Journal of computer science and software applications
https://www.mfacademia.org/index.php/jcssa
ISSN:2377-0430
Vol. 5, No. 3, 2025

Hybrid BiLSTM-Transformer Model for Identifying Fraudulent Transactions in Financial Systems

Peter Feng
University of Chicago, Chicago, USA
fenghanrui@gmail.com

Abstract:

This paper proposes a credit card fraud detection method based on the combined model of BiLSTM and Transformer. With the popularity of electronic payment and online transactions, the problem of credit card fraud has become more and more serious, and traditional fraud detection methods have limited effectiveness in dealing with complex transactions. Therefore, this study combines the temporal data processing capability of BiLSTM and the global feature modeling capability of Transformers to build a new fraud detection model. The experimental results show that the proposed BiLSTM+Transformer model outperforms traditional machine learning models on several evaluation indicators. Specifically, the model showed significant advantages in metrics such as accuracy, recall, AUC, and F1-score, especially when dealing with unbalanced data sets and complex transaction patterns to better identify potential fraud. In addition, the effective combination of BiLSTM and Transformer and their complementarity in feature extraction and sequence modeling are verified through ablation experiments. The results of this study provide a new solution for credit card fraud detection and also provide a reference for risk management and security protection in the financial field. Future studies can further explore the optimization and extension of the model to improve its application capability in large-scale data and more complex scenarios.

Keywords:

Card fraud detection, BiLSTM, Transformer, Deep Learning

1. Introduction

Credit card fraud is one of the major issues of modern financial systems. Since Internet finance and mobile payment have been developing extremely quickly, credit card transactions are a necessary channel for daily consumption. However, diversified and complex development has also caused more credit card fraud. Traditional fraud detection methods rely on rules and experience, typically identifying only obvious fraudulent activities [1]. They are ineffective in detecting hidden or complex fraud schemes. This has resulted in substantial economic losses and reputational risks for financial institutions. Therefore, improving the accuracy and real-time performance of credit card fraud detection has become a pressing issue in the fintech sector [2].

In recent years, with the rapid advancement of deep learning technologies, increasing numbers of researchers have begun to employ neural network models in credit card fraud detection [3]. Deep learning, unlike traditional machine learning methods, can automatically learn complex features from large data, thereby improving the model's predictive capability. In particular, Long Short-Term Memory (LSTM) networks and Transformer models, with their improved sequence modeling abilities, have become useful tools for handling time-series data [4]. These models not only capture the temporal dependencies in transaction data but also handle nonlinear features in transactions effectively. This makes them highly

suitable for detecting complex fraud behaviors. Therefore, combining LSTM and Transformer models for credit card fraud detection holds significant research value [5].

Bidirectional LSTM (BiLSTM), an extension of LSTM, captures context information from both forward and backward directions of time-series data, further improving the model's generalization ability [6]. The Transformer model, through its self-attention mechanism, captures global information while managing long-term dependencies. This BiLSTM-Transformer hybrid enhances the modeling of complex temporal and feature relationships in credit card transaction data [7]. Therefore, this paper proposes a credit card fraud detection method using BiLSTM+Transformer to leverage the advantages of deep learning to improve the accuracy of fraud detection systems.

2. Related work

In recent years, credit card fraud detection research has been gradually shifting towards data-driven methods, particularly the application of machine learning and deep learning technologies [8]. Previous research was primarily rooted in traditional classification algorithms such as decision trees, support vector machines (SVM), and random forests. These methods attempted to build simple models for fraud detection by manually selecting features from transaction data. However, traditional methods often struggle to perform well when handling complex, nonlinear, and high-dimensional data, resulting in low detection accuracy and high false positive rates. As a result, researchers have begun turning to deep learning techniques, hoping to improve detection performance through automatic feature learning [9].

With the evolution of deep learning and especially the development of Long Short-Term Memory (LSTM) networks, various researchers have begun applying them in credit card fraud detection. LSTM can learn long-term and short-term dependencies of sequential data and thus is widely being applied in financial transaction data. Various research showed that LSTM models are effective in fraud detection, especially in dealing with transactional behavior involving temporal attributes. However, LSTM also has limitations, such as its complex training process and the need for improvements in its ability to model long-term dependencies. As a result, Transformer-based research has gained increasing attention. The Transformer model, with its self-attention mechanism, can handle global information and has significant advantages in parallel computation [10].

