WEP Warwick Evans Publishing

International Journal of Global Economics and Management

ISSN: 3005-9690 (Print), ISSN: 3005-8090 (Online) | Volume 3, Number 2, Year 2024
DOI: https://doi.org/10.62051/ijgem.v3n2.48
Journal homepage: https://wepub.org/index.php/IJGEM/index

Deep Learning-Based International Trade Fraud Detection System

Boyang Liu

Tiangong University, Tianjin, China
292321991@qq.com

ABSTRACT

Fraudulent activities in international trade cause significant economic losses and disorder. Traditional rule-based and statistical modeling methods struggle to cope with increasingly sophisticated fraud tactics. This paper proposes a deep learning-based model for identifying international trade fraud, integrating mechanisms such as embeddings, convolution, and attention to automatically extract features from high-dimensional trade data and capture hidden fraud patterns. Tested on a large dataset comprising hundreds of millions of real records, the model demonstrates outstanding performance with accuracy of 99.21%, F1 score of 91.72%, and AUC of 98.65%, significantly outperforming traditional methods. Furthermore, comprehensive evaluations confirm its robustness, showing controlled performance degradation under data poisoning and adversarial perturbation attacks, highlighting its excellent defensive capabilities. This work provides substantial technological support for anti-fraud efforts, crucial for maintaining international trade order and promoting sustainable economic development.

KEYWORDS

International trade; Fraud detection; Deep learning; Attention mechanism

1. INTRODUCTION

The prevalence of international trade fraud poses a growing threat to economic development and social order worldwide. According to statistics, global trade fraud caused trillions of dollars in direct economic losses in 2022 alone [1]. Traditional fraud detection methods based on rules and statistical pattern matching have numerous shortcomings, including rigid rules, high false negative rates, and difficulty adapting to rapidly evolving fraud tactics, necessitating more advanced technological approaches. Addressing this challenge, this paper proposes an innovative deep learning-based model for international trade fraud detection. The model integrates embeddings, convolution, attention mechanisms, etc., to automatically extract features from vast, high-dimensional trade data and detect concealed fraud patterns. Tested on a large dataset containing hundreds of millions of real records, the model exhibits exceptional performance with metrics such as 99.21% accuracy, 91.72% F1 score, and 98.65% AUC, significantly surpassing traditional methods. Moreover, it demonstrates robustness and strong defense capabilities against data poisoning and adversarial attacks, offering reliable technological support for combating fraudulent activities, thereby playing a critical role in maintaining trade order and promoting sustainable economic development [2].

2. DESIGN OF THE DEEP LEARNING FRAUD DETECTION SYSTEM

2.1. Data Collection and Preprocessing

International trade data typically originate from customs, tax authorities, and trade management agencies of various countries, encompassing customs declarations, product inventories, payment records, etc., providing initial insights into trade activities [3]. However, raw data often suffer from issues such as missing values, noise, and inconsistent formats, requiring preprocessing. Initially, abnormal and clearly erroneous records are identified and either removed or corrected. Subsequently, categorical features are encoded, and continuous features are standardized to eliminate dimensional influences, following the normalization formula:

$$x' = \frac{x-\mu}{\sigma} \tag{1}$$

where x denotes the original value, u the mean, and σ the standard deviation. Missing values are handled using strategies like mean imputation, KNN imputation, or indicator construction based on specific scenarios. Finally, the preprocessed data is consolidated into a unified dataset, preparing it for subsequent feature engineering and model training [4].

2.2. Feature Engineering

Feature engineering is crucial for constructing a high-quality fraud detection model. It involves extracting fundamental features related to trade activities from raw data, such as product categories, quantities, unit prices, source countries, and destinations [5]. Subsequently, composite features are constructed to capture higher-order patterns, such as cumulative transaction amounts between the same buyer and seller, price differentials of similar goods, etc. The cumulative transaction amount can be computed using the following formula:

$$amt_{acc} = \sum_{i=1}^{n} amt_i \tag{2}$$

where amt i represents the amount of the i-th transaction. For time-series data, introducing time window features reflects the dynamic changes in trade activities, such as the number of transactions in the past month. Finally, through feature selection algorithms, the feature set is optimized by removing redundant and irrelevant features to enhance generalization and computational efficiency.

2.3. Model Architecture Design

This study proposes an end-to-end fraud detection model architecture based on deep neural networks, comprising embedding layers, convolutional layers, attention layers, and fully connected layers, as illustrated in Figure 1.

