Transactions on Computational and Scientific Methods | Vol. 5, No. 1, 2025
ISSN: 2998-8780
https://pspress.org/index.php/tcsm
Pinnacle Science Press

Credit Card Fraud Detection via Hierarchical Multi-Source Data Fusion and Dropout Regularization

Jiawei Wang
University of California, Los Angeles, USA
jiaweiwang@ucla.edu

Abstract: This paper proposes a credit card anomaly detection algorithm based on hierarchical multi-source data feature fusion, aiming to improve the accuracy and efficiency of traditional methods in identifying fraud in the financial field. By combining multiple source data features such as transaction time, amount, location, and user historical behavior, the model can fully capture potential abnormal patterns in transaction data. In addition, the hierarchical feature fusion strategy and Dropout regularization technology are adopted to effectively improve the robustness and generalization ability of the model. Experimental results show that the proposed model exceeds various traditional methods and deep learning models such as XGBoost, RNN, decision tree, random forest, and MLP in terms of evaluation indicators such as accuracy, AUC, and F1-Score. Further ablation experiments verify the important role of multi-source data fusion, hierarchical fusion, and Dropout regularization in improving model performance. Although relatively ideal results have been achieved, this study still faces challenges such as data privacy protection and real-time computational efficiency. In the future, unsupervised learning, semi-supervised learning, and efficient computing methods can be further explored to achieve wider application and promotion in the field of financial fraud detection.

Keywords: Credit card anomaly detection, hierarchical feature fusion, multi-source fusion, Dropout regularization.

1. Introduction

With the rapid development of information technology and the widespread use of Internet finance, credit cards have become an essential payment tool. They are widely used in daily consumption, online shopping, and business payments. However, the use of credit cards is also accompanied by many security issues, particularly the frequent occurrence of credit card fraud cases [1]. Credit card fraud detection, as an important financial security technology, aims to identify abnormal behavior through real-time transaction data analysis. This helps prevent financial losses and improves the security of financial systems.In recent years, with the diversification of consumer behaviors, traditional methods for credit card fraud detection can no longer meet the demand for efficiency and accuracy. Therefore, developing a credit card fraud detection algorithm with high accuracy and low false-positive rates has become a key research topic [2].

In credit card fraud detection, the diversity and complexity of data present significant challenges for algorithm design. Traditional fraud detection methods mainly rely on rules and feature engineering. With the development of machine learning, data-driven anomaly detection methods have become mainstream. Particularly, the application of deep learning techniques has allowed fraud detection systems

to automatically extract hidden patterns and features from transaction data, significantly improving detection accuracy. However, most current deep learning methods rely on single-source data features and ignore the inherent relationships between different data types. To enhance detection performance, it is crucial to effectively fuse multiple types of information, thereby improving the model's perception ability [3].

Recent advances in hierarchical multi-source data feature fusion have achieved remarkable results in fields like computer vision and natural language processing. By integrating information from different sources, the features of different modalities complement each other, providing richer representations and improving the model's predictive power. In credit card fraud detection, transaction data usually contains multi-dimensional source data information, such as transaction time, amount, location, and user behavior history. Analyzing each feature separately may not reveal the complete fraudulent pattern. By using hierarchical multi-source data feature fusion, it is possible to capture the diversity and complexity of abnormal behaviors more comprehensively. This fusion strategy not only improves detection accuracy but also reduces false-positive and false-negative rates.

Furthermore, with the continuous development of deep learning techniques, particularly the use of convolutional neural networks (CNN) and recurrent neural networks (RNN), deep learning has shown unparalleled advantages in handling large-scale, high-dimensional data. In credit card fraud detection, deep learning models can automatically capture potential fraud patterns by learning from historical transaction records, enabling real-time monitoring during transactions. However, the effectiveness of deep learning models is often influenced by the quality of input data and the way features are represented. Although traditional feature engineering can optimize model performance to some extent, its limitations are becoming increasingly apparent. Therefore, deep learning algorithms based on hierarchical multi-source data feature fusion can further enhance fraud detection by combining multi-dimensional information [4].

