, deep learning methods have become increasingly important in financial transaction analysis. In addition to conventional applications such as economic forecasting and credit evaluation, substantial progress has been achieved in fraud risk identification during transaction processes. Therefore, the design of intelligent financial transaction tracking models for fraud detection should fully exploit the representation

learning and data processing capabilities of deep learning to enable earlier and more effective risk identification. This is of considerable significance for promoting the secure and sustainable development of the digital economy.

3 Methodology

3.1 LSTM and GNN

When multiple high-risk transactions occur within a short period, LSTM can identify the abnormal sequence pattern and support fraud recognition. This characteristic makes it more suitable than conventional machine learning methods for modelling complex and continuous fraudulent behaviours, particularly in scenarios involving dynamic temporal variation (Shi et al., 2023). Therefore, LSTM is adopted in this study for sequential feature extraction. The key mechanism of LSTM lies in its gating structure, which regulates the retention, updating, and removal of information in the cell state. Among these components, the forget gate determines whether the existing cell-state information should be retained or discarded, as defined in equation (1):

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (1)$$

where f_t is the output, σ is the activation function, W_f and b_f are the weights and biases, h_{t-1} is the hidden state at $t-1$, and x_t is the input. The input gate determines which new information should be incorporated into the cell state and is defined in equation (2):

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (2)$$

where the variables are consistent with those defined in equation (1). The output gate is defined in equation (3):

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \quad (3)$$

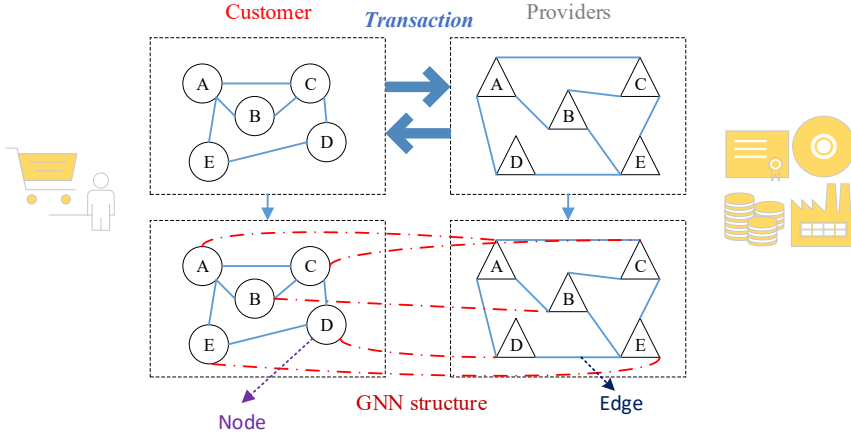
To further capture the interaction structure inherent in financial transactions, this study introduces a GNN to enhance feature extraction and relational analysis. The combination of LSTM and GNN enables joint modelling of temporal dependence and structural correlation in transaction data. The architecture of the transaction model is shown in Figure 1.

As shown in Figure 1, a typical financial transaction involves multiple interacting entities. For individual users, historical credit status, transaction records, user profiles, and other financial attributes jointly constitute a personal information network. Similarly, the service provider or institution can also be characterised by multiple attributes. Financial transactions are generated through interactions between these entities under specific transaction conditions. Since such interactions naturally form a complex relational structure, GNNs provide an appropriate framework for modelling financial transaction data.

GNNs are specifically designed for graph-structured data and can learn node representations by propagating and aggregating information over the connections among nodes. In financial systems, entities such as users, accounts, and transactions are often embedded in highly interconnected networks. This makes GNNs particularly suitable for

fraud detection tasks that require the extraction of relational features and structural dependencies. Fraudulent behaviour is often reflected in abnormal connection patterns, such as fabricated transactions or unusually dense interaction frequencies. By modelling the topological relationships between nodes and edges, GNNs can effectively identify such irregular patterns. The core mechanism of GNNs lies in learning node feature representations through message passing and neighbourhood feature aggregation (Liu et al., 2021).

Figure 1 GNN structure and transaction model (see online version for colours)



A graph $G = (V, E)$ consists of a collection of nodes V and a collection of edges E consisting of a collection of nodes and a collection of edges. Each node $v \in V$ has a feature vector x_v , each edge $(u, v) \in E$ represents the node u and v association relationship between them. The feature representation of each node is updated through information exchange with its neighbouring nodes. The update process is formulated as follows:

$$h_v^{(k)} = \sigma \left(W^{(k)} \cdot \sum_{u \in \mathcal{N}(v)} h_u^{(k-1)} + b^{(k)} \right) \quad (4)$$

where $h_v^{(k)}$ is the feature vector of node v at layer k , $\mathcal{N}(v)$ denotes the set of neighbouring nodes of node v , $W^{(k)}$ and $b^{(k)}$ are the weights and bias parameters at layer k . In GNN, node features are updated through multi-layer neighbourhood aggregation. At the k^{th} layer, each node representation contains both local and higher-order neighbourhood information. The resulting node embeddings can be used for downstream tasks such as classification or regression.

