Finance Research Letters 58 (2023) 104547

Contents lists available at ScienceDirect

Finance Research Letters

journal homepage: www.elsevier.com/locate/frl

A distributed deep neural network model for credit card fraud detection

Yu-Tian Lei [a,c], Chao-Qun Ma [a,c,d], Yi-Shuai Ren [b,c,d,e,*], Xun-Qi Chen [a,c], Seema Narayan [f], Anh Ngoc Quang Huynh [g]

[a] *Business School, Hunan University, China*
[b] *School of Public Administration, Hunan University, China*
[c] *Research Institute of Digital Society and Blockchain, Hunan University, China*
[d] *Centre for Resource and Environmental Management, Hunan University, China*
[e] *The Energy Centre, University of Auckland, 12 Grafton Rd, Auckland, 1010, New Zealand*
[f] *Monash Business School, Monash University, Melbourne, Australia*
[g] *College of Technology and Design, University of Economics Ho Chi Minh City (UEH University), Ho Chi Minh City, Vietnam*

ARTICLE INFO

Keywords:
Credit card fraud
Fraud detection
Deep neural network model
Distributed model

ABSTRACT

This paper develops a distributed neural network model (DDNN) for detecting credit card fraud to federate credit card transaction data among different financial institutions. In addition, the convergence of the DDNN model is achieved by introducing a model optimization algorithm. The results demonstrate that (1) The use of a distributed model can avoid privacy leakage and data handling costs; (2) The DDNN model accelerates the convergence of the model through simultaneous computation of multiple clients; (3) The DDNN model detects credit card fraud better than multiple types of centralized models.

1. Introduction

In the context of the rapid development of the consumer finance market, the traditional consumer finance field based on the credit card business has become one of the expansion directions for banks, and how to detect credit card fraud risks effectively has become a hot topic for regulators and academics (Carcillo et al., 2021; Zhang et al., 2021). As one of the most emblematic types of financial fraud, credit card fraud has a larger risk component and a higher level of concealment, and it can easily result in enormous economic losses (Zhu et al., 2021). In recent years, credit card fraud risk has been a big concern for commercial banks (Repousis et al., 2019). Although the magnetic stripe on credit cards promotes quick transactions, they are vulnerable to fraud (Karpoff et al., 2021). In the meantime, the expansion of online payment options is fueling the rise in credit card fraud (Forough et al., 2021). According to credit card fraud data, credit card issuers, retailers, and consumers lost a combined $32.34 billion to credit card fraud in 2021, and authorities are not even tackling 1% of the daily frauds[1]. Detecting credit card fraud has a growing effect on financial institutions' service quality, costs, and reputation (Lin et al., 2021). Therefore, an effective model for detecting credit card fraud is essential for regulators, banks, and customers.

Checking "in advance" and detecting credit card fraud are crucial to minimizing customer risk and reducing credit card fraud from a

* Corresponding author at: School of Public Administration, Hunan University, China.
E-mail address: yishuai_hnu@hnu.edu.cn (Y.-S. Ren).

[1] https://moneytransfers.com/news/2022/09/21/credit-card-fraud-statistics

https://doi.org/10.1016/j.frl.2023.104547
Received 20 July 2023; Received in revised form 24 August 2023; Accepted 30 September 2023
Available online 2 October 2023

risk prevention perspective (Dal et al., 2014). Fraud detection is analyzing historical data to determine whether a transaction is fraudulent[2] (Carcillo et al., 2021). In recent years, machine learning models such as Logistic Regression (LR), Decision Tree (DT), and Support Vector Machine (SVM), as well as models that combine these classifiers, have been widely applied to the identification of credit card fraud (Bhattacharyya et al., 2011; Bahnsen et al., 2016; Carneiro et al., 2017). However, credit card fraud detection based on deep learning technology can not only increase the accuracy and effectiveness of anti-fraud efforts, but it is also a critical technology for intelligence, accuracy, and effectiveness (Pumsirirat et al., 2018; Fiore et al., 2019). Consequently, deep learning models can be utilized more effectively for credit card fraud detection (Kim et al., 2019).