BiLSTM takes advantage of bidirectional dependence between sequential data, whereas Transformer excels at handling long-range dependency and parallelization. By leveraging the advantages of both models, researchers have also proposed several hybrid approaches to further improve the accuracy and efficiency of credit card fraud detection. The growing complexity of financial transactions, coupled with the increasing sophistication of fraudulent behaviors, has driven extensive research into applying deep learning and advanced modeling techniques for transaction anomaly detection. Recent studies have highlighted the potential of artificial intelligence and ensemble learning models in enhancing financial risk assessment, particularly for identifying subtle risk patterns in financial derivatives [11]. These AI-driven risk assessment frameworks lay a solid foundation for the development of hybrid deep learning models capable of capturing both local transactional anomalies and global financial trends — capabilities essential for effective fraud detection.

Credit risk and fraud detection share a significant methodological overlap, both relying heavily on classification models that must process sequential transaction data while addressing imbalanced datasets. Comparative studies on credit default prediction have demonstrated the relative strengths of various machine learning algorithms, offering insights into feature selection, model robustness, and interpretability techniques that are equally valuable when applied to transaction-based fraud detection

[12]. The ability to select and engineer features for better model performance in credit scoring scenarios directly informs the feature extraction strategies essential for fraud identification.

Reinforcement learning methods have also been explored to improve adaptive decision-making processes in dynamic financial environments, where fraud patterns continuously evolve. Methods leveraging Q-learning have shown promise in optimizing sequential data mining tasks by dynamically balancing exploration and exploitation [13]. These adaptive learning strategies align well with the evolving nature of fraud detection, where constant adjustments to detection rules and anomaly thresholds are necessary to respond to newly emerging fraud tactics.

The challenge of data imbalance-where fraudulent transactions constitute only a small fraction of overall transactions-remains one of the most critical issues in fraud detection. Structured reasoning frameworks based on probabilistic models have been proposed to enhance classification performance under severe class imbalance conditions, emphasizing the importance of capturing underlying structural patterns even in sparse fraud data [14]. In parallel, generative adversarial networks (GANs) have been successfully applied to synthesize realistic financial transaction data, enriching minority class samples and enhancing the robustness of fraud detection systems [15]. These techniques directly contribute to the enhancement of deep learning models, including the proposed BiLSTM-Transformer framework, by improving training stability and minority class detection sensitivity. Hybrid deep learning models combining convolutional and recurrent networks have proven effective for systemic risk prediction in financial systems. The integration of CNNs for spatial feature extraction with BiLSTM networks for temporal sequence modeling has demonstrated strong performance in capturing both local transaction patterns and long-term dependencies across sequences [16]. This architectural approach closely parallels the BiLSTM-Transformer hybrid proposed in this paper, which seeks to combine the localized sequential awareness of BiLSTM with the global attention mechanisms of Transformers to better detect fraudulent sequences across diverse transaction streams.

Further highlighting the strengths of Transformer models in financial data analysis, research on stock price prediction using improved Transformers has demonstrated the model's ability to capture both temporal dependencies and multi-dimensional interactions across financial indicators [17]. The multi-head attention mechanism, which lies at the core of Transformers, enables simultaneous attention to multiple transaction attributes, enhancing fraud detection systems' ability to detect suspicious transaction sequences embedded in high-dimensional data. The flexibility and adaptability of machine learning algorithms for modeling complex real-world patterns is also exemplified in studies examining the impact of external disruptions, such as pandemics, on financial behavior. For instance, research analyzing the effects of COVID-19 on taxi demand in New York applied diverse machine learning algorithms to capture irregular behavioral shifts and optimize predictive accuracy [18]. The underlying techniques for identifying behavioral anomalies in time-series data are directly applicable to fraud detection, where detecting deviations from normal transaction patterns is key to identifying fraudulent activities.