3.2 RL for fraud detection

RL is a branch of machine learning in which an agent learns an optimal policy by interacting with an environment to maximise cumulative rewards. Unlike supervised and unsupervised learning, RL relies on trial-and-error feedback to optimise sequential decision-making. In financial fraud detection, RL provides a mechanism for adapting detection strategies to evolving fraud patterns (Tekkali and Natarajan, 2023). Through continuous interaction with transaction data, RL can improve the model's ability to

identify and respond to emerging fraudulent behaviours. The basic components of RL include state S_t , action A_t , reward R_t strategy π and value functions $Q(s, a)$. The action-state value function $Q(s, a)$ is used to represent the long-term return in a certain state, the goal is to find the strategy that maximises the future return, which is calculated as shown in equation (5):

$$Q^\pi(s, a) = \mathbb{E}^\pi \left[\sum_{t=0}^{\infty} \gamma^t R_{t+1} \mid S_0 = s, A_0 = a \right] \quad (5)$$

This function represents the expected return of taking action a in state s under policy π . It is optimised iteratively based on the Bellman equation. Typical policy optimisation methods include Q-learning and policy gradient methods, as shown in equation (6) and equation (7), respectively:

$$Q(s, a) \leftarrow Q(s, a) + \alpha \left(R_{t+1} + \gamma \max_{a'} Q(S_{t+1}, a') - Q(s, a) \right) \quad (6)$$

$$\nabla J(\theta) = \mathbb{E}_\pi \left[\nabla_\theta \log \pi(a \mid s; \theta) Q^\pi(s, a) \right] \quad (7)$$

where α is the learning rate, and γ is the discount factor, and $J(\theta)$ is the objective function of the strategy. In this study, the fraud detection task is formulated as a sequential decision process with the following components:

- 1 State s_t : At each decision step t , the environment state is defined by the joint temporal structural representation of transactions. Specifically, s_t includes:
 - temporal embeddings h_t^{LSTM} extracted from each account's transaction sequence by the LSTM
 - graph embeddings h_t^{GNN} capturing relational dependencies from the GNN
 - auxiliary transaction features x_t .

The above component will constitute the $s_t = [h_t^{\text{LSTM}} \parallel h_t^{\text{GNN}} \parallel x_t]$.

- 2 Action a_t : The RL agent selects detection actions, such as assigning a fraud risk score, adjusting a detection threshold, or flagging a transaction for further inspection. These actions directly influence the classification outcome and subsequent reward.
- 3 Reward r_t : A reward signal is defined to encourage accurate fraud detection while penalising false positives and false negatives.

$$r_t = \begin{cases} +\alpha, & \text{if a fraudulent transaction is correctly identified} \\ +\beta, & \text{if a normal transaction is correctly classified} \\ -\gamma, & \text{if a false positive occurs} \\ -\delta, & \text{if a false negative occurs} \end{cases}$$

where $\delta > \gamma$ reflects the higher practical cost of missed fraud.

- 4 Policy π_θ : The agent's policy is parameterised by θ and is optimised to maximise the expected cumulative reward:

$$J(\theta) = \mathbb{E} \left[\sum_{t=0}^T r_t \right] \quad (8)$$

Policy optimisation is performed using policy gradient methods, which update θ based on the observed state-action-reward trajectories.

- 5 **Transition:** The environment transitions are determined by the sequence of transactions, their network interactions, and any changes induced by the agent's actions. These transitions capture how actions influence future states and detection opportunities.

By integrating the LSTM-GNN backbone with this RL formulation, a closed-loop representation-to-policy mechanism is established. The temporal-structural embeddings provide informative states, and the RL agent continuously adapts the detection strategy to evolving transaction patterns, improving robustness in non-stationary financial environments.

3.3 *RL-LGNN for dynamic financial fraud detection*

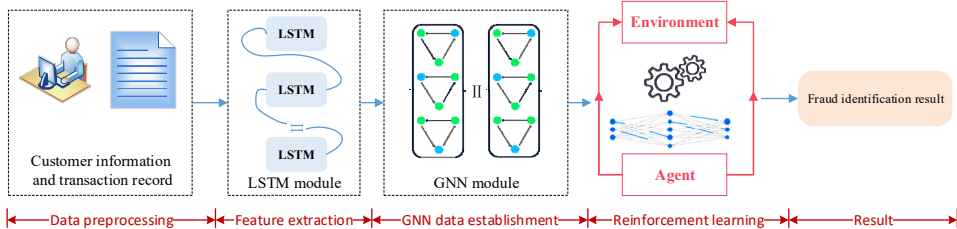
Based on the proposed model framework, this study develops an RL-LGNN fraud detection framework for financial transaction networks by coupling LSTM-based temporal modelling, GNN-based relational learning, and RL-based adaptive decision optimisation. The objective is not only to combine multiple learning modules, but to build a unified mechanism in which transaction behaviour evolution, network dependency, and decision policy are jointly connected. Different from a straightforward cascading architecture, the proposed framework is centred on a representation-to-policy coupling strategy. Specifically, LSTM first encodes the sequential transaction behaviours of each node and generates temporal embeddings that characterise behavioural evolution over time. These embeddings are then injected into the GNN as node representations, allowing graph learning to be conditioned on dynamic behavioural patterns rather than static attributes alone. On this basis, RL further takes the joint temporal-structural representation as the environment state and learns an adaptive fraud detection policy through reward-driven optimisation.