Sadly, existing studies mainly focus on centralized deep learning and can only train models locally by utilizing datasets (Pumsirirat et al., 2018; Kim et al., 2019; Fiore et al., 2019; Benchaji et al., 2021; Forough et al., 2021). Before training a deep learning model with data from several sources, it is often necessary to aggregate the data into a single set (Côté-Allard et al., 2019). In this procedure, the original data must be transported and stored, and the associated cost increases exponentially with the volume of the data. It may lead to data privacy leakage after the data has left the supplier (Fu. et al., 2019). Therefore, many data owners are unwilling to exchange pertinent data, forming "data silos". In contrast, distributed deep learning addresses the challenges of data handling cost and privacy leaks in centralized training models by changing the model construction method. In addition, distributed deep learning models permit several clients to train the models simultaneously using parallel computing, accelerating model convergence.

Therefore, we propose a distributed deep neural network (DDNN) model to detect credit card fraud. The model utilizes credit card transaction data from numerous financial institutions or companies through a distributed network, enabling the sharing of data value without the original data leaving the company. In addition, we offer an algorithm for solving the DDNN model that enables gradual convergence by continuously aggregating parameters globally and uniformly updating client-side model parameters. In detecting credit card fraud, the results demonstrate that DDNN optimizes the model faster than CDNN and beats CDNN and several centrally built machine-learning models.

The paper's contributions are: (1) This study proposes a DDNN model for detecting credit card fraud through a distributed structure; (2) A distributed model optimization algorithm is developed, and optimal convergence of the DDNN model is achieved in our study; (3) The DDNN model is trained and evaluated using real credit card transaction data, and experimental results indicate that the DDNN model outperforms the CDNN model and other machine learning models in terms of detection performance.

2. Distributed deep neural network model

2.1. Model structure

The DDNN model leverages credit card fraud data from multiple financial institutions or companies via a distributed structure, providing a technology path for synergistic collaboration across multiple organizational levels. As shown in Fig. 1, the DDNN model employs a client/server computing structure with numerous local clients and a central service. Each enterprise involved in developing a fraud detection model has a client that utilizes their credit card transaction data to independently train a local model. The central server aggregates the parameters of all local models and uses them to update the global model's parameters, which are subsequently relayed back to the clients.

The global and local models are identical, a deep neural network (DNN) with several layers of neurons. The DNN model is comprised of both linear and nonlinear computations for the activation function. The DNN model is capable of processing complex financial transaction data by merging a large number of neurons. As shown in Fig. 2, the typical DNN model consists of an input layer, a hidden layer, and an output layer.

1) **Input layer:** The data enters the model in the input layer. The input data for credit card transactions comprises multidimensional feature vectors with real-world meaning for each characteristic.
2) **Hidden layer:** The hidden layer consists of multiple layers of neurons, where the i-th neuron of the l-th layer is calculated as follows:

$$z_i^l = \sum_{j=1}^{m} w_{ij}^l x_j + b_i^l \tag{1}$$

where w_{ij}^l denotes the weight parameter of the connection of the i-th neuron of the l-th layer to the j-th neuron of the previous layer and b_i^l denotes the bias parameter of that neuron. Then x_j denotes the output of the j-th neuron in the previous layer, and m denotes the number of neurons in the previous layer. After linear computation, the activation function is then used to obtain the final result. The hidden layer uses the ReLU as the activation function[3].

[2] Specifically, a relevant detection model is built on payment data containing both fraudulent and non-fraudulent credit card transactions, and then the current transaction is passed into the model to determine whether it is a fraudulent transaction.

[3] It is worth noting that the use of nonlinear activation functions here increases the learning capability of the DNN model, enabling it to effectively identify fraudulent transactions in complex credit card transaction data.