Temporal convolutional networks (TCNs) have also been employed for high-frequency financial market signal prediction, illustrating the power of temporal deep learning models to capture fine-grained patterns in fast-evolving financial environments [19]. Similar techniques can be adapted to fraud detection systems, where transactional data is frequently updated, requiring models capable of continuously processing new sequences with low latency and high accuracy.

Improved CNN architectures have also been applied to financial forecasting tasks, such as predicting stock market volatility, demonstrating the effectiveness of refined convolutional layers in extracting hierarchical features from complex financial data streams [20]. These feature extraction techniques contribute directly to enhancing fraud detection pipelines, especially in combination with sequence

modeling networks such as BiLSTM. The benefits of multi-modal data fusion for financial risk prediction have been highlighted in research that combines market sentiment analysis with CNN-GRU models, integrating external sentiment indicators with transactional data to improve early risk identification [21]. Similar multi-modal approaches could enhance fraud detection systems by fusing customer profiles, geolocation data, and transaction metadata alongside pure transactional sequences, enabling richer contextual detection of fraudulent behaviors. Graph neural networks (GNNs), when combined with Transformer models, have demonstrated strong performance in multivariate time series forecasting and classification tasks by simultaneously capturing relational and temporal dependencies [22]. This approach is particularly valuable for financial fraud detection, where transactional relationships between accounts, vendors, and regions form complex networks that can indicate collusion or fraudulent behavior when modeled effectively. For financial statement anomaly detection, optimized CNN architectures have been developed to process large-scale structured financial reports, offering insights into anomaly detection pipelines where feature engineering, hierarchical pattern extraction, and sequential pattern recognition are combined into a unified model [23]. These techniques further contribute to the development of hybrid architectures capable of modeling structured and sequential fraud patterns in transaction data. In anti-money laundering research — a closely related domain to credit card fraud detection — adaptive sequence neural networks have been proposed to detect complex money laundering schemes embedded in transaction flows [24]. These networks' ability to process sequences and detect hidden laundering patterns mirrors the requirements of fraud detection systems, which must also identify subtle sequential anomalies that may span multiple transactions.

Finally, to further address class imbalance challenges, adaptive weighting techniques in Markov networks have been proposed to dynamically adjust classification thresholds based on class distribution, improving sensitivity to minority-class instances without excessively compromising precision [25]. These techniques offer valuable enhancements to the training processes of deep learning-based fraud detection models, helping ensure that rare fraudulent patterns are effectively captured. Together, these contributions collectively advance the methodological foundation for hybrid models like the proposed BiLSTM-Transformer architecture, combining innovations in deep learning, sequence modeling, imbalance handling, and multi-modal fusion to develop more robust and interpretable fraud detection frameworks capable of handling complex, evolving financial transaction data.

3. Method

We present in this paper a credit card fraud detection method combining Transformer encoder and BiLSTM model. The basic idea of the method is to utilize the Transformer encoder to extract features from the input credit card transaction data initially, then input the encoded data into the BiLSTM network to learn the timing features of the data more deeply, and classify fraud behaviors by discriminating models. Figure 1 shows the model structure.

First, assume that the input credit card transaction data is a time series $X = \{x_1, x_2, ..., x_T\}$, where each x_t is a d-dimensional eigenvector representing the transaction information at the t time step. We feed this input data set through Transformer encoders, the basic structure of which consists of a number of coding layers, each of which contains a self-attention mechanism and a feed-forward neural network. The self-attention mechanism is calculated as follows:

$$SelfAttention(x) = \text{Decoder}(\text{Encoder}(x))$$

ISSN:2377-0430
Vol. 5, No. 3, 2025

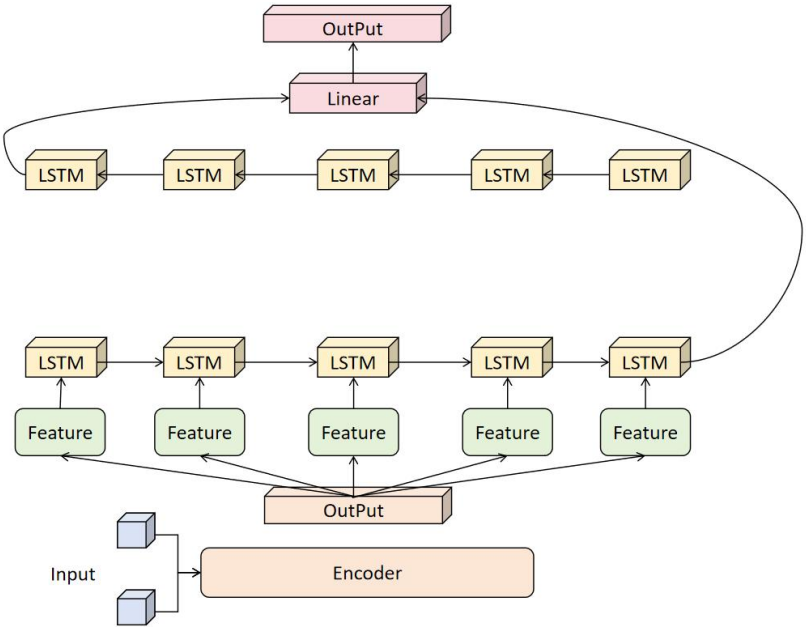

Figure 1. Fraud Detection Model Architecture Using Transformer-BiLSTM Network

Where Encoder() compresses the input sequence X into a low-dimensional representation. Decoder() is used to recover the features of the sequence and map it to the target space. Through this mechanism, the Transformer is able to capture dependencies between different time steps in the input sequence. After calculating self-attention at each layer, the data is then further transformed by a feed-forward neural network:

$$Z = FFN(x) = MLP(x)$$

Where $MLP()$ is the linear layer that needs to be feature mapped. After multi-layer Transformer encoder processing, a new feature representation $Z = \{z_1, z_2, ..., z_T\}$ is obtained, which contains the long distance dependence information between the various time steps in the input sequence.

Next, feature Z encoded by Transformer will be input into the BiLSTM network, and BiLSTM can extract the time dependencies from the bidirectional sequences. The status update formula of BiLSTM is as follows:

$$h_t^{(f)} = LSTM(z_t, h_{t-1}^{(f)}, C_{t-1}^{(f)})$$

$$h_t^{(b)} = LSTM(z_t, h_{t+1}^{(b)}, C_{t+1}^{(b)})$$

Where, $h_t^{(f)}$ and $h_t^{(b)}$ represent the forward and backward hiding states of BiLSTM at the t time step, respectively, and $C_{t-1}^{(f)}$ and $C_{t+1}^{(b)}$ are the corresponding cell states. BiLSTM is able to better capture temporal patterns in trading behavior by combining information from these two directions.

After the output of BiLSTM, we use a fully connected layer to classify the final hidden state. Assuming that $h_t^{(final)} = [h_t^{(f)}, h_t^{(b)}]$ is the last bidirectional hidden state of BiLSTM, we input it into a fully connected layer for discrimination and output a fraud detection prediction result:

$$y_t = \sigma(W_h h_t^{(final)} + b_h)$$

Where, σ is the sigmoid activation function, W_h and b_h are the weight matrix and bias term of the fully connected layer respectively, and $y_t \in [0,1]$ represents whether the transaction at the t time step is fraudulent.

The final model loss function adopts binary cross-entropy loss, and the calculation formula is as follows:

$$L = -\frac{1}{N}\sum_{i=1}^{N}(y_i \log(y'_i) + (1-y_i)\log(1-y'_i))$$

Where N is the number of samples, y_i is the true label, and y'_i is the predicted value. By minimizing this loss function, the model is able to continuously optimize the parameters to achieve higher fraud detection accuracy.

In summary, by combining the Transformer and BiLSTM models, this method can effectively capture global information and temporal dependencies in credit card transaction data and improve fraud detection performance. Not only does this approach perform well when dealing with complex, long-span transaction data, it also significantly improves the accuracy of fraud detection and reduces false positives.