The overall workflow of the proposed framework is shown in Figure 2. The framework consists of five modules: data preprocessing, temporal feature extraction, graph construction and relational learning, RL-based policy optimisation, and output generation. First, raw transaction records are preprocessed and organised into node-level sequential data and graph-structured interaction data. Second, LSTM is applied to each node's transaction sequence to extract time-dependent behavioural features. Third, these temporal features are incorporated into the GNN, which aggregates neighbourhood information over transaction edges to capture inter-node dependency patterns in the transaction network.

To support adaptive decision-making, the fraud detection process is further formulated as a sequential decision task. At each step, the RL agent observes the state constructed from the LSTM-GNN backbone, including temporal embeddings, graph embeddings, and transaction context information. Based on this state, the agent selects a detection action, such as assigning a fraud label or adjusting the decision strategy for suspicious transactions. After the action is executed, the environment returns a reward based on the detection outcome, so that correct identification is encouraged while false

alarms and missed fraud cases are penalised. Through iterative interaction, the RL module learns a dynamic policy that is better suited to evolving transaction environments. Therefore, the proposed RL-LGNN framework goes beyond a simple modular combination of LSTM, GNN, and RL. Its key characteristic is that sequential representation learning, relational reasoning, and adaptive policy optimisation are explicitly linked into a closed-loop fraud detection process, which enhances both representation quality and decision robustness in complex financial transaction systems.

Figure 2 Framework for RL-LGNN (see online version for colours)



4 Experiments and analysis

4.1 Experimental settings

In addition to the widely used transaction fraud datasets [credit card fraud detection dataset (Zhang et al., 2022b) and PaySim dataset (Azamuke et al., 2022)], a practical financial dataset was collected for over 150 publicly listed companies. Fraud labels were assigned based on regulatory disclosures and reported financial misconduct. Features were constructed from annual financial indicators, corporate governance metrics, and transaction network attributes. Transaction graphs were generated by representing companies as nodes, with edges reflecting financial relationships such as shared ownership, direct transactions, or supply-chain connections. Temporal sequences were created to capture year-by-year behavioural changes. The dataset was split chronologically, with data from 2006–2019 used for training and 2020–2023 reserved for testing, ensuring that the model is evaluated on unseen future instances and improving the transparency and reproducibility of the experimental validation.

Since fraud detection is essentially a binary classification task, accuracy is used as a primary evaluation metric. To obtain a more reliable assessment of model performance, additional feature-based analyses are also conducted during the evaluation process.

Because training LSTM-based models requires substantial computational resources, the experimental environment used in this study is summarised in Table 1.

Table 1 Experimental environment

<i>Environment</i>	<i>Information</i>
CPU	I7-13650HX
GPU _s	RTX 4060TI
Language	Python 3.9
Framework	Pytorch and Scikit-learn

After configuring the experimental environment, model training and comparative experiments were conducted. The benchmark methods include extreme gradient boosting (XGBoost) (Hajek et al., 2023), a CNN combined with LSTM model (El Naby et al., 2021), and a standalone GNN model (Liu et al., 2021).

4.2 Method comparison and result analysis

After model construction and experimental environment configuration, comparative experiments were conducted to evaluate the performance of the proposed model. The training results on the two public datasets are shown in Figure 3 and Figure 4.

As shown in Figure 3 and Figure 4, the proposed RL-LGNN model exhibits faster convergence than the comparison models on both datasets and achieves better overall performance than the standalone GNN and LSTM models. In both experiments, RL-LGNN approaches stable and near-optimal performance at approximately 30 training iterations. A similar trend is observed in the accuracy curves, further indicating the stability and effectiveness of the proposed method.

Figure 3 Training process on credit card fraud detection dataset (see online version for colours)

