Journal of Computer Technology and Software

ISSN:2998-2383

Vol. 4, No. 1, 2025

Leveraging GANs for Financial Fraud Detection: A Paradigm Shift

Kaelen Rivera[1], Liner Chen[2], Xiaofei Wang[3]
[1]University of California, Riverside, USA
[2]University of California, Riverside, USA
[3]University of California, Riverside, USA

*Corresponding author: Kaelen Rivera, kaelen.rivera72@ucr.edu

Abstract: This paper addresses the critical issue of financial fraud detection, emphasizing the shift from traditional credit assessments to leveraging big data and machine learning for enhanced risk assessment. It introduces an innovative model that combines autoencoders with adversarial generative learning to tackle the challenge of sample imbalance without relying on actual fraudulent samples. The model, termed AE-GAN, generates fraudulent samples from normal transaction data, facilitating binary classification. The paper highlights two key contributions: the novel approach to sample generation and the construction of a detection model that not only mitigates class imbalance but also improves detection capabilities through adversarial learning. This research underscores the importance of emerging technologies in bolstering financial institutions' competitiveness in the fintech era.

Keywords: Generative Adversarial Networks (GANs), Financial Fraud Detection, Sample Imbalance.

1. Introduction

Financial fraud is of a severe nature and can lead to significant economic losses for victims and financial institutions. The effective application of machine learning anti-fraud models implies a reduction in economic losses caused by fraud. Against the backdrop where traditional credit indicator assessment methods can no longer effectively cope with the diverse financial fraud detection demands in a big data environment, leveraging big data resources to mine valuable information from multi-source data to establish risk assessment models, and enhancing financial fraud detection capabilities with emerging technologies such as big data, machine learning, and deep learning, has become the key for financial institutions to enhance their core competitiveness in the era of financial technology.

In the issue of financial fraud detection, the technologies mainly adopted by the industry can be summarized into two categories: traditional statistical learning methods and machine learning-based methods. This paper designs and constructs a model based on autoencoders combined with adversarial generative learning. The innovations of this paper are mainly reflected in the following aspects:

(1) The issue of sample imbalance is the biggest challenge in financial fraud detection. The detection model constructed in this paper is trained solely using normal samples from financial data. Based on the proposed hypothesis about the distribution relationship between normal transaction samples and fraudulent transaction samples, the distribution of fraudulent transaction samples is defined. Fraudulent samples are generated through the normal sample distribution, which is different from the conventional methods of expanding the dataset using oversampling, SMOTE, etc. The method of generating fraudulent samples proposed in this paper does not require the assistance of actual fraudulent samples, achieving binary classification learning based on one type of sample.

(2) Constructing financial fraud detection models using autoencoders and adversarial generative learning, implemented on both autoencoders and variational autoencoders. Based on the distinct characteristics of autoencoders and variational autoencoders, a financial fraud detection model is proposed: AE-GAN, which is based on the autoencoder and integrates a generative adversarial network.

The financial fraud detection model presented in this paper is based on the premise that only normal samples are used, and "fraudulent samples" are generated by introducing adversarial learning. The foundation for generation is the feature extraction capability of the autoencoder. The model constructed in this paper not only addresses the issue of class data imbalance to a certain extent but also enhances the detection capability of the model with the assistance of the generated "fraudulent samples".

2. Related Work

Financial fraud detection has increasingly leveraged deep learning techniques to enhance accuracy and robustness. Traditional methods based on statistical models and rule-based approaches struggle with evolving fraudulent behaviors and highly imbalanced datasets. Deep learning models, particularly those incorporating generative adversarial networks (GANs), autoencoders, and hybrid architectures, have demonstrated significant improvements in anomaly detection and financial risk assessment. Jiang et al. [1] explored the use of GANs for addressing data imbalance in financial market supervision, which aligns closely with our approach of generating synthetic fraudulent samples to improve fraud detection performance. Traditional oversampling techniques, such as SMOTE, often fail to capture the complex distribution of fraudulent transactions, whereas GAN-based synthetic sample generation provides more realistic and representative fraudulent data, facilitating more effective training of fraud detection models. In addition to GANs, autoencoders have been widely studied for their ability to learn latent representations of normal financial transactions. The combination of variational autoencoders (VAEs) with adversarial learning has been explored in anomaly detection tasks, as highlighted by Huang et al. [2], demonstrating the potential of generative models in rare-event classification problems.