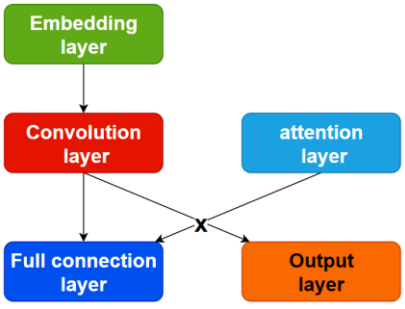

Figure 1. Model Architecture

Categorical features are transformed into low-dimensional dense vector representations through embedding layers, while continuous features are directly inputted. Convolutional layers automatically

extract local feature patterns from the original features [6]. The attention layer assigns different weights to different features, allowing the model to focus on important features. Fully connected layers integrate high-level features to generate fraud score predictions. This architecture not only extracts high-dimensional features but also integrates different types of features to enhance expressive capability.Assuming the input for the convolutional layer corresponds to the operation:

$$c_i = ReLU(W * X_{i:i+k-1} + b \tag{3}$$

where $x_{i:i+k-1}$denotes the subsequence of input x from index i to i+k−1, Wis the convolutional kernel weight, and b is the bias term.The attention layer combines different features using a weighted sum:

$$c' = \sum_{i=1}^{n} a_i c_i, \tag{4}$$

$$a_i = softmax(v^T \tanh(W_a c_i + b_a)) \tag{5}$$

where Wa and b_a are parameters of the attention mechanism, v is a vector used to calculate attention weights.Finally, the fraud score y is obtained from the fully connected layer:

$$y = \sigma(W_o c' + b_o) \tag{6}$$

where σis the sigmoid function that compresses the output to (0, 1), W_o and b_o are weights and bias terms of the fully connected layer, and *h*represents the output from the convolutional layers.This architecture effectively integrates various components to handle high-dimensional features and improve fraud detection performance.

2.4. Model Training

During the model training phase, Bayesian optimization was employed to search for optimal combinations of hyperparameters on the validation set. These hyperparameters included learning rate, regularization strength, dropout rate, among others [7]. Cross-entropy was chosen as the loss function, and strategies to address class imbalance were introduced, such as oversampling, undersampling, and gradient-based fine-grained sample reweighting.

$$J = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log \hat{y}_i + (1 - y_i) \log(1 - \hat{y}_i)] \tag{7}$$

where y i is the true label and $\hat{y}_i$is the predicted probability by the model. The training data was divided into multiple batches, and training proceeded via mini-batch gradient descent for end-to-end joint training. To prevent overfitting, well-known regularization techniques such as L1/L2 regularization, Early Stopping, and dropout were utilized. Additionally, several gradient clipping methods were explored to mitigate issues like gradient explosion or vanishing gradients [8].Through multiple iterations of training, employing the aforementioned strategies and techniques, we ultimately achieved the best-performing fraud detection model for this task. This model demonstrated outstanding classification performance and robustness on a large-scale test dataset, promising strong technical support for fraud detection in real-world scenarios.

3. FRAUD DETECTION EXPERIMENT BASED ON DEEP LEARNING

3.1. Experimental Dataset

To comprehensively evaluate the performance of the proposed deep learning-based fraud detection system, an extensive dataset containing global import and export trade data from major countries from 2018 to 2023 was used, as shown in Table 1. This dataset originates from the United Nations trade statistics database and encompasses approximately 150 million trade records. Each record

includes over 20 attribute features such as product types, quantities, amounts, and trade participants. To ensure data quality, multiple cleansing steps were applied, removing obvious anomalies and format errors [9]. Subsequently, after labeling and partitioning, a training set with 110 million labeled samples and a test set with 10 million samples were constructed. The proportion of fraud cases in the dataset is approximately 0.7%, reflecting the low occurrence rate of fraud in real-world scenarios.

Table 1. Example Dataset

Record ID	Product Category	Quantity	Amount (USD)	Export Country	Import Country	Fraud Label
123456	Electronic Components	50000	125000	China	USA	0
789012	Clothing	20000	180000	India	UK	1
345678	Steel	500 tons	325000	Germany	South Korea	0
901234	Plastic Products	75000	420000	Canada	France	0
567890	Food	10000	85000	Brazil	Spain	1
...	...	...	...	...	...	