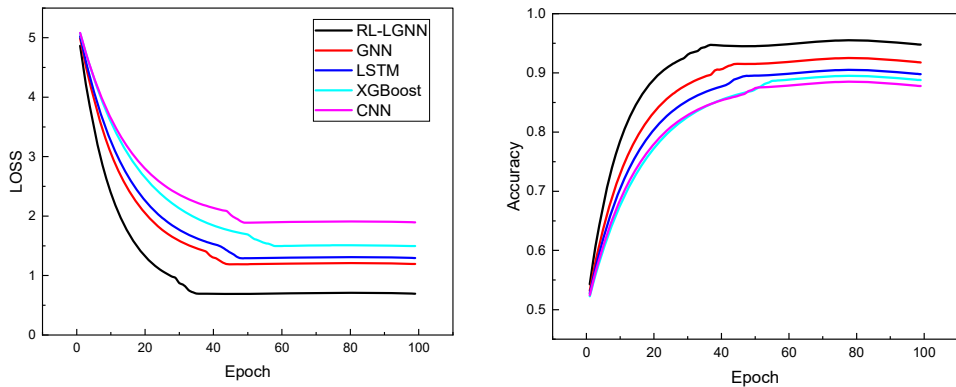
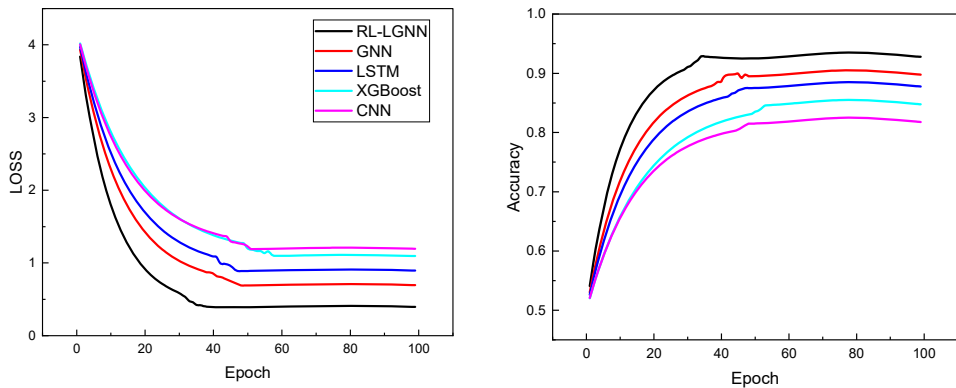


Figure 4 Training process on PaySim dataset (see online version for colours)



To provide a clearer comparison of recognition performance, the fraud detection accuracies on the two datasets are summarised in Figure 5.

Figure 5 Recognition results on both public datasets (see online version for colours)

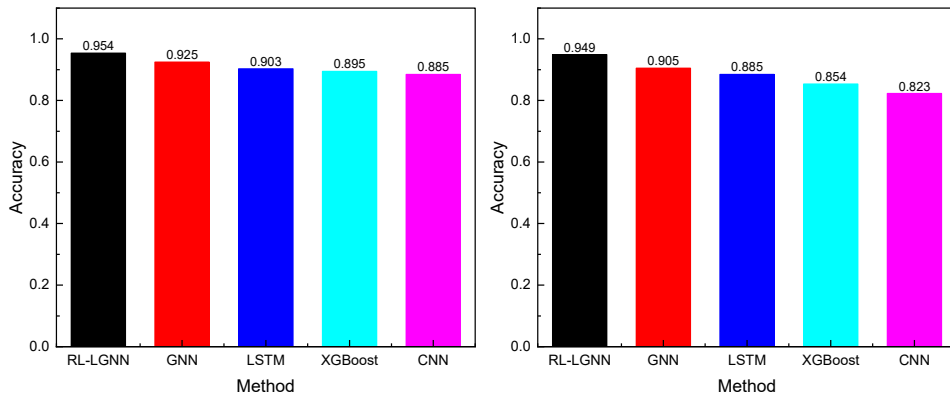


Table 2 The recognition results on credit card fraud detection dataset

Method	Precision	Recall	F1
RL-LGNN	0.937	0.929	0.932
GNN	0.897	0.885	0.891
LSTM	0.871	0.861	0.866
XGBoost	0.859	0.861	0.859
CNN	0.873	0.864	0.868

Table 3 The recognition results on PaySim dataset

Method	Precision	Recall	F1
RL-LGNN	0.941	0.937	0.938
GNN	0.891	0.883	0.887
LSTM	0.875	0.863	0.868
XGBoost	0.832	0.815	0.823
CNN	0.791	0.807	0.798

As shown in Figure 5, on the credit card fraud detection dataset, the recognition accuracy of RL-LGNN exceeds 0.95, whereas the standalone GNN and LSTM models both achieve accuracies above 0.90. This result indicates that the integration of temporal modelling and relational representation can improve fraud detection performance. On the PaySim Dataset, RL-LGNN achieves an accuracy of 0.949, which is markedly higher than the 0.905 obtained by the standalone GNN model. The precision, recall, and F1 scores are also reported in Tables 2 and 3. RL-LGNN consistently outperforms all baseline models across these metrics, indicating that the integration of sequential and structural information contributes to both detection sensitivity and specificity. Notably, the results highlight that the adaptive RL-based policy optimisation further enhances performance compared with models that only leverage static LSTM or GNN representations. These findings suggest that the proposed coupled framework not only

improves classification accuracy but also strengthens robustness in identifying fraudulent transactions under varying data distributions.