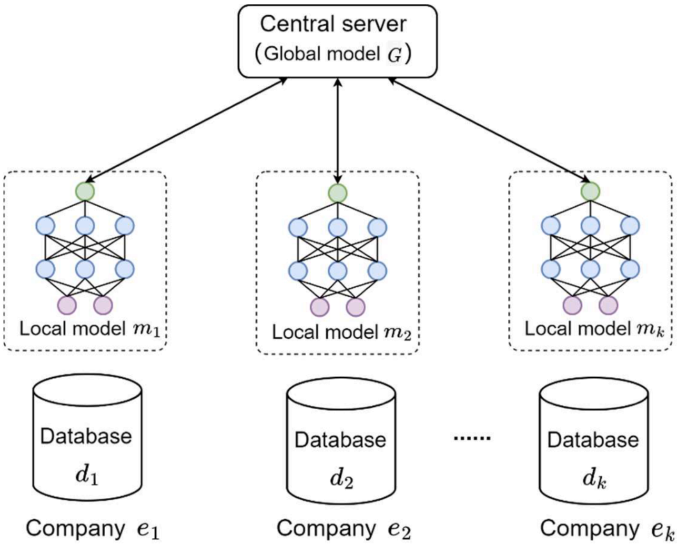


Fig. 1. Distributed deep learning model structure.

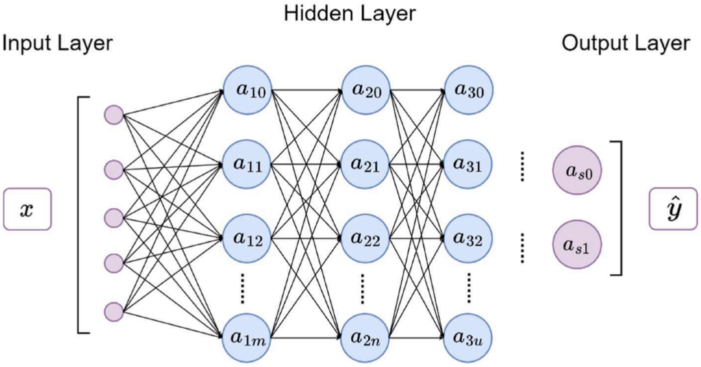


Fig. 2. Deep neural network model structure.

1) **Output layer:** The output layer provides the model's computed results. Considering the nature of credit card fraud detection as a binary classification problem, the output layer consists of only one neuron. Therefore, the Sigmoid function is used as the activation function to normalize the computed results. The Sigmoid function finally maps the output values to between 0 and 1, representing the corresponding predicted classification. Note that 0 is used here to represent normal transactions and 1 for fraudulent transactions.

2.2. Model optimization method

To quantify the difference between predicted and true values, the local DNN model uses the cross-entropy of predicted and true values as the loss function with the following objective function:

$$J(w,b) = \frac{1}{m}\sum_{i=1}^{m} L(\widehat{y}_i, y_i) = -\frac{1}{m}\sum_{i=1}^{m}[y_i \log(\widehat{y}_i) + (1-y_i)\log(1-\widehat{y}_i)] \tag{2}$$

where w and b are the parameters of the neural network. y_i denotes the label of the i-th transaction data in this batch data, and $\widehat{y}_i$ denotes the predicted value of this transaction data. And m denotes the size of the data volume in a batch. Due to the massive amount of data associated with credit card transactions, minibatch is used to train the DNN model.

To achieve the solution of the objective function, the DNN model uses minibatch gradient descent of momentum to update the parameters w and b as follows:

$$\begin{aligned} v_{t+1} &= \mu * v_t + (1-\mu) g_{t+1} \\ w_{t+1} &= w_t - \eta * v^w_{t+1} \\ b_{t+1} &= b_t - \eta * v^b_{t+1} \end{aligned} \tag{3}$$

where g_{t+1} denotes the gradient of parameters *w* and *b* calculated at time $t+1$. μand η denote the momentum coefficient and learning rate, respectively, both constants set in advance. Since each layer of the model involves different calculations, the gradients of the parameters need to be calculated separately by the chain derivative rule.

2.3. Global model parameters optimization

The most important aspect of DDNN models is the optimization of the global model's parameters. Each client uploads local model parameters to the central server, and the server then combines these parameters to update global model parameters. Since the Federated Averaging (FedAvg) aggregating algorithm is robust to imbalanced datasets and non-independently identically distributed datasets, it is suitable for use in various applications (McMahan et al., 2017). Therefore, for the imbalanced credit card transaction dataset, we utilize the FedAvg aggregation algorithm with the following parameter aggregation formula to obtain iterative parameter updates of the global model:

$$G_{t+1} = G_t + \frac{n_k}{n} \sum_{k=1}^{C} \left(L^k_{t+1} - G^k_{t+1} \right) \tag{4}$$

where n_k denotes the number of datasets owned by client *k*, while *n* denotes the number of datasets used by the global model. *L* denotes the parameters *w* and *b* of the local model, while *G* denotes the parameters *w* and *b* of the global model.