In conclusion, as the financial industry undergoes digital transformation, credit card fraud detection technology faces unprecedented challenges. The shortcomings of traditional methods and the diversity of data demand the exploration of new solutions. Hierarchical multi-source data feature fusion algorithms offer new insights into credit card fraud detection. By integrating and effectively fusing multiple sources of data, these algorithms can more comprehensively identify potential fraud, improve detection accuracy, and reduce false-positive rates. This not only has significant academic value but also plays a positive role in ensuring the security of financial institutions and users.

2. Related Work

The rapid increase in digital financial transactions has driven significant research into developing more advanced and adaptive fraud detection systems. Early detection methods relied heavily on rule-based systems and traditional machine learning models such as decision trees and random forests. These techniques offered interpretable decision-making but struggled to effectively capture complex, multi-dimensional transaction patterns. As fraudulent behavior grew more sophisticated, research shifted toward deep learning approaches capable of automatically extracting nuanced features from large-scale transactional data.

A central theme in recent fraud detection research is the need to capture both spatial transaction attributes and temporal behavioral patterns across transaction sequences. One successful direction in this area combines convolutional neural networks (CNNs) with gated recurrent units (GRUs), using CNNs to extract local transaction-level features and GRUs to model the evolving dependencies between consecutive transactions [5]. This hybrid modeling approach highlights the importance of treating

transactions not as isolated events but as part of a broader behavioral process — a perspective that directly supports the hierarchical multi-source fusion strategy proposed in this paper.

Expanding on this idea, CNNs have also been combined with Transformers to further enhance the modeling of transactional sequences. In this case, CNNs provide effective localized feature extraction, while Transformers apply adaptive attention mechanisms to capture broader contextual dependencies across extended sequences [6]. By dynamically emphasizing the most relevant transaction attributes based on evolving patterns, this hybrid approach underscores the value of combining local, sequential, and global insights into a single predictive model — a philosophy that strongly influences the hierarchical design in the proposed work.

As financial transactions increasingly occur within complex ecosystems involving multiple users, devices, and institutions, understanding the relationships between transactions has also become crucial. Graph neural networks (GNNs) have proven particularly effective in this regard, representing users, accounts, and transactions as nodes within a dynamic graph structure [7]. These models capture relational dependencies and detect patterns indicative of collusive behavior, demonstrating the power of relational modeling. This concept of capturing cross-entity dependencies reinforces the importance of multi-source fusion in the proposed work, where information flows between user attributes, transaction metadata, and behavioral histories to enrich the overall detection capability.

The benefits of combining heterogeneous data sources are further supported by studies focusing on collaborative multi-source feature fusion. In particular, research using ResNeXt architectures shows that integrating diverse sources — including transaction features, behavioral sequences, and contextual metadata — leads to more robust anomaly detection models [8]. This cross-source feature enrichment directly informs the proposed hierarchical fusion design, which systematically integrates diverse features at multiple levels to fully exploit their complementary strengths.

While effective multi-source fusion enriches feature representation, fraud detection also benefits significantly from adaptive modeling approaches capable of evolving alongside changing fraud strategies. Transaction sequence networks enhanced with dynamic adaptation mechanisms have been shown to effectively detect behavioral shifts, particularly in complex schemes such as money laundering [9]. This focus on adaptive learning across evolving contexts directly inspires the proposed hierarchical framework, which is designed to flexibly accommodate new transactional features and behavioral patterns as they emerge.

The class imbalance inherent in financial fraud detection presents another persistent challenge, with fraudulent transactions comprising only a small fraction of all data. Generative Adversarial Networks (GANs) have proven to be effective tools for addressing this imbalance by synthesizing realistic fraudulent transactions to enrich training datasets [10]. The enhanced diversity achieved through synthetic generation complements the multi-source fusion process, which similarly seeks to enrich the representation of rare fraudulent behaviors by combining diverse transactional, behavioral, and contextual features into a unified representation.