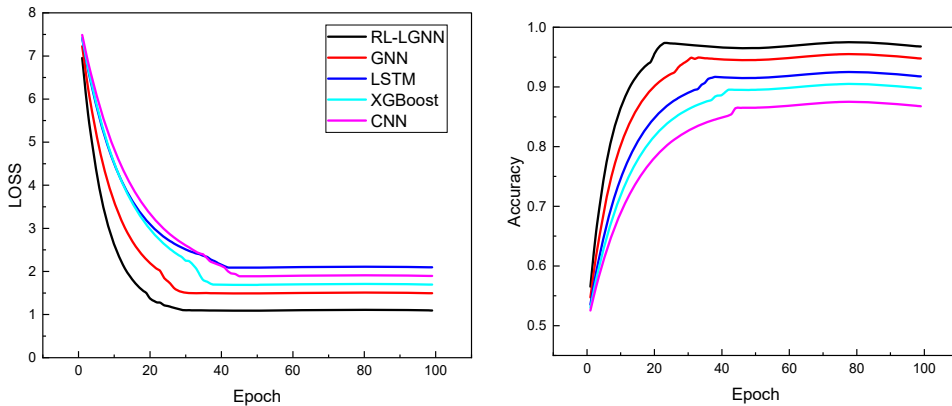
These results demonstrate that the integration of GNN, LSTM, and RL improves fraud detection accuracy across different transaction scenarios. Overall, the experimental results on both datasets verify the effectiveness of the proposed framework and confirm the contribution of temporal dependency modelling, relational feature extraction, and dynamic policy optimisation to fraud detection performance.

4.3 Practical testing and model deployment analysis

To further evaluate the applicability of the proposed framework in realistic financial scenarios involving smart contracts and distributed ledger systems, data were collected for over 150 publicly listed companies, including firms involved in financial fraud during 2006–2019, paired 1:1 with non-fraud firms. Features were constructed from financial indicators, governance attributes, and network metrics, with missing values and outliers handled via standard preprocessing. Fraud labels were assigned based on regulatory reports. Transaction graphs were built with companies as nodes and edges representing financial relationships or shared ownership. Annual sequences captured temporal behaviours. The dataset was split chronologically, with 2006–2019 for training and 2020–2023 for testing, ensuring evaluation on unseen future data.

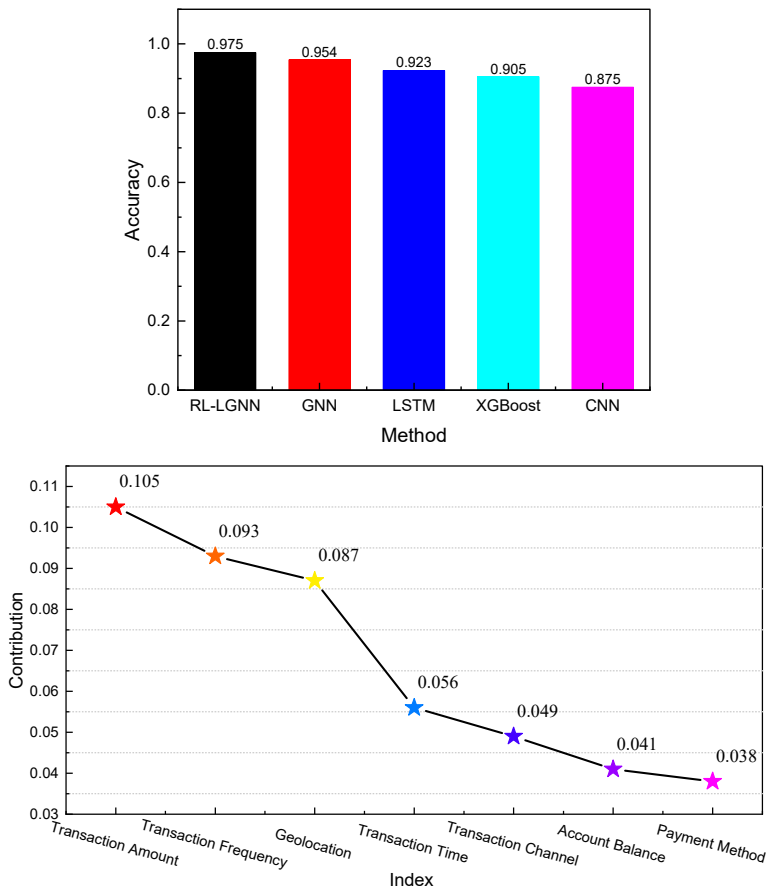
Feature importance rankings were obtained using a perturbation-based analysis, measuring the impact of feature changes on the RL-LGNN agent's output. Features causing larger output variations were considered more influential, providing interpretability despite the deep graph model's inherent opacity. The training loss and accuracy curves on this test set are shown in Figure 6, demonstrating the model's practical effectiveness under realistic deployment conditions.

Figure 6 Training loss and accuracy variation on the test dataset (see online version for colours)



As shown in Figure 6, the proposed RL-LGNN model exhibits a performance trend consistent with that observed on the public datasets. However, convergence is achieved more rapidly on this test set, which can be attributed to the relatively lower data volume and structural complexity. To further examine model performance, the recognition results of different methods and the corresponding feature importance rankings are presented in Figure 7.