Beyond generative models, various deep learning architectures have been applied to financial risk assessment and fraud detection. Wang et al. [3] proposed a hybrid approach that combines convolutional neural networks (CNNs) with transformers for predictive modeling in risk-based applications, emphasizing the importance of hierarchical feature extraction and attention mechanisms in financial data analysis. Similarly, Sun et al. [4] leveraged time-series transformer models for advanced bank risk prediction, illustrating the effectiveness of self-attention mechanisms in capturing temporal dependencies in financial transactions. Another notable approach involves graph-based learning, where Zhang et al. [5] introduced robust graph neural networks (GNNs) for stability analysis in dynamic networks, which can be extended to fraud detection by modeling financial transaction relationships. Yao et al. [6] further demonstrated the application of hierarchical graph neural networks in stock type prediction, reinforcing the adaptability of graph-based models for financial applications.

Another challenge in fraud detection is the trade-off between model complexity and computational efficiency. Wang et al. [7] investigated feature alignment-based knowledge distillation for compressing large language models, providing insights into optimizing deep learning models for real-world deployment. Yan et al. [8] explored neural architecture search (NAS) techniques for advancing deep learning frameworks, which can be leveraged to fine-tune fraud detection models for improved efficiency and accuracy. Similarly, Jiang et al. [9] studied dynamic risk control and asset allocation using reinforcement learning, which could be adapted for fraud detection by dynamically adjusting detection thresholds based on evolving transaction patterns.

Recent research has also emphasized collaborative optimization and ensemble learning in financial data mining. Feng et al. [10] applied deep learning and ResNeXt-based architectures for collaborative financial data optimization, demonstrating the potential of ensemble methods in improving predictive performance. Liang et al. [11] explored contextual analysis using deep learning for sensitive information detection, which could be extended to identifying anomalous transaction behaviors in fraud detection. Furthermore, Long et al. [12] introduced an adaptive transaction sequence neural network for money laundering detection, emphasizing the importance of sequential modeling in fraud detection systems. Wu et al. [13] integrated CNN and GRU for financial sentiment analysis and risk prediction, showcasing the applicability of hybrid deep learning models in financial security applications. Additionally, Xu et al. [14] proposed a Hybrid LSTM-GARCH framework for financial market volatility prediction, highlighting the benefits of combining deep learning with traditional statistical models in risk forecasting. Wang et al. [15] conducted a comparative study on machine learning models for credit default prediction, offering interpretability insights that could be relevant for fraud detection applications. Lastly, Gao et al. [16] proposed a multi-level attention and contrastive learning-based transformer model for enhanced text classification, which aligns with the need for robust feature extraction in fraud detection tasks.

The advancements in deep learning, generative models, and financial fraud detection reviewed in this section provide a strong foundation for the AE-GAN model proposed in this paper. By integrating autoencoders with adversarial generative learning, our approach builds upon prior work in anomaly detection, data augmentation, and financial risk modeling while addressing key challenges in class imbalance and fraud detection accuracy. The use of synthetic fraudulent samples enables more robust learning and surpasses traditional oversampling techniques, positioning GAN-based generative methods as a viable solution for addressing real-world financial fraud detection challenges.

3. Background

In recent years, deep learning algorithms have been increasingly applied to the financial sector, particularly in the field of financial risk identification [17]. Yu et al. [18], in their study on default risk using a publicly available Japanese consumer dataset, employed a deep belief network as an ensemble strategy. They trained Extreme Learning Machine (ELM) sub-classifiers on training subsets and integrated the classification results as input to train a Deep Belief Network (DBN) model for classification, achieving the best classification performance. However, in the aforementioned studies, the dataset's features that represent credit risk were pre-selected, failing to truly demonstrate the capability and advantages of deep learning in feature extraction.

Ha et al. [19] proposed a deep learning-based credit scoring feature selection method, which was also based on artificially set and pre-selected feature sets, without conducting comparative experiments. Tran et al. [20] integrated deep neural networks and genetic programming to propose a hybrid credit scoring model, which achieved a higher classification accuracy in experiments compared to other machine learning methods.Luo [21] and others used deep learning algorithms such as Deep Belief Networks on credit default swap (CDS) datasets to build corporate credit scoring models, and compared them with logistic regression, multilayer perceptrons, and support vector machines in experiments. Their classification performance was the best in terms of accuracy, AUC, and other evaluation metrics. Convolutional Neural Networks (CNNs) have also been used by scholars to address anomaly detection [22] and financial fraud issues [23], consisting of convolutional layers, pooling layers, and fully connected layers. In the case of high-dimensional sparse financial data, the capability of convolutional layers to extract features and the dimensionality reduction of pooling layers can reduce the number of parameters in the network. The final fully connected layer of the network can be output to a softmax layer for classification.