As shown in Fig. 3, *Algorithm 1* describes the optimization process of the entire DDNN model. Where *C* denotes the number of company clients, and Epoch denotes the number of times the model is trained using the entire data. The accuracy of the model to detect fraud is evaluated using the test set data at each global update. DDNN model can leverage credit card transaction data from multiple financial companies. Each company's client trains the model several times using the local dataset. Then, the central server aggregates the parameters and updates the parameters of the global model. The server then distributes the updated global model parameters to each client and replaces the local model parameters. This procedure will continue until the convergence of the global model.

3. Dataset

3.1. Data preprocessing

We employ the dataset[4] recording real European credit card transactions to train and validate the proposed DDNN model, which is frequently utilized in credit card fraud detection research (Benchaji et al., 2021; Forough et al., 2021; Li et al., 2021; Esenogho et al., 2022). This dataset contains 284,807 transactions, of which 492 records are fraudulent transactions. Most of the features in this dataset have been specially processed to protect the privacy of credit card users[5]. To accelerate the convergence of the model optimization procedure and enhance the training efficiency, the data are normalized using the following equation:

$$z = \frac{x-\mu}{\sigma} \tag{5}$$

whereμ and σ denote the mean and standard deviation of the data, respectively.

3.2. Dataset split

During training, this study divides the credit card transaction dataset into the training set and the test set to generate a credit card fraud detection model with fewer generalization errors. The training set are used to train the detection model, while the test set are used to evaluate the model's generalization capabilities after finishing training[6].

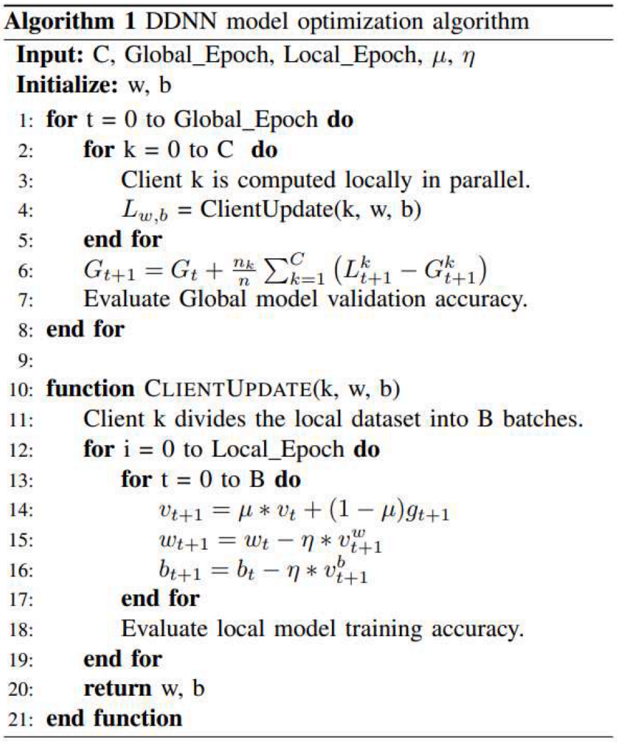
4. Experimental process and results

To validate the performance of the DDNN model for detecting credit card fraud, we train and test the model using credit card transaction data. This training set is broken into four sections and placed on separate clients to imitate the participation of multiple financial institutions in the model training. In the meantime, the test set is uploaded to the central server and utilized to assess the

[4] https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

[5] The feature Time indicates the time between each transaction and the first transaction. The feature Amount indicates the amount of the transaction made with the credit card. The feature Class is the label of the dataset, with 0 indicating a normal transaction and 1 indicating a fraudulent transaction. The rest of the features are processed with PCA.