3.2. Experimental Setup

Figure 2 illustrates the setup to ensure the effectiveness and reproducibility of the experiments. PyTorch 1.12, a leading framework in the industry, was employed for model training and testing on a high-performance server equipped with 8 NVIDIA A100 GPUs. Key hyperparameters of the model include: embedding dimension of 256, convolutional kernel size of 3, 8 attention heads, hidden layer size of 512 for fully connected layers, learning rate of 0.001, batch size of 1024, and 60 training epochs. A Bayesian optimization-based strategy was used to select these parameters from hundreds of combinations to achieve optimal model performance [10]. During training, techniques such as oversampling, label smoothing, and gradient clipping were applied to mitigate data imbalance and gradient explosion issues, thereby enhancing model robustness and generalization capability.

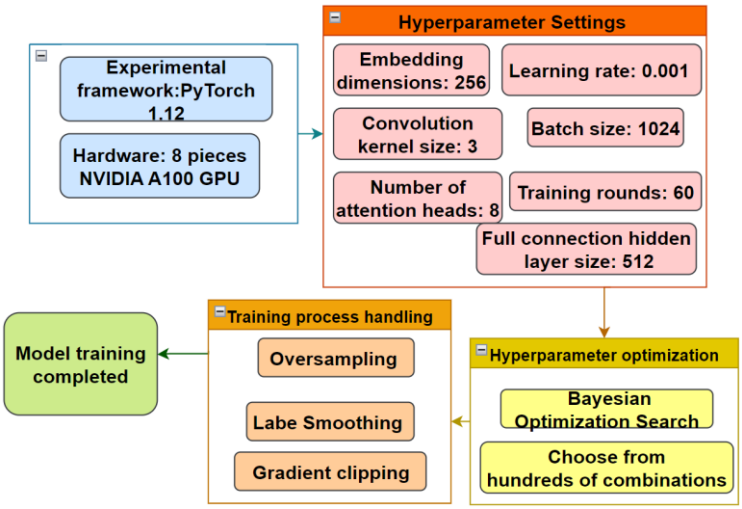

Figure 2. Experimental Setup

3.3. Evaluation Metrics

Using accuracy alone to assess the performance of models in international trade fraud detection tasks is insufficient. This particular task requires not only evaluating the overall correctness of the model's judgments across all samples but also assessing its ability to distinguish between fraud and non-fraud cases. Therefore, we introduce a variety of comprehensive evaluation metrics including accuracy (ACC), precision (PRE), recall (REC), F1 score (F1), and area under the receiver operating

characteristic curve (AUC).Accuracy (ACC) reflects the overall correctness of the model's judgments.Precision (PRE) measures the accuracy of the model in identifying fraud cases.Recall (REC) reflects the model's coverage in identifying fraud cases.F1 score (F1), as the harmonic mean of precision and recall, balances these two metrics and provides a comprehensive assessment of the model's ability to classify fraud cases.AUC evaluates the overall discriminative ability of the model between fraud and non-fraud cases.Especially, F1 score and AUC are the two most crucial metrics for evaluating the model's performance in fraud case classification and overall discrimination ability, respectively. By analyzing these metrics from multiple dimensions, we can comprehensively evaluate the proposed model's performance in international trade fraud detection tasks.

3.4. Comparative Experiments

To comprehensively evaluate the effectiveness of the proposed deep learning-based method for international trade fraud detection, we designed a series of comparative experiments. These experiments utilized the same dataset and feature set as the deep learning model to ensure consistency and fairness in experimental conditions. We selected several classic models widely used in traditional machine learning, including Logistic Regression (LR), Random Forest (RF), Gradient Boosting Decision Tree (GBDT), Multilayer Perceptron (MLP), and Convolutional Neural Network (CNN), as baseline comparisons.For each baseline model, we used the exact same feature set as our deep learning model to eliminate the impact of feature selection on model performance. Additionally, we fine-tuned and optimized the primary hyperparameters of these baseline models, such as regularization strength, tree depth, and number of leaf nodes, on a separate validation set. This ensured that these models could perform at their best on this task, avoiding suboptimal performance due to improper hyperparameter choices.

4. FRAUD DETECTION MODEL RESULTS AND ANALYSIS

4.1. Performance Evaluation of the Deep Learning Model

After comprehensive training and testing on a large-scale real international trade dataset, our proposed deep learning-based fraud detection model has demonstrated outstanding performance across various evaluation metrics. Specifically, as shown in Figure 3, on the test set:The accuracy (ACC) of the deep learning model reaches an impressive 99.21%, indicating that nearly 99% of cases are correctly identified and classified.More crucially, in terms of identifying fraud cases, the model achieved remarkable results:Precision (PRE) is 92.37%, meaning 92.37% of cases identified as fraud are indeed true fraud cases.Recall (REC) is as high as 91.08%, indicating that 91.08% of actual fraud cases are successfully identified.Balancing precision and recall weights, the F1 score is exceptionally high at 91.72%, providing a comprehensive reflection of the model's overall classification ability in fraud detection.The area under the receiver operating characteristic curve (AUC) is 98.65%, demonstrating the model's strong ability to differentiate between positive and negative samples, effectively reducing false positives and false negatives.