Figure 7 Recognition results and feature importance ranking on the test dataset (see online version for colours)



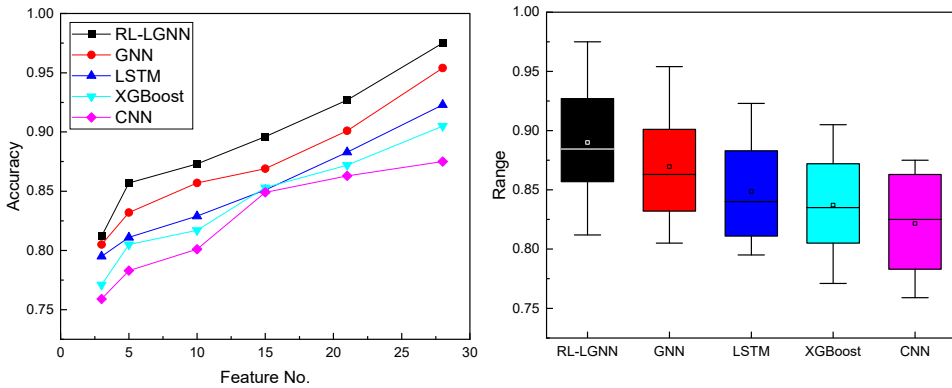
In terms of recognition accuracy, RL-LGNN achieves 0.975, outperforming the standalone GNN model at 0.954 and the LSTM model at 0.923. These results indicate that the integrated framework provides a more effective representation of both temporal and relational characteristics, thereby improving fraud identification performance. The feature importance analysis further shows that the seven most influential variables account for nearly 50% of the overall contribution, with trading volume ranked as the most important feature. This finding suggests that trading volume is a critical indicator in evaluating the risk of fraudulent behaviour in listed companies.

Considering the feature characteristics of the credit card fraud detection dataset, additional experiments were conducted under different dimensionality reduction settings. The results are shown in Figure 8.

As shown in Figure 8, the proposed RL-LGNN method maintains favourable performance across different dimensionality settings. Although the performance gap between RL-LGNN and the comparison methods is relatively limited under low-dimensional conditions, the advantage of RL-LGNN becomes more evident as the feature dimension increases. In addition, the boxplot results indicate that RL-LGNN

exhibits better overall stability, with smaller performance fluctuations and stronger consistency than the competing methods. Although the RL-LGNN framework integrates LSTM, GNN, and RL components, it has been designed to ensure efficiency and scalability. In our experiments, training was performed on an NVIDIA Tesla V100 GPU. For the Credit Card Fraud Detection Dataset, training completed within approximately 15 minutes, while for the larger PaySim Dataset, training required around 2.3 hours due to the larger graph and sequence size. The listed company dataset was trained in roughly 47.8 minutes.

Figure 8 Experimental results under different feature dimensionalities (see online version for colours)



Inference is efficient because the LSTM-GNN backbone evaluates sequences and graph embeddings sequentially, and the RL policy is applied iteratively during training without imposing overhead at runtime. Batch processing and modular design allow each component to scale independently according to dataset size as shown in Table 4.

These characteristics demonstrate that the proposed framework can be deployed in practical financial monitoring systems, enabling near-real-time fraud detection while incorporating both temporal and relational dependencies.

Table 4 Training time and deployment feasibility of RL-LGNN

<i>Dataset</i>	<i>Training time</i>	<i>Notes</i>
Credit card fraud detection	15.8 minutes	Small-scale dataset, two-day transaction records
PaySim	2.3 hours	Large synthetic dataset, batch processing applied
Listed company dataset	47.8 minutes	Temporal sequences per company-year, moderate size

To evaluate the contribution of each module in the proposed RL-LGNN framework, we conducted an ablation study under the same experimental settings as the main experiments. Specifically, RL-GNN removes the LSTM module, RL-LSTM removes the GNN module, LSTM-GNN removes the RL module, and RL-LGNN denotes the complete model. The results are shown in Table 5. It can be observed that the full RL-LGNN model achieves the best performance on both datasets, while removing any one component leads to a noticeable decline. This indicates that temporal modelling,

graph relational learning, and RL-based decision optimisation all play important roles in improving fraud detection performance.

Table 5 Ablation results of different model variants

<i>Method</i>	<i>Credit card fraud detection dataset</i>			<i>PaySim dataset</i>		
	<i>Precision</i>	<i>Recall</i>	<i>F1</i>	<i>Precision</i>	<i>Recall</i>	<i>F1</i>
RL-GNN (without LSTM)	0.934	0.911	0.922	0.947	0.926	0.936
RL-LSTM (without GNN)	0.928	0.903	0.915	0.941	0.919	0.930
LSTM-GNN (without RL)	0.946	0.925	0.935	0.955	0.934	0.944
RL-LGNN (full model)	0.962	0.941	0.951	0.971	0.948	0.959

5 Conclusions

The proposed RL-LGNN framework provides an effective solution for fraud detection in financial transaction settlement. By integrating LSTM for temporal feature extraction, GNN for relational modelling, and RL for dynamic strategy optimisation, the framework improves both detection accuracy and robustness. Experimental results on three datasets show fraud recognition accuracies of 0.954, 0.949, and 0.975, respectively, demonstrating its effectiveness in complex transaction environments with dense interactions and heterogeneous structures. These findings indicate that RL-LGNN has strong potential for practical application in financial fraud detection and can provide technical support for financial security and compliance management.