[6] Typically, 80% of the dataset is utilized as training set and 20% as test set.



```
Algorithm 1 DDNN model optimization algorithm
Input: C, Global_Epoch, Local_Epoch, $\mu$, $\eta$
Initialize: w, b
for t = 0 to Global_Epoch do
    for k = 0 to C do
        Client k is computed locally in parallel.
        $L_{w,b}$ = ClientUpdate(k, w, b)
    end for
    $G_{t+1} = G_t + \frac{n_k}{n} \sum_{k=1}^{C} \left( L_{t+1}^{k} - G_{t+1}^{k} \right)$
    Evaluate Global model validation accuracy.
end for

function ClientUpdate(k, w, b)
    Client k divides the local dataset into B batches.
    for i = 0 to Local_Epoch do
        for t = 0 to B do
            $v_{t+1} = \mu * v_t + (1 - \mu) g_{t+1}$
            $w_{t+1} = w_t - \eta * v_{t+1}^{w}$
            $b_{t+1} = b_t - \eta * v_{t+1}^{b}$
        end for
        Evaluate local model training accuracy.
    end for
    return w, b
end function
```

Fig. 3. DDNN model optimization algorithm.

global model's precision. Fig. 4 shows the entire optimization process for the DDNN model using Algorithm 1. Figure (a) depicts the loss value of the objective function for a client training a local model, which exhibits a fluctuating decreasing trend and eventually converges to a level indicating that the model has converged. The objective function loss value of the global model on the test set is shown in Figure (b), and the value eventually converges to a level indicating that the global model has converged.

To compare with the DDNN model, we completed experiments related to the CDNN model[7]. The optimization process of the CDNN model is shown in Fig. 5, where the loss values of the objective function show an overall decreasing trend, and the final oscillation tends to be horizontal, indicating that the model has converged. From the loss values of training and validation, both DDNN and CDNN also achieve the convergence of the model. In particular, since DDNN uses distributed parallelism to optimize the model, the model proposed in this paper takes less time to converge[8].

Based on Zhang et al. (2022), while considering the loss value of the model's objective function, we select Accuracy, Precision, Recall, F1-score receiver operating characteristic curve (ROC) and the area under the ROC curve (AUC) metrics to evaluate the model's capacity to detect fraud. On the test set, we demonstrate the performance of the DDNN model, the CDNN model, multiple centrally developed machine learning models, and the experimental results are presented in Table 1 and Fig. 6. Compared to deep learning models proposed in previous research (Benchaji et al., 2021; Forough et al., 2021; Esenogho et al., 2022), the DDNN model proposed in our study performs better on metrics such as accuracy, F1-score and ROC. Therefore, our proposed DDNN model is more effective at detecting credit card fraud.

5. Conclusion

This study proposes a DDNN model for credit card transaction fraud detection and an algorithm for DDNN model optimization. By learning from actual credit card transaction data, the DDNN model achieves convergence and obtains the ability to detect fraudulent transactions. Building the DDNN model in a distributed manner allows numerous clients to train the model simultaneously and eliminates the data handling costs and privacy leakage of centrally built models. The experimental results suggest that the DDNN proposed in this study optimizes the model faster and has a more robust detection capability than models constructed centrally. In addition, the distributed model enables data sharing across financial institutions and provides an efficient and secure collaboration path for financial regulation and anti-fraud activities.

[7] Here the CDNN model is set up in the same way as the DDNN model, the only difference is the way the model is optimally solved.
[8] With the simultaneous participation of four financial companies, the DDNN model took only about 70% of the time of the CDNN model.

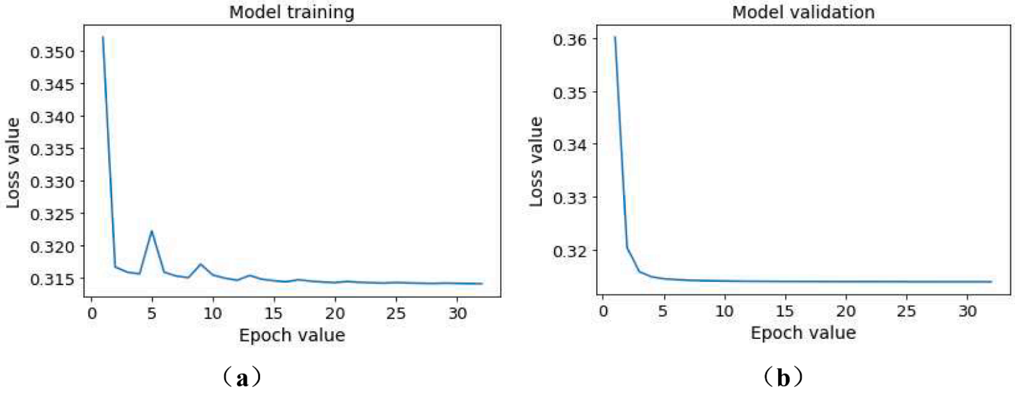


Fig. 4. DDNN model optimization process.