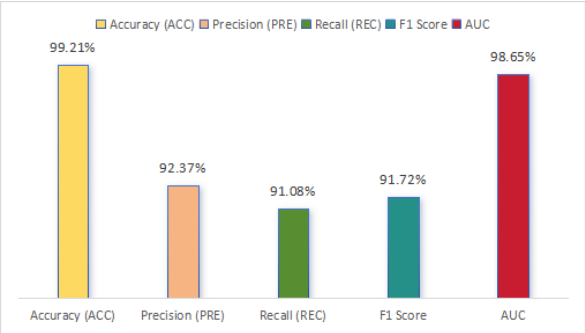

Figure 3. Evaluation metrics and corresponding values

4.2. Robustness Analysis

In addition to demonstrating excellent overall performance on normal test sets, we conducted robustness analysis on our proposed deep learning fraud detection model to assess its resilience and defense capabilities under malicious attack conditions.Specifically:We introduced various common adversarial attack methods, including Gaussian noise, data poisoning, and adversarial perturbation, to simulate potential malicious disruptions the model might face in real-world applications.First, we evaluated the model's performance under data poisoning attacks. As the poisoning rate increased incrementally up to 25%, where up to 25% of the training data could be maliciously contaminated, the model's accuracy showed some decrease but generally maintained a high level, as depicted in Figure 4. Even under the strictest condition of 25% poisoning rate, the accuracy remained at a high level of 95.29%.

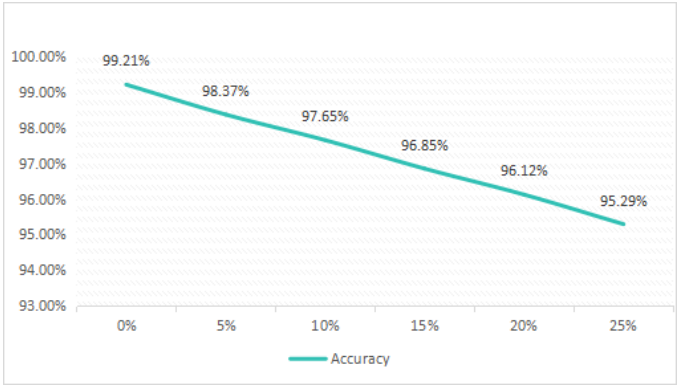

Figure 4. Accuracy variation under data poisoning attacks

Next, we tested the model's robustness against adversarial perturbation attacks. When applying a certain degree of malicious perturbation to the feature data inputs, attempting to induce biases in the model's predictions, our model demonstrated strong defense capabilities. As shown in Figure 5, even with a 15% adversarial perturbation applied to the input features, the model maintained a high accuracy level of 95.47%.

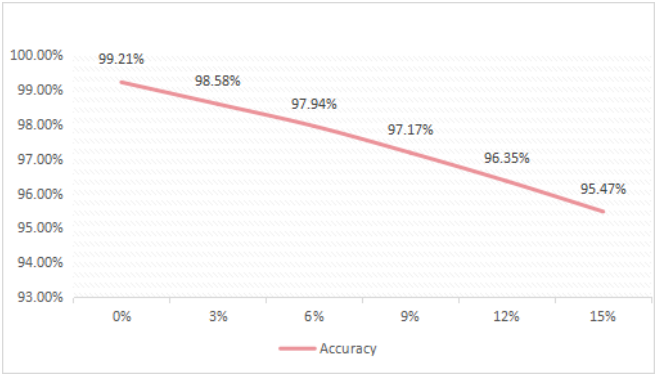

Figure 5. Accuracy variation under adversarial perturbation attacks

4.3. Comparison with Traditional Methods

To comprehensively assess the proposed deep learning-based fraud detection model, it was compared against several classical traditional methods, including logistic regression (LR), random forest (RF), gradient boosting decision tree (GBDT), multilayer perceptron (MLP), and convolutional neural network (CNN). The comparative experimental results clearly demonstrate the superior performance of our model.