Several limitations should also be noted. First, the current evaluation is conducted on public datasets and a limited self-constructed dataset, which may not fully reflect the diversity and complexity of real-world financial transaction scenarios. Second, although the proposed framework shows favourable performance in static experimental settings, its effectiveness in real-time monitoring and large-scale cross-border transaction environments remains to be further verified. Third, the integration of LSTM, GNN, and RL increases model complexity and computational cost, which may restrict deployment efficiency in resource-constrained settings. In addition, the adaptability of the framework to more complex fraud patterns and rapidly evolving transaction behaviours still requires further investigation.

Declarations

Author declares no conflicts of interest.

References

- Azamuke, D., Katarahweire, M. and Bainomugisha, E. (2022) ‘Scenario-based synthetic dataset generation for mobile money transactions’, in *Proceedings of the Federated Africa and Middle East Conference on Software Engineering (FAMECSE '22)*, Association for Computing Machinery, New York, NY, USA, pp.64–72, DOI: 10.1145/3531056.3542774.
- Bello, O.A., Folorunso, A., Ejiofor, O.E., Budale, F.Z., Adebayo, K. and Babatunde, O.A. (2023) ‘Machine learning approaches for enhancing fraud prevention in financial transactions’, *International Journal of Management Technology*, Vol. 10, No. 1, pp.85–108.
- Chen, Y. and Han, X. (2021) ‘CatBoost for fraud detection in financial transactions’, in *2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, IEEE, Piscataway, NJ, USA, pp.176–179, DOI: 10.1109/ICCECE51280.2021.9342475.
- El Naby, A.A., El-Din Hemdan, E. and El-Sayed, A. (2021) ‘Deep learning approach for credit card fraud detection’, in *2021 International Conference on Electronic Engineering (ICEEM)*, IEEE, Piscataway, NJ, USA, pp.1–5, DOI: 10.1109/ICEEM52022.2021.9480639.
- Fiore, U., De Santis, A., Perla, F., Zanetti, P. and Palmieri, F. (2019) ‘Using generative adversarial networks for improving classification effectiveness in credit card fraud detection’, *Information Sciences*, Vol. 479, pp.448–455, DOI: 10.1016/j.ins.2017.12.030.
- Fu, K., Cheng, D., Tu, Y. and Zhang, L. (2016) ‘Credit card fraud detection using convolutional neural networks’, in Hirose, A. et al. (Eds.): *Neural Information Processing*, Springer International Publishing, Cham., pp.483–490, DOI: 10.1007/978-3-319-46675-0_53.
- Gülmez, B. (2023) ‘Stock price prediction with optimized deep LSTM network with artificial rabbits optimization algorithm’, *Expert Systems with Applications*, Vol. 227, p.120346, DOI: 10.1016/j.eswa.2023.120346.
- Hajek, P., Abedin, M.Z. and Sivarajah, U. (2023) ‘Fraud detection in mobile payment systems using an XGBoost-based framework’, *Information Systems Frontiers*, Vol. 25, No. 5, pp.1985–2003, DOI: 10.1007/s10796-022-10346-6.
- Heryadi, Y. and Warnars, H.L.H.S. (2017) ‘Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNN-LSTM’, in *2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, IEEE, Piscataway, NJ, USA, pp.84–89, DOI: 10.1109/CYBERNETICSCOM.2017.8311689.
- Johora, F.T., Hasan, R., Farabi, S.F., Akter, J. and Mahmud, M.A.A. (2024) ‘AI-Powered fraud detection in banking: safeguarding financial transactions’, *The American Journal of Management and Economics Innovations*, Vol. 6, No. 6, pp.8–22, DOI: 10.37547/tajmei/Volume06Issue06-02.
- Li, Z., Liu, G. and Jiang, C. (2020) ‘Deep representation learning with full center loss for credit card fraud detection’, *IEEE Transactions on Computational Social Systems*, Vol. 7, No. 2, pp.569–579, DOI: 10.1109/TCSS.2020.2970805.
- Liu, Y., Ao, X., Qin, Z., Chi, J., Feng, J., Yang, H. and He, Q. (2021) ‘Pick and choose: a GNN-based imbalanced learning approach for fraud detection’, in *Proceedings of the Web Conference 2021 (WWW '21)*, Association for Computing Machinery, New York, NY, USA, pp.3168–3177, DOI: 10.1145/3442381.3449989.
- Naritomi, Y. and Adachi, T. (2020) ‘Data augmentation of high frequency financial data using generative adversarial network’, in *2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, IEEE, Piscataway, NJ, USA, pp.641–648, DOI: 10.1109/WIAT50758.2020.00097.
- Olorunnimbe, K. and Viktor, H. (2023) ‘Deep learning in the stock market – a systematic survey of practice, backtesting, and applications’, *Artificial Intelligence Review*, Vol. 56, No. 3, pp.2057–2109, DOI: 10.1007/s10462-022-10226-0.
- Ozbayoglu, A.M., Gudelek, M.U. and Sezer, O.B. (2020) ‘Deep learning for financial applications: a survey’, *Applied Soft Computing*, Vol. 93, p.106384, DOI: 10.1016/j.asoc.2020.106384.