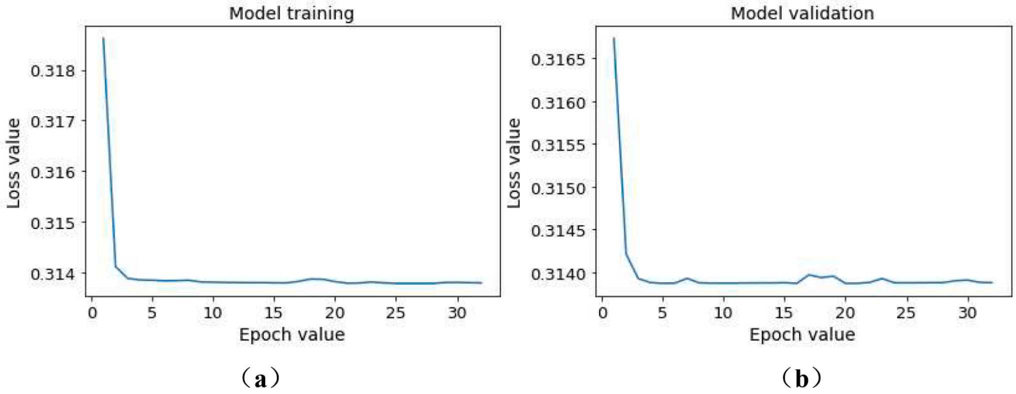


Fig. 5. CDNN model optimization process.

Table 1
Multiple models detection accuracy results.

	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
DDNN	**99.9422**	**99.9649**	99.9772	**99.9710**
CDNN	99.9369	99.9579	99.9789	99.9684
LR	99.8911	99.9331	99.9577	99.9454
SVM	99.9297	99.9349	**99.9947**	99.9648
DT	99.9051	99.9613	99.9437	99.9525

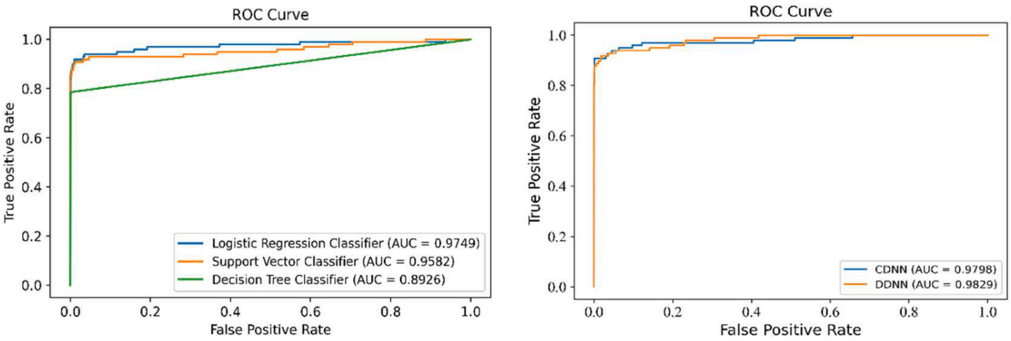


Fig. 6. ROC curves for multiple models.

Funding

This work is financially supported by the National Natural Science Foundation of China (No. 72104075, 72274056), the National Social Science Fund of China (No. 19AZD014, 21&ZD125), the Natural Science Foundation of Hunan Province (No. 2022JJ40106), and Hunan University Youth Talent Program.

CRediT authorship contribution statement

Yu-Tian Lei: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Software. **Chao-Qun Ma:** Resources, Funding acquisition, Supervision, Investigation, Visualization, Project administration. **Yi-Shuai Ren:** Conceptualization, Methodology, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization, Resources, Project administration, Funding acquisition. **Xun-Qi Chen:** Conceptualization, Writing – review & editing. **Seema Narayan:** Writing – review & editing. **Anh Ngoc Quang Huynh:** Writing – review & editing.