This method has also been frequently used in Kaggle competitions, achieving good results. A non-neural network deep learning algorithm, Deep Forest [24], was first proposed by Zhou Zhihua and others in 2017. Deep Forest is an innovation in the ensemble of decision trees, conducting representation learning through cascade structures of decision trees. Additionally, Deep Forest enhances representation learning ability through multi-granularity scanning. The team of Zhou Zhihua, in collaboration with Ant Financial, proposed a financial fraud detection method targeting Ant Financial's customer base based on Deep Forest, which has been proven to be more effective than the current detection methods used by Ant Financial.

This paper primarily focuses on autoencoders and Generative Adversarial Networks (GANs) for research, organizing relevant literature. Autoencoders were initially used in early anomaly detection studies, mainly detecting anomalies through reconstruction error [25]. Domestically, Liu Yan and others [26] used autoencoders for financial fraud detection, training autoencoders to obtain the distribution of normal samples, and then identifying fraudulent transaction samples based on the differences in sample distributions across different categories. I. Goodfellow and others proposed a zero-sum game-based adversarial training network in 2014, which is the well-known Generative Adversarial Network (GAN) [27].

4. Method

4.1 Autoencoder and Generative Adversarial Networks

Traditional machine learning approaches to financial fraud detection rely heavily on feature engineering based on empirical knowledge. Autoencoders possess excellent feature extraction capabilities, enabling them to extract high-level intermediate representations of samples, thus overcoming the limitations of conventional machine learning algorithms. This paper explores broader applications of autoencoders in financial fraud detection, focusing on two models as illustrated in Figure 1. The paper begins with an overview of autoencoder-based financial fraud detection methods, then proposes an AE-GAN model that integrates autoencoders with generative adversarial networks. Subsequently, improvements are made to both the autoencoder and generative adversarial network components of AE-GAN, leading to the proposal of the AE-G model.

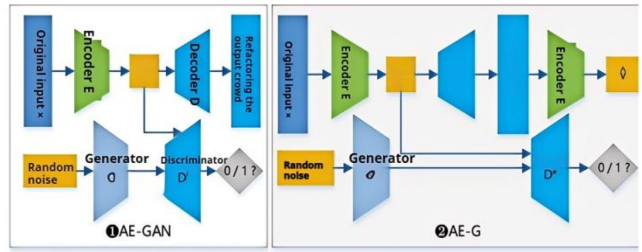

Figure 1. Main Models Covered in This paper

4.2 Autoencoder-Based Financial Fraud Detection Methods

An autoencoder is a type of artificial neural network algorithm consisting of an encoder network and a decoder network.

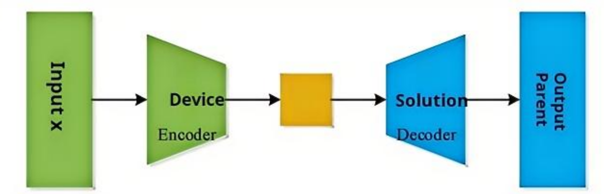

Figure 2. Schematic Diagram of Autoencoder Network

Through the encoder, representation learning is performed on input samples to obtain high-level abstract representations. The decoder then utilizes these high-level abstract representations to reconstruct the original input. Autoencoders train specific encoder and decoder pairs for a class of samples. The reconstructed output from an autoencoder is inherently degraded compared to the original input and can only reconstruct sample data similar to the training data. Autoencoders can be used for nonlinear dimensionality reduction and anomaly detection.

Given the number of hidden layer nodes m, activation function g(·), learning rate η, maximum iteration count N_max (or other stopping conditions such as desired error), the autoencoder algorithm is described as follows:

(1) Encoding phase: The training sample x is input to the encoder network. Through the transformation of hidden layers with nonlinear activation functions in the encoder, x is compressed into a low-dimensional vector z. z can be viewed as a representation of the input data x and is called the hidden layer feature. In this process, the encoder compresses the original data into meaningful low-dimensional vectors, achieving nonlinear dimensionality reduction that is similar to but superior to Principal Component Analysis (PCA). Equation 3.1 shows x being encoded through function f_θ into a low-dimensional space $z \in R^m$:

$$z = f_\theta(x) = \sigma_e(W_e x + b_e) \tag{1}$$

where θ={W,b} represents the autoencoder network parameters, W and b represent the weight matrix and bias term respectively, and σ is the activation function, such as sigmoid, ReLU, or tanh.