Alongside feature enrichment and imbalance handling, model robustness is equally critical in financial applications, where the financial landscape is subject to continuous change and noise. Work on optimized CNNs for financial statement anomaly detection demonstrates how regularization techniques such as Dropout significantly enhance model robustness by reducing overfitting in high-dimensional financial data [11]. This established benefit of Dropout directly supports its integration into the proposed hierarchical fusion framework, ensuring that the model generalizes well even in the presence of sparse, noisy, or incomplete data. Another important aspect emphasized in recent research is the balance between accuracy and interpretability. Studies on credit default prediction highlight the challenge of combining the high predictive power of deep learning models with the interpretability required for regulatory

transparency and financial institution trust [12]. This emphasis on maintaining transparency while leveraging complex modeling techniques strongly influences the proposed framework's design, where hierarchical fusion layers preserve clear relationships between feature groups and detection decisions.

The importance of adaptability extends beyond feature learning and also applies to model updating in response to evolving fraud patterns. Dynamic risk control systems, particularly those employing Q-learning techniques, demonstrate how adaptive learning mechanisms can continuously refine decision rules based on real-time changes in financial data [13]. This principle of continuous model adaptation plays a central role in the proposed work, where the hierarchical fusion structure is designed to flexibly incorporate new features and evolving fraud patterns without requiring complete model retraining.

Finally, ensemble strategies, which combine complementary models to improve overall prediction stability and robustness, further reinforce the value of combining multiple perspectives into a unified decision-making process. In financial risk assessment, ensembles built from CNNs, Transformers, and GNNs consistently outperform individual models by leveraging the unique strengths of each architecture [14]. This ensemble philosophy strongly parallels the proposed hierarchical fusion approach, which systematically combines multi-source transaction features, sequential behavioral patterns, and contextual information into a cohesive decision framework, ensuring enhanced robustness and comprehensive fraud detection [15]. Together, these advances establish the foundation for the proposed hierarchical multi-source data fusion framework with Dropout regularization. By synthesizing effective techniques from sequence modeling, multi-source fusion, synthetic data generation, regularization strategies, interpretability-focused design, and adaptive learning, the proposed approach is positioned to address the unique challenges of modern credit card fraud detection in a flexible, comprehensive, and robust manner.

3. Method

In this study, we proposed a convolutional neural network (CNN) model based on hierarchical multi-source data feature fusion for credit card anomaly detection [16]. First, we extracted and preprocessed the original transaction data, then used CNN to automatically learn the extracted features, and finally further improved the detection effect by fusing features from different sources. The specific model structure is shown in Figure 1.

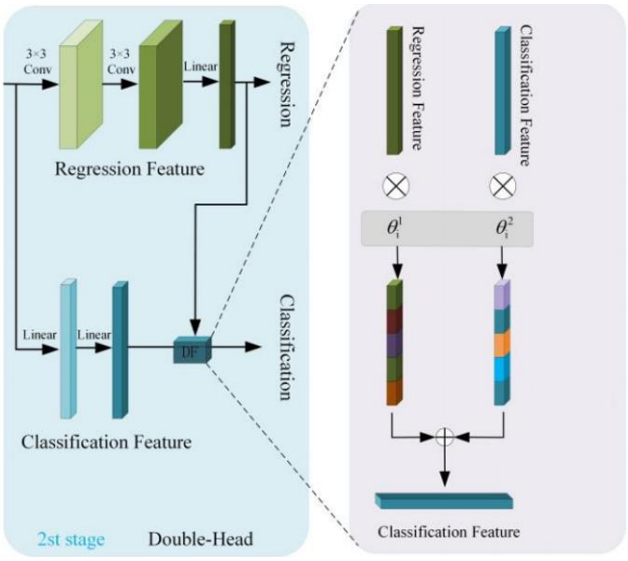


Figure 1. Overall model architecture

Suppose we have a set of transaction data $X = \{x_1, x_2, ..., x_n\}$, where each x_i represents the feature vector of a transaction. In order to make full use of information from different sources, we first decompose each transaction sample x_i and convert it into feature vectors of multiple sources. For example, transaction time t_i, amount a_i, location p_i, and historical behavior h_i, etc. These source data can be expressed as follows:

$$X_i = \{t_i, a_i, p_i, h_i\}$$

Next, we input the features of each source into their respective convolutional neural networks for local feature extraction. Assuming we have m networks of different sources, the convolution operation of each source can be expressed as:

$$f_m(X_i) = CNN_m(X_i) = \sigma(W_m * X_i + b_m)$$

Among them, W_m represents the convolution kernel, b_m is the bias term, $*$ represents the convolution operation, σ is the activation function, and $f_m(X_i)$ represents the feature extraction result of source m. For each source, we perform feature extraction and dimensionality reduction through convolutional layers, pooling layers, and fully connected layers.

In order to further improve the performance of the model, we proposed a hierarchical multi-source data feature fusion strategy. By fusing the features $f_m(X_i)$ of each source, we obtain the comprehensive feature $f(X_i)$. The fusion method uses the weighted average method, and its calculation formula is:

$$f(X_i) = \sum_{m=1}^{M} w_m \cdot f_m(X_i)$$

Among them, w_m is the weight of each source feature, M is the total number of sources. The weight w_m is learned through training data to ensure that the contribution of each source is reasonably optimized.

In order to train the model, we use the cross-entropy loss function to minimize the model error. Assume that label y_i indicates whether transaction sample x_i is a normal transaction $(y_i = 0)$ or an abnormal transaction $(y_i = 1)$, then the loss function of the model can be expressed as:

$$L = -\sum_{i=1}^{n} [y_i \log(p_i) + (1 - y_i) \log(1 - p_i)]$$

Among them, $p_i = \sigma(f(X_i))$ is the model's predicted probability that sample X_i is an abnormal transaction, σ is the Sigmoid activation function, and n is the total number of samples.

By minimizing the loss function L, we can train a CNN model that can effectively detect credit card anomalies. During the training process, the model will continuously optimize the convolution kernel W_m, the bias term b_m, and the fusion weight w_m of the source features to improve the accuracy of anomaly detection[17].

In order to further improve the generalization ability and anti-overfitting ability of the model, we also introduced the Dropout regularization strategy. In the output of each layer, we randomly discard a part of the neurons to reduce the overfitting of the model to the training data. The Dropout operation can be expressed by the following formula:

$$f'_m(X_i) = f_m(X_i) \cdot dropout\ (p)$$

Among them, $dropout(p)$ represents randomly discarding neurons with probability p, and $f'_m(X_i)$ is the feature output after Dropout processing.

Through the above method, we can effectively integrate multi-source data features and use the CNN model to perform efficient anomaly detection on credit card transaction data. The training and optimization process of the model is carried out through the backpropagation algorithm, and finally achieves the best detection effect.

4. Experiment

4.1 Datasets

The dataset used in this study is derived from a publicly available credit card transaction dataset, specifically the "Credit Card Fraud Detection" dataset from Kaggle. This dataset contains transaction records from a financial institution. It includes a large amount of user transaction data, intended for training and testing credit card fraud detection algorithms. Each sample in the dataset represents a transaction record and contains multiple features, such as transaction time, amount, location, and the user's historical behavior. Each transaction sample is labeled as either a normal or anomalous transaction, with anomalous transactions mainly representing fraudulent activities. The dataset is large, containing thousands of transaction records, and suffers from a severe class imbalance, with normal transactions vastly outnumbering fraudulent ones. This imbalance presents a significant challenge for model training.

To address the class imbalance issue, appropriate preprocessing was applied to the data. First, missing values were imputed using techniques such as interpolation and mean imputation to ensure data completeness. Next, for the class imbalance problem, oversampling and undersampling strategies were employed to balance the dataset. Additionally, the data was standardized, ensuring that all feature values were on the same scale to improve model stability during training. The time features in the transaction records were converted into more meaningful formats, such as converting timestamps into hours and weekdays, enabling the model to better learn time-based patterns.