Declaration of Competing Interest

No potential conflict of interest was reported by the author(s).

Data availability

Data will be made available on request.

References

Bahnsen, A.C., Aouada, D., Stojanovic, A., Ottersten, B., 2016. Feature engineering strategies for credit card fraud detection. *Expert Syst.* Appl. 51, 134–142.

Benchaji, I., Douzi, S., El Ouahidi, B., Jaafari, J., 2021. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. J. Big Data 8, 1–21.

Bhattacharyya, S., Jha, S., Tharakunnel, K., Westland, J.C., 2011. Data mining for credit card fraud: a comparative study. Decis. *Support Syst.* 50 (3), 602–613.

Carcillo, F., Le Borgne, Y.A., Caelen, O., Kessaci, Y., Oblé, F., Bontempi, G., 2021. Combining unsupervised and supervised learning in credit card fraud detection. Inf. Sci. 557, 317–331.

Carneiro, N., Figueira, G., Costa, M., 2017. A data mining based system for credit-card fraud detection in e-tail. Decis. Support Syst. 95, 91–101.

Côté-Allard, U., Fall, C.L., Drouin, A., Campeau-Lecours, A., Gosselin, C., Glette, K., Laviolette, F., Gosselin, B., 2019. Deep learning for electromyographic hand gesture signal classification using transfer learning. IEEE Trans. Neural Syst. Rehabil. Eng. 27 (4), 760–771.

Dal Pozzolo, A., Caelen, O., Le Borgne, Y.A., Waterschoot, S., Bontempi, G., 2014. Learned lessons in credit card fraud detection from a practitioner perspective. Expert Syst. Appl. 41 (10), 4915–4928.

Esenogho, E., Mienye, I.D., Swart, T.G., Aruleba, K., Obaido, G., 2022. A neural network ensemble with feature engineering for improved credit card fraud detection. IEEE Access 10, 16400–16407.

Fiore, U., De Santis, A., Perla, F., Zanetti, P., Palmieri, F., 2019. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Inf. Sci. 479, 448–455.

Forough, J., Momtazi, S., 2021. Ensemble of deep sequential models for credit card fraud detection. Appl. Soft Comput. 99, 106883.

Fu, A., Chen, Z., Mu, Y., Susilo, W., Sun, Y., Wu, J., 2019. Cloud-based outsourcing for enabling privacy-preserving large-scale non-negative matrix factorization. IEEE Trans. Serv. Comput. 15 (1), 266–278.

Karpoff, J.M., 2021. The future of financial fraud. J. Corp. Finance 66, 101694.

Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S.K., Song, Y., Yoon, J.A., Kim, J.I., 2019. Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. Expert Syst. Appl. 128, 214–224.

Li, Z., Huang, M., Liu, G., Jiang, C., 2021. A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. Expert Syst. Appl. 175, 114750.

Lin, W., Sun, L., Zhong, Q., Liu, C., Feng, J., Ao, X., Yang, H., 2021. Online credit payment fraud detection via structure-aware hierarchical recurrent neural network. IJCAI, pp. 3670–3676.

McMahan, B., Moore, E., Ramage, D., Hampson, S., y Arcas, B.A., 2017. Communication-efficient learning of deep networks from decentralized data. In: Artif. Intell. and statistics, PMLR, pp. 1273–1282.

Pumsirirat, A., Liu, Y., 2018. Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. Int. J. Adv. Comput. Sci. Appl. 9 (1).

Repousis, S., Lois, P., Veli, V., 2019. An investigation of the fraud risk and fraud scheme methods in Greek commercial banks. J. Money Laund. Control 22 (1), 53–61.

Zhang, X., Han, Y., Xu, W., Wang, Q., 2021. HOBA: a novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Inf. Sci. 557, 302–316.

Zhang, Y., Hu, A., Wang, J., Zhang, Y., 2022. Detection of fraud statement based on word vector: evidence from financial companies in China. Finance Res. Lett. 46, 102477.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., Li, J., 2021. Intelligent financial fraud detection practices in post-pandemic era. Innovation 2 (4), 100176.