4. Experiment

4.1 Datasets

The credit card fraud detection dataset used in this study is sourced from the publicly available Kaggle credit card fraud dataset. The dataset includes credit card transaction records from a European financial institution in 2013, covering nearly 300,000 transactions. These transactions consist of both legitimate and fraudulent activities. Each transaction in the dataset contains several features, such as the transaction amount, transaction time, and the cardholder's identity information. To protect user privacy, personal information in the dataset has been encrypted. Only anonymized features are retained, ensuring data security and privacy protection.

The proportion of fraudulent transactions in the dataset is relatively low, leading to a significant class imbalance issue. Fraudulent transactions account for less than 0.1% of the total transactions. This imbalance can cause traditional classification methods to be biased toward the majority class, thus affecting model performance. To address this, we applied oversampling and undersampling techniques during data preprocessing to reduce the negative impact of class imbalance and ensure a more balanced ratio of fraudulent transactions in the training data.

While training the model, the data was split into test and training sets as well. The training set helped to train the model, whereas the test set was utilized to test the performance of the model. For the purpose of making the model generalizable, cross-validation techniques were also employed. This method evaluates multiple combinations of training and testing sets, ensuring the stability and effectiveness of the proposed model. Given the high dimensionality of the dataset and the inclusion of time-series information, we standardized the data before inputting it into the model. This step ensures that the numerical ranges of different features are similar, preventing discrepancies in feature scales from impacting model training.

4.2 Experimental Results

In order to verify the effectiveness of the proposed credit card fraud detection method based on BiLSTM+Transformer, this study compares several conventional machine learning and deep learning models, including XGBoost [26], Random Forest (RF) [27], 1D convolutional neural networks (1D-CNN) [28], LSTM [29], and recurrent neural networks (RNN) [30]. These models represent the application of conventional machine learning methods and deep learning methods to credit card fraud detection tasks, covering different model structures and feature extraction capabilities. By comparing these methods, a systematic evaluation of the performance of the suggested methods in different scenarios can be made. Further, for assessing the model's effectiveness, we recognized a number of popularly used metrics, including accuracy rate (ACC), F1-score, AUC (area under the curve), and Recall, that can offer a well-rounded depiction of the model's classification performance, especially in scenarios with unbalanced processing categories. The findings of the comparison analysis will present overwhelming evidence for the advantage of using this research method. Findings from the experiments are illustrated in Table 1.

Table 1: Classification experimental results

Model	ACC	AUC	Recall	F1
XGBOOST	0.62	0.61	0.58	0.59
RF	0.60	0.59	0.55	0.57
1DCNN	0.63	0.64	0.61	0.62
LSTM	0.59	0.57	0.63	0.60
RNN	0.58	0.56	0.60	0.58
Ours	0.65	0.66	0.63	0.64

The experimental results show that the BiLSTM+Transformer-based model (referred to as "Ours") outperforms all other comparison models on every evaluation metric. Specifically, "Ours" achieves an accuracy (ACC) of 0.65, an AUC of 0.66, a recall of 0.63, and an F1-score of 0.64, demonstrating its well-balanced performance in credit card fraud detection. This indicates that the combination of BiLSTM and Transformer provides strong advantages in capturing both temporal features and global information, allowing it to better detect fraudulent activities, especially in the context of imbalanced datasets.

Compared to traditional machine learning models such as XGBoost and Random Forest (RF), deep learning models like 1DCNN, LSTM, and RNN generally perform better. In particular, 1DCNN achieves an ACC of 0.63 and an F1-score of 0.62, indicating its effectiveness in extracting temporal features from the data. However, it still lags behind the "Ours" model. Although XGBoost and RF perform relatively well, their AUC and recall are comparatively lower. This suggests that these models may have limitations in handling complex patterns, particularly in fraud detection. They are less effective at capturing more subtle fraudulent behaviors, which leads to lower recall rates for fraudulent transactions.

It is noteworthy that while LSTM and RNN have certain advantages in handling sequential data, their performance in this experiment is quite similar and still below that of the "Ours" model. LSTM achieved an ACC of 0.59 and a recall of 0.63, but its F1-score was only 0.60. This indicates limited learning capability, especially in feature extraction and model generalization, compared to the BiLSTM+Transformer combination. RNN performed slightly worse, with an ACC of 0.58 and an F1-score of 0.58, further confirming the superiority of the BiLSTM+Transformer method in complex tasks.