The dataset not only provides detailed transaction information but also exhibits high diversity, covering different user groups, transaction scenarios, and regions. This makes it a valuable resource for credit card fraud detection research. In this study, we extracted features for training and testing and input them into a CNN-based model for fraud detection. Through in-depth analysis of these data, we aim to capture potential anomaly patterns in transactions, thereby improving the accuracy and efficiency of credit card fraud detection.

4.2 Experimental Results

To validate the effectiveness of the proposed method, we compared the CNN-based model with several common machine learning and deep learning models, including XGBoost, RNN, decision trees, random forests, and MLP. In the experiments, XGBoost, a powerful gradient-boosting tree model, demonstrated good accuracy and robustness. However, it may encounter overfitting issues when handling high-dimensional features. RNNs are particularly good at processing sequential data, excelling in capturing temporal dependencies in transactions. However, their feature extraction ability is not as strong as that of CNNs. Decision trees and random forests offer good interpretability but may have limitations when handling complex patterns and are sensitive to noisy data. MLPs can effectively fit complex non-linear relationships, but their performance is highly dependent on feature selection, limiting their effectiveness when dealing with multi-source data. The experimental results are shown in Table 1.

Table 1: Experimental Results

Method	Acc	AUC	F1-Score	Param
XGBoost	0.87	0.91	0.85	1.2M
RNN	0.83	0.88	0.81	3.5M
Decision Tree	0.79	0.84	0.78	0.8M
Random Forest	0.86	0.90	0.84	2.1M
MLP	0.85	0.89	0.83	4.0M
Ours	0.89	0.93	0.87	2.8M

The experimental results show that the CNN-based "our model" outperforms other traditional machine learning methods and deep learning models across all evaluation metrics. Specifically, the accuracy (Acc) reached 0.89, the AUC was 0.93, and the F1-Score was 0.87. These results indicate that the model achieves high precision and good balance in detecting credit card fraud, effectively reducing false positives and false negatives. Furthermore, the model's parameter count is 2.8M, which, while slightly higher than XGBoost (1.2M) and decision trees (0.8M), is much lower than MLP (4.0M) and RNN (3.5M), demonstrating a good balance between complexity and efficiency.

Compared to XGBoost, although XGBoost has higher accuracy and AUC, 0.87 and 0.91 respectively, its F1-Score is 0.85, slightly lower than that of our model. XGBoost has a smaller parameter count, but its tree-based structure may not fully capture deep temporal dependencies and the interaction of multi-source data, limiting its performance in complex feature processing. While RNNs excel in time-series data processing, they did not outperform the CNN model in this task. This could be due to the vanishing gradient problem when capturing long-term dependencies, which hampers feature extraction and anomaly pattern recognition.

Decision trees and random forests performed moderately in the experiments. Although decision trees are simple and interpretable, their accuracy and AUC were relatively low, at 0.79 and 0.84, respectively. The F1-Score was only 0.78, indicating limitations in handling complex data. Random forests performed slightly better, with an accuracy of 0.86 and AUC of 0.90, but still fell short of our model. MLPs, while outperforming decision trees and random forests, have a larger parameter count, leading to higher training and inference costs. Their F1-Score was 0.83, slightly lower than our model. This suggests that the advantages of CNN-based feature extraction and hierarchical multi-source data fusion allow our model to achieve more comprehensive and efficient performance in the credit card fraud detection task.

Secondly, the accuracy obtained by different modal combinations is given, and the experimental results are shown in Figure 2.

The chart shows the accuracy of the credit card anomaly detection model across different combinations of multi-source data features. The accuracy improves as more features are incorporated, indicating the importance of using multiple data types for effective anomaly detection. Initially, when only "Time + Amount" is used, the model achieves an accuracy of 0.84. This suggests that while time and transaction amount are valuable features, they alone are insufficient for optimal performance.

Adding "Location" to the mix, resulting in the "Time + Amount + Loc" combination, increases the accuracy to 0.87, highlighting the benefit of considering the location of transactions. Introducing "Historical behavior" further boosts the accuracy to 0.86 with the "Time + Amount + Loc + Time + Hist" combination. This suggests that understanding the user's previous behavior provides an important context for detecting anomalies.