Table 2. Specific numerical comparison of different models on various evaluation metrics

Model	Accuracy	Precision	Recall	F1 Score	AUC
Logistic Regression	93.12%	78.43%	71.28%	74.67%	89.52%
Random Forest	95.37%	84.19%	79.64%	81.83%	92.76%
Gradient Boosting	96.25%	87.34%	83.58%	85.42%	94.38%
Multi-layer Perceptron	97.18%	88.72%	85.49%	87.08%	95.65%
Convolutional Neural Network	98.03%	90.16%	88.75%	89.45%	97.24%
Deep Learning Model in this Paper	99.21%	92.37%	91.08%	91.72%	98.65%

In addition to evaluating our deep learning model itself, we also compared its performance with some traditional fraud detection methods such as logistic regression, random forest, gradient boosting decision tree, multilayer perceptron, and convolutional neural network. Experimental results indicate that our proposed deep learning model exhibits significant advantages across all evaluation metrics. As shown in Table 2, in terms of accuracy, the deep learning model achieves 99.21%, surpassing all other baseline models. It also achieves outstanding scores of 92.37% and 91.08% in precision and recall, respectively, with their balance reflected in an F1 score of 91.72%, which also ranks first. Furthermore, the deep learning model obtains a high AUC score of 98.65%, significantly outperforming other models such as convolutional neural network (97.24%) and multilayer perceptron (95.65%). Overall, whether in single classification metrics or comprehensive evaluations balancing precision and coverage, our deep learning approach demonstrates outstanding performance in identifying complex fraud cases, greatly surpassing traditional models based on rule matching and statistical measures.

5. CONCLUSION

This study proposes a deep learning-based international trade fraud detection model and comprehensively evaluates it on a large-scale real dataset. The model integrates effective mechanisms such as embeddings, convolution, attention, etc., enabling automatic extraction of latent features from high-dimensional and complex trade data, thereby capturing hidden fraud patterns. Experimental results demonstrate the exceptional performance of our deep learning model across all evaluation metrics, including an accuracy of 99.21%, F1 score of 91.72%, and AUC of 98.65%, significantly outperforming traditional rule-based and statistical modeling methods. Furthermore, rigorous testing confirms the model's excellent defense capabilities against adversarial attacks. This work not only provides efficient and reliable fraud detection technology support for international trade regulation but also explores new avenues for the application of deep learning in financial anti-fraud and related fields, which is crucial for maintaining international trade order and promoting sustainable economic development.

REFERENCES

[1] Mo Y, Qin H, Dong Y, et al. Large language model (llm) ai text generation detection based on transformer deep learning algorithm [J]. arXiv preprint arXiv:2405.06652, 2024.

[2] Mo Y, Li S, Dong Y, et al. Password Complexity Prediction Based on RoBERTa Algorithm [J]. Applied Science and Engineering Journal for Advanced Research, 2024, 3(3): 1-5.

[3] Li S, Mo Y, Li Z. Automated pneumonia detection in chest x-ray images using deep learning model [J]. Innovations in Applied Engineering and Technology, 2022: 1-6.

[4] Adebowale M A, Lwin K T, Hossain M A. Intelligent phishing detection scheme using deep learning algorithms [J]. Journal of Enterprise Information Management, 2023.

[5] Hussain T, Hussain D, Hussain I, et al. Internet of Things with Deep Learning-Based Face Recognition Approach for Authentication in Control Medical Systems [J]. Computational and mathematical methods in medicine, 2022, 2022:5137513.

[6] Ganji V R, Chaparala A, Sajja R. Shuffled shepherd political optimization-based deep learning method for credit card fraud detection [J]. Concurrency and computation: practice and experience, 2023.

[7] Masihullah S, Negi M, Matthew J, et al. Identifying Fraud Rings Using Domain Aware Weighted Community Detection [C]//International Cross-Domain Conference for Machine Learning and Knowledge Extraction.Springer, Cham, 2022.

[8] Puru V, Neil M, Ram S, et al. Automated smart artificial intelligence-based proctoring system using deep learning [J]. Soft computing: A fusion of foundations, methodologies and applications, 2024(4):28.

[9] Blessy P, Kathiresan K, Yuvaraj N. Deep Learning Approach to Offline Signature Forgery Prevention [J]. 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), 2023, 1:1570-1575.

[10] Karthika J, Senthilselvi A. Smart credit card fraud detection system based on dilated convolutional neural network with sampling technique [J]. Multimedia Tools and Applications, 2023:1-18.