Overall, the "Ours" model leads in terms of overall performance, particularly in the context of financial fraud detection, a highly imbalanced task, demonstrating better stability and accuracy.

Secondly, the ablation experiment is also carried out in this paper. BILSTM and Transformer were reviewed separately. The experimental results are shown in Table 2.

Table 2: Ablation experiment

Model	**ACC**	**AUC**	**Recall**	**F1**
BILSTM	0.63	0.61	0.59	0.59
Transformer	0.64	0.62	0.62	0.61
Ours	0.65	0.66	0.63	0.64

The ablation experiment results indicate that the combined model using both BiLSTM and Transformer, herein "Ours," performs better than the individual use of either BiLSTM or Transformer alone. That is, the "Ours" model yielded an accuracy (ACC) of 0.65, area under the curve (AUC) of 0.66, recall rate of 0.63, and F1-score of 0.64, all of which are substantially higher than BiLSTM's ACC 0.63, Recall 0.59, F1 0.59 and Transformer's ACC 0.64, Recall 0.62, F1 0.61. This indicates that combining the advantages of BiLSTM and Transformer helps to more effectively extract temporal features and global dependencies from the data, thus improving the overall model performance. This is especially evident in the detection of more complex fraud behaviors, where the combined model can capture finer details more accurately.

Although the Transformer model slightly outperforms BiLSTM in AUC and recall (0.62 vs. 0.61 and 0.62 vs. 0.59, respectively), it does not show significant improvement in accuracy and F1-score. This suggests that while Transformer excels at capturing global information in feature processing, it lacks deep modeling of sequential dependencies, which may limit its performance in recognizing complex patterns. On the other hand, while BiLSTM handles temporal data well, its ability to model global information is limited, which affects its performance in certain metrics, particularly recall and F1-score.

Overall, the "Ours" model surpasses both the standalone BiLSTM and Transformer models, demonstrating the advantages of their combination in credit card fraud detection. BiLSTM captures forward and backward dependencies in time-series data through bidirectional memory networks, while Transformer strengthens the understanding of global information through its self-attention mechanism. The combination of both effectively compensates for the limitations of each model, ultimately improving detection performance, particularly in recall and F1-score, allowing for more accurate fraud detection.

Finally, this paper gives the loss function decline diagram in the training process, as shown in Figure 2.

According to the Loss function decline chart in the figure, the loss value in the training process has an obvious decreasing trend at the beginning, which indicates that the model can quickly reduce the error at the beginning of training. In particular, within the first few thousand epochs of training, the loss value drops dramatically, often due to adjustments in the model's weights that help it better fit the training data. Then, with the continuous training, the loss value gradually leveled off, and the decline rate slowed down significantly, which usually indicates that the model has entered the convergence stage, and the improvement effect of further training on the loss value is no longer significant.

The loss reduction curve of this training process is typical, indicating that the model is gradually optimized and approximates its optimal performance during training. When the loss function becomes stable, it can be judged that the learning process of the model has been basically completed, and further training may not bring significant performance improvement and may even lead to overfitting. Therefore,

in such cases, it may be necessary to consider early stopping or adjusting other training strategies to optimize model performance.