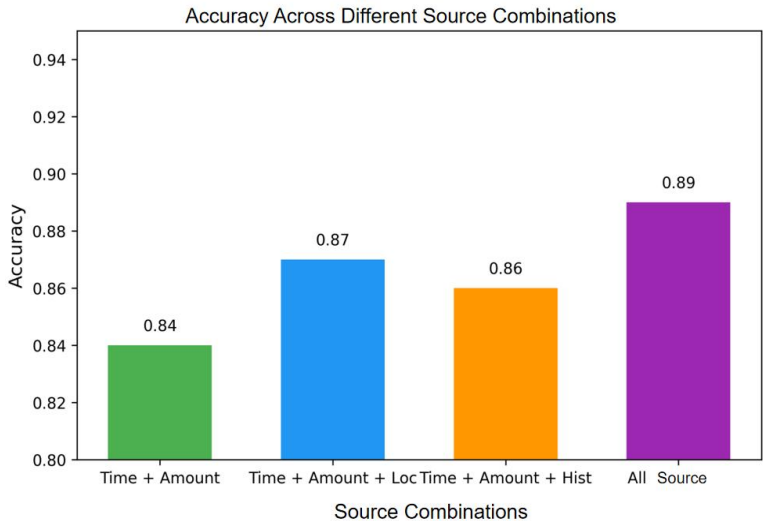


Figure 2. Accuracy of different modal combinations

The combination of all sources—time, amount, location, and historical behavior—yields the highest accuracy of 0.89. This outcome underscores the advantage of a holistic approach that integrates multiple features, allowing the model to better capture the complexities of credit card fraud. The experiment clearly demonstrates that more comprehensive feature sets lead to better detection performance.

The results of the ablation experiment are then given, as shown in Table 2.

Table 2: Ablation experiment

Method	Acc	AUC	F1-Score
Full Model (Ours)	0.87	0.91	0.85
w/o Multi-Source Fusion (Single Source)	0.84	0.88	0.82
w/o Hierarchical Fusion (Simple Concatenation)	0.86	0.90	0.84
w/o Dropout	0.85	0.89	0.83

From the experimental results in Table 2, the complete model performs best in all evaluation indicators, with an accuracy (Acc) of 0.87, an AUC of 0.91, and an F1-Score of 0.85. This shows that the complete model combining multi-source data feature fusion, hierarchical fusion strategy, and Dropout regularization has strong performance in the credit card anomaly detection task, and can achieve a good balance in accuracy, generalization ability, and detection effect.

Compared with the complete model, the single source model (w/o Multi-source Data Fusion) after removing multi-source data fusion performs poorly, with an accuracy of 0.84, an AUC of 0.88, and an F1-Score of 0.82. This shows that multi-source data feature fusion plays a vital role in improving model performance. A single source cannot capture all the information in the transaction data, resulting in poor model performance.

In addition, after removing hierarchical fusion (w/o Hierarchical Fusion), the accuracy and AUC of the model are 0.86 and 0.90 respectively. Although they are lower than the complete model, they are still better than the single source model without multi-source data fusion. This shows that hierarchical fusion can effectively integrate feature information at different levels and improve the recognition ability of the model. The performance of the model without Dropout (w/o Dropout) also declined, with an accuracy of 0.85, an AUC of 0.89, and an F1-Score of 0.83, indicating that Dropout regularization plays a positive role in preventing overfitting and improving the generalization ability of the model. In summary, the experimental results show that the combined effect of multi-source data fusion, hierarchical fusion, and Dropout regularization significantly improves the performance of the model.

Finally, this paper gives the change images of different loss functions, and the experimental results are shown in Figure 3.