(2) Decoding phase: The decoder restores the hidden layer features z from low-dimensional space to high-dimensional space, reconstructing output X to be as similar as possible to the original input sample data. The low-dimensional representation $z \in R^m$ is reconstructed into an approximation $\hat{x} \in R^n$ of the input $x \in R^n$, as shown in Equation 2:

$$\hat{x} = g_{\theta'}(z) = \sigma_d(W_d z + b_d) \tag{2}$$

(3) Backpropagation to update weights W and biases b. The autoencoder aims to have the reconstructed output approximate the original input x. Mean Square Error (MSE) or Cross Entropy is typically used as the loss function to minimize their difference. The autoencoder updates weights W and biases b through backpropagation, as shown in Equations 3 and 4:

$$W = W - \eta * \partial J(W, b)/\partial W \tag{3}$$

$$b = b - \eta * \partial J(W, b)/\partial b \tag{4}$$

The final mapping function is given by Equation 5:

$$f(x) = \sigma_d(W_d \sigma_e(W_e X + b_e) + b_d) \tag{5}$$

The training process of autoencoders includes unsupervised training and supervised fine-tuning. Unsupervised training is performed using one class of samples, followed by supervised algorithms to fine-tune the autoencoder network parameters, updating weights through backpropagation like regular neural networks. Original autoencoders face the issue of failing to learn effective feature representations, potentially learning only an identity function that mechanically copies input to output without encoding functionality.

To address this issue, improvements to the original autoencoder network structure or additional constraints have led to enhanced algorithms such as sparse autoencoders, denoising autoencoders, and variational autoencoders. Among these, the denoising autoencoder proposed by Vincent et al. is particularly suitable for financial fraud detection. Denoising autoencoders introduce a degradation mechanism by adding noise to input data to alter the input data distribution.

By training the denoising autoencoder to reconstruct data while minimizing the error between original and reconstructed data, it prevents the autoencoder from learning features that are merely identity representations of the original input. The extracted hidden layer features become more noise-resistant while better reflecting the data's essential characteristics and achieving higher robustness. The network structure of a denoising autoencoder is shown in Figure 3:

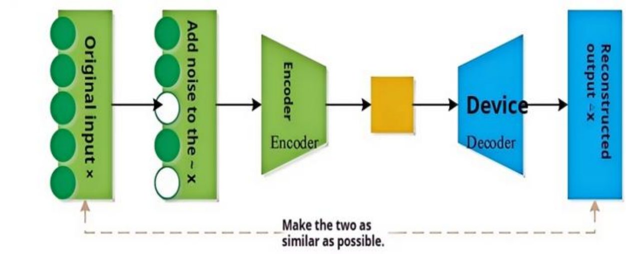

Figure 3. AE-GAN network structure

4.3 Autoencoder in AE-GAN

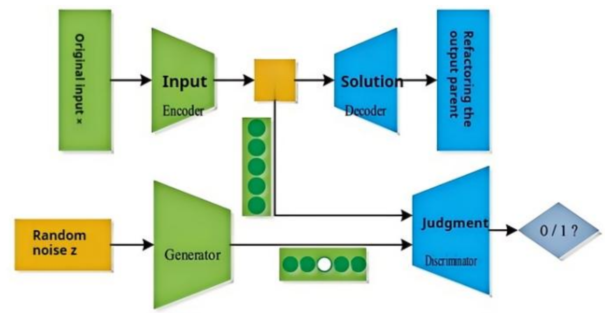

Figure 4. Schematic Diagram of AE-GAN Network Structure

This section proposes the AE-GAN financial detection model that integrates an autoencoder with a generative adversarial network, as shown in Figure 4. The model consists of an autoencoder and a generative adversarial network. AE-GAN learning occurs in two phases: The first phase trains the autoencoder to learn latent variables from normal samples to obtain high-level abstract representations of the original sample data. The encoder's encoding process has certain denoising effects and can extract more essential data features. The second phase trains a generative adversarial network, using the latent variables of normal samples obtained in the first phase as input samples. The generator of the GAN attempts to generate data approximating the original input samples, producing latent variables of pseudo-normal samples, which are used as latent variables of "fraudulent transactions" to assist in model classification training. The discriminator of the GAN serves as a classifier and, after training, is used to detect actual fraudulent samples.

The sparse autoencoder, proposed by Ng[50], avoids learning a simple identity function by adding sparsity constraints. It introduces sparsity constraints in the hidden layer outputs, forcing the network to use fewer neural nodes to extract effective features, discovering specific data structures through high-dimensional sparse hidden layer features. In sparse autoencoders, most hidden layer nodes are suppressed by sparsity constraints, with outputs close to 0, making the network rely