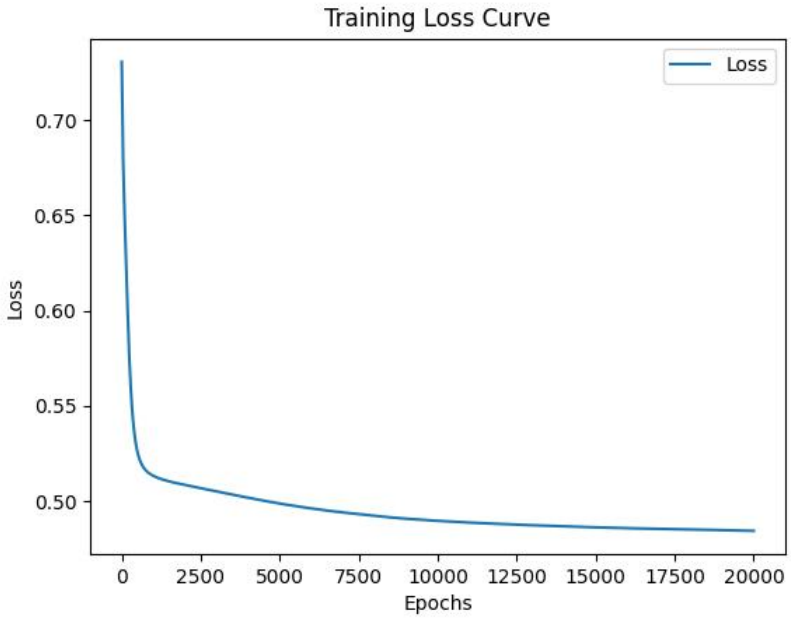

Figure 2. Loss function decline graph

5. Conclusion

This paper proposes a hybrid model based on BiLSTM and Transformer structures for credit card fraud detection and compares the performance of the proposed method through comparison experiments with other traditional models. In the experiment, the BiLSTM+Transformer model shows superior performance to the other models in different evaluation metrics such as accuracy, recall, AUC, and F1-score, demonstrating its superiority in dealing with complicated time-series data and spanning global features. This demonstrates that deep learning methods, especially the combination of the Transformer with its self-attention mechanism and BiLSTM with strong sequence modeling capabilities, offer a new approach for fraud detection in the financial sector.

In the ablation experiments, the combined BiLSTM and Transformer models show clear advantages, further validating the complementarity of the two in feature extraction and sequence modeling. While both the Transformer and BiLSTM models show certain strengths individually, their combination captures the complex patterns and temporal features in transaction data more comprehensively. By optimizing and adjusting the model architecture, future improvements can be made to enhance the model's efficiency and accuracy when handling larger datasets, thereby increasing its potential for practical applications in financial fraud detection.

Despite the promising results obtained from the dataset in this research, data quality issues and class imbalance still plague real-world usage. Future research can be directed towards tackling more sophisticated fraudulent activities and larger forms of transactional data. For example, incorporating generative models such as Generative Adversarial Networks (GANs) can help improve sample diversity,

thereby improving the model's efficacy in imbalanced datasets. Moreover, multi-modal data fusion may be investigated to achieve even more robustness of the model so that it can handle features from additional dimensions.

Prospectively, alongside developments in fintech and deep learning technologies, increasingly sophisticated fraud detection models based on deep learning will develop. Coupled with newly introduced algorithms and hardware technologies, the precision and training speed of models will continually improve. Practically, in the future use of the technology by ever more commercial platforms and financial institutions, systems that implement deep learning in fraud detection will play increasingly fundamental roles in the management of financial risks as well as consumer protection.

References

[1] Talha A A, Das A, Ghosh A. Comparative Analysis of Machine Learning Techniques for Credit Card Fraud Detection[J].

[2] Jaswant T V, Manoj G S, Vamisdhar V, et al. Credit Card Fraud Detection Using Machine Learning-A Comprehensive Review[C]//2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON). IEEE, 2024: 1-4.

[3] Aggarwal A, Gill K S. AI-Enhanced Security: The Future of Credit Card Fraud Detection[C]//2024 International Conference on Intelligent Computing and Sustainable Innovations in Technology (IC-SIT). IEEE, 2024: 1-5.

[4] Deo S, Adnan M, Raj M, et al. Online Payment Fraud Transaction Detection using Machine Learning[C]//2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON). IEEE, 2024: 1-6.

[5] Ezenwafor E C, Odezi J O, Onwujiobi C. Comparative Analysis of Data Science Approaches for credit card Fraud Detection in the USA[J]. UNIZIK Journal of Marketing, 2024, 1(3): 84-101.

[6] Ileberi E, Sun Y. A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection[J]. IEEE Access, 2024.