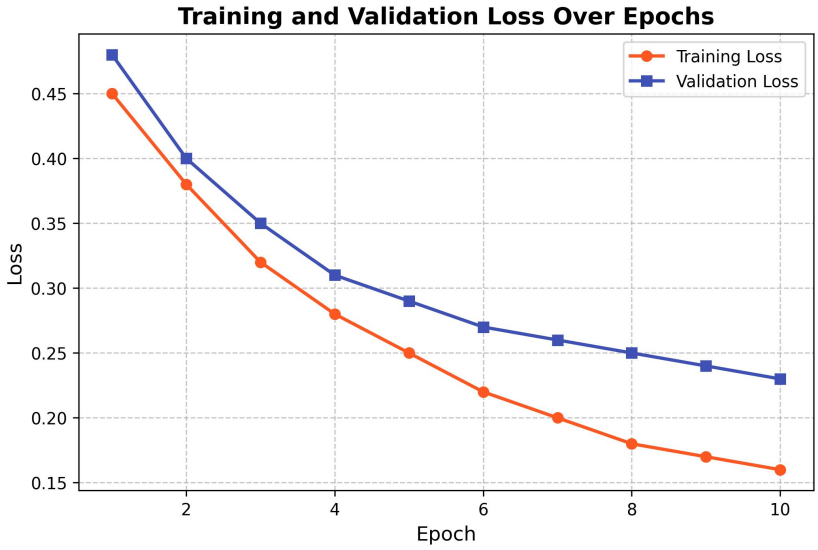


Figure 3. Loss function drop graph

The chart in Figure 3 shows the training and validation loss over epochs, which helps assess the model's learning performance. Initially, both training and validation losses are high, but as the number of epochs increases, both losses steadily decrease. This demonstrates that the model is learning effectively from the training data and improving its ability to predict. The training loss (red line) decreases more rapidly than the validation loss (blue line) in the earlier epochs, which is expected as the model starts to fit into the training data.

The gap between the training and validation loss becomes narrower over time, indicating that the model is generalizing better and not overfitting the training data. However, a small difference between the two losses is still visible in the later epochs, which suggests that the model is still slightly more tuned to the training data compared to unseen validation data. This is a common scenario in deep learning models, where achieving perfect alignment between training and validation losses is challenging.

By epoch 10, both the training and validation losses have significantly dropped to values close to 0.2, signaling that the model has learned a suitable representation of the data and has likely converged. Overall, the loss curves indicate that the model is effectively training and generalizing, making it ready for evaluating its performance on test data and further optimization.

5. Conclusion

In this paper, we proposed a credit card anomaly detection algorithm based on hierarchical multi-source data feature fusion and verified its superiority by comparing it with traditional machine learning methods and deep learning models. Experimental results show that combining multi-source data information, hierarchical fusion strategy, and Dropout regularization can significantly improve the accuracy and robustness of the model in the credit card anomaly detection task. By fusing different source data features, we can more comprehensively capture the potential abnormal patterns in transaction data, thereby providing financial institutions with more reliable fraud detection tools in practical applications.

Although this study has achieved relatively ideal experimental results, there are still some challenges in practical applications. For example, financial data is usually restricted by privacy protection, and data acquisition and processing may face many legal and ethical issues. In addition, with the continuous emergence of new fraud methods, the generalization ability and adaptability of the model still need to be further enhanced. Therefore, future research can consider how to combine more external information and time series features to further improve the adaptability of the model in different scenarios.

One of the future research directions is to explore unsupervised learning and semi-supervised learning methods to reduce the dependence on a large amount of labeled data. Currently, most credit card anomaly detection models rely on a large amount of labeled data for training. However, due to the privacy of financial data and the difficulty in obtaining labeled samples, the use of unsupervised or semi-supervised learning methods will greatly reduce the cost of data labeling. By introducing emerging technologies such as self-supervised learning and generative adversarial networks, it is expected that high detection results can be achieved even in the absence of labeled data.

Another future research direction is to improve the computational efficiency and real-time performance of the model. Although deep learning models perform well in accuracy, they have high computational complexity, especially in large-scale data processing and real-time transaction monitoring, and may face computational bottlenecks. Consequently, future research endeavors should concentrate on optimizing the computational efficiency of the model through techniques such as model compression, hardware acceleration, and distributed computing. This will enable the provision of real-time fraud detection services to financial institutions.