- Qiu, J., Shu, L. and Zhang, Y. (2025) 'The deep learning-based security assessment and optimization model for enterprise information systems under digital economy', *Journal of Organizational and End User Computing (JOEUC)*, Vol. 37, No. 1, pp.1–52, DOI: 10.4018/JOEUC.382092.
- Rong, C., Sial, M.S., Saci, F., Jasimuddin, S.M. and Zhang, J.Z. (2025) 'AI adoption in the finance sector of a developing economy: The mediating role of perceived trust', *Journal of Organizational and End User Computing (JOEUC)*, Vol. 37, No. 1, pp.1–29, DOI: 10.4018/JOEUC.371412.
- Shi, X., Wang, Z., Zhao, H., Qiu, S., Liu, R., Lin, F. and Tang, K. (2023) 'Threshold-free phase segmentation and zero velocity detection for gait analysis using foot-mounted inertial sensors', *IEEE Transactions on Human-Machine Systems*, Vol. 53, No. 1, pp.176–186, DOI: 10.1109/THMS.2022.3228515.
- Tekkali, C.G. and Natarajan, K. (2023) 'RDQN: Ensemble of deep neural network with reinforcement learning in classification based on rough set theory for digital transactional fraud detection', *Complex & Intelligent Systems*, Vol. 9, No. 5, pp.5313–5332, DOI: 10.1007/s40747-023-01016-4.
- Théate, T. and Ernst, D. (2021) 'An application of deep reinforcement learning to algorithmic trading', *Expert Systems with Applications*, Vol. 173, p.114632, DOI: 10.1016/j.eswa.2021.114632.
- Tong, G. and Shen, J. (2023) 'Financial transaction fraud detector based on imbalance learning and graph neural network', *Applied Soft Computing*, Vol. 149, p.110984, DOI: 10.1016/j.asoc.2023.110984.
- Xu, J., Yang, T., Zhuang, S., Li, H. and Lu, W. (2024) 'AI-based financial transaction monitoring and fraud prevention with behaviour prediction', *Applied and Computational Engineering*, Vol. 77, pp.218–224, DOI: 10.54254/2755-2721/77/2024MA0068.
- Zhang, S., Zhong, Y., Sentosa, I. and Liang, X. (2025) 'Optimizing the operation mechanism of public data assets and data-driven decision models in the digital economy with deep neural networks', *Journal of Organizational and End User Computing (JOEUC)*, Vol. 37, No. 1, pp.1–22, DOI: 10.4018/JOEUC.390258.
- Zhang, Y., Zhao, P., Wu, Q., Li, B., Huang, J. and Tan, M. (2022a) 'Cost-sensitive portfolio selection via deep reinforcement learning', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 34, No. 1, pp.236–248, DOI: 10.1109/TKDE.2020.2979700.
- Zhang, Y-F., Lu, H-L., Lin, H-F., Qiao, X-C. and Zheng, H. (2022b) 'The optimized anomaly detection models based on an approach of dealing with imbalanced dataset for credit card fraud detection', *Mobile Information Systems*, Vol. 2022, No. 1, p.8027903, DOI: 10.1155/2022/8027903.
- Zhang, Z., Chen, L., Liu, Q. and Wang, P. (2020) 'A fraud detection method for low-frequency transaction', *IEEE Access*, Vol. 8, pp.25210–25220, DOI: 10.1109/ACCESS.2020.2970614.
- Zhang, Z., Zhou, X., Zhang, X., Wang, L. and Wang, P. (2018) 'A model based on convolutional neural network for online transaction fraud detection', *Security and Communication Networks*, Vol. 2018, No. 1, p.5680264, DOI: 10.1155/2018/5680264.
- Zhou, L., Wang, Y., Ge, J., Chen, B., Ge, B. and Wu, C-H. (2025) 'Organizational financialization and innovative investment: Calculation on the enterprise data of a typical economy', *Journal of Organizational and End User Computing (JOEUC)*, Vol. 37, No. 1, pp.1–24, DOI: 10.4018/JOEUC.389251.
- Zou, H., Zhu, J., Rosset, S. and Hastie, T. (2009) 'Multi-class AdaBoost', *Statistics and its Interface*, Vol. 2, pp.349–360.