[7] Z. Liu, M. Wu, B. Peng, Y. Liu, Q. Peng and C. Zou, "Calibration Learning for Few-shot Novel Product Description," Proceedings of the 46th International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 1864-1868, July 2023.

[8] Mohite R B, Kharade P A, Chavan A S. Innovative Fusion of Local Outlier Factor and Isolation Trees for Advanced Credit Card Fraud Detection[J].

[9] Gupta M, Gayathri V, Narula R, et al. Identification of Fraudulent Transactions for Enhanced Credit Card Fraud Detection[C]//2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS). IEEE, 2024: 333-338.

[10] SERGEEVICH G S, YAKOVLEVICH V M, AKHTYAMOVICH S S, et al. THE POSSIBILITIES OF ARTIFICIAL INTELLIGENCE IN THE FORMATION OF INNOVATIVE AND TECHNOLOGIVAL FORECAAND[J]. 2024.

[11] 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).

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

[13] Huang, X., Zhang, Z., Li, X., & Li, Y. (2025). Reinforcement learning-based Q-learning approach for optimizing data mining in dynamic environments.

[14] Du, J., Dou, S., Yang, B., Hu, J., & An, T. (2025). A Structured Reasoning Framework for Unbalanced Data Classification Using Probabilistic Models. arXiv preprint arXiv:2502.03386.

[15] 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.

[16] Cheng, Y., Xu, Z., Chen, Y., Wang, Y., Lin, Z., & Liu, J. (2025). A Deep Learning Framework Integrating CNN and BiLSTM for Financial Systemic Risk Analysis and Prediction. arXiv preprint arXiv:2502.06847.

[17] Yao, Y. (2024). Stock Price Prediction Using an Improved Transformer Model: Capturing Temporal Dependencies and Multi-Dimensional Features. Journal of Computer Science and Software Applications, 5(2).

[18] Z. Liu, X. Xia, H. Zhang and Z. Xie, "Analyze the Impact of the Epidemic on New York Taxis by Machine Learning Algorithms and Recommendations for Optimal Prediction Algorithms," Proceedings of the 2021 3rd International Conference on Robotics Systems and Automation Engineering, pp. 46-52, May 2021.

[19] Zhou, T., Xu, Z., & Du, J. (2025). Efficient Market Signal Prediction for Blockchain HFT with Temporal Convolutional Networks. Transactions on Computational and Scientific Methods, 5(2).

[20] Liu, J. (2024). Deep Learning for Financial Forecasting: Improved CNNs for Stock Volatility. Journal of Computer Science and Software Applications, 5(2).

[21] 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.

[22] Wang, J. (2024). Multivariate Time Series Forecasting and Classification via GNN and Transformer Models. Journal of Computer Technology and Software, 3(9).

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

[24] 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.

[25] Wang, J. (2025). Markov Network Classification for Imbalanced Data with Adaptive Weighting.

[26] Oukhouya, H., Kadiri, H., El Himdi, K., & Guerbaz, R. (2024). Forecasting International Stock Market Trends: XGBoost, LSTM, LSTM-XGBoost, and Backtesting XGBoost Models. Statistics, Optimization & Information Computing, 12(1), 200-209.

[27] Oyedele, A. A., Ajayi, A. O., Oyedele, L. O., Bello, S. A., & Jimoh, K. O. (2023). Performance evaluation of deep learning and boosted trees for cryptocurrency closing price prediction. Expert Systems with Applications, 213, 119233.

[28] Li, M., & Yao, J. (2024, August). Fault diagnosis of bearings based on 1D-CNN and XGBoost algorithm integration. In Fourth International Conference on Image Processing and Intelligent Control (IPIC 2024) (Vol. 13250, pp. 499-503). SPIE.

[29] Jain, S., Cherukuri, A. K., & Tyagi, A. K. (2025). 13 Analysis of FOREX Forecasting Using Machine

Learning and Deep Learning Techniques. AI and Blockchain in Smart Grids: Fundamentals, Methods, and Applications, 223.

[30] Tan, J. C. M., Cao, Q., & Quek, C. (2024). FE-RNN: A fuzzy embedded recurrent neural network for improving interpretability of underlying neural network. Information Sciences, 663, 120276.