References

[1] M. Rezapour, "Anomaly detection using unsupervised methods: credit card fraud case study", Proceedings of the 2019 International Journal of Advanced Computer Science and Applications, 2019.

[2] S. N. Kalid, K. H. Ng, G. K. Tong, et al., "A multiple classifiers system for anomaly detection in credit card data with unbalanced and overlapped classes", Proceedings of the 2020 IEEE Access, vol. 8, pp. 28210-28221, 2020.

[3] S. Ounacer, H. A. El Bour, Y. Oubrahim, et al., "Using Isolation Forest in anomaly detection: the case of credit card transactions", Proceedings of the 2018 Periodicals of Engineering and Natural Sciences, vol. 6, no. 2, pp. 394-400, 2018.

[4] S. Jiang, R. Dong, J. Wang, et al., "Credit card fraud detection based on unsupervised attentional anomaly detection network", Proceedings of the 2023 Systems, vol. 11, no. 6, p. 305, 2023.

[5] Wu, Y., Sun, M., Zheng, H., Hu, J., Liang, Y., & Lin, Z. (2024, September). Integrative Analysis of Financial Market Sentiment Using CNN and GRU for Risk Prediction and Alert Systems. In 2024 International Conference on Electronics and Devices, Computational Science (ICEDCS) (pp. 410-415). IEEE.

[6] Wang, Y., Xu, Z., Yao, Y., Liu, J., & Lin, J. (2024). Leveraging Convolutional Neural Network-Transformer Synergy for Predictive Modeling in Risk-Based Applications. arXiv preprint arXiv:2412.18222.

[7] Sun, M., Sun, W., Sun, Y., Liu, S., Jiang, M., & Xu, Z. (2024, October). Applying Hybrid Graph Neural Networks to Strengthen Credit Risk Analysis. In 2024 3rd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE) (pp. 373-377). IEEE.

[8] Feng, P., Li, Y., Qi, Y., Guo, X., & Lin, Z. (2024). Collaborative Optimization in Financial Data Mining Through Deep Learning and ResNeXt. arXiv preprint arXiv:2412.17314.

[9] Long, S., Yi, D., Jiang, M., Liu, M., Huang, G., & Du, J. (2024, September). Adaptive Transaction Sequence Neural Network for Enhanced Money Laundering Detection. In 2024 International Conference on Electronics and Devices, Computational Science (ICEDCS) (pp. 447-451). IEEE.Jiang, M., Liang, Y., Han, S., Ma, K., Chen, Y., & Xu, Z. (2024). Leveraging Generative Adversarial Networks for Addressing Data Imbalance in Financial Market Supervision. arXiv preprint arXiv:2412.15222.

[10] Du, X. (2024). Optimized convolutional neural network for intelligent financial statement anomaly detection. Journal of Computer Technology and Software, 3(9).

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

[12] [13]Jiang, M., Xu, Z., & Lin, Z. (2024). Dynamic Risk Control and Asset Allocation Using Q-Learning in Financial Markets. Transactions on Computational and Scientific Methods, 4(12).

[13] Huang, G., Xu, Z., Lin, Z., Guo, X., & Jiang, M. (2024). Artificial Intelligence-Driven Risk Assessment and Control in Financial Derivatives: Exploring Deep Learning and Ensemble Models. Transactions on Computational and Scientific Methods, 4(12).

[14] B. Chugh, N. Malik, D. Gupta, et al., "A probabilistic approach driven credit card anomaly detection with CBLOF and isolation forest models", Proceedings of the 2025 Alexandria Engineering Journal, vol. 114, pp. 231-242, 2025.

[15] M. Alamri, M. Ykhlef, "Survey of credit card anomaly and fraud detection using sampling techniques", Proceedings of the 2022 Electronics, vol. 11, no. 23, p. 4003, 2022.

[16] M. Ahmed, A. N. Mahmood, M. R. Islam, "A survey of anomaly detection techniques in financial domain", Proceedings of the 2016 Future Generation Computer Systems, vol. 55, pp. 278-288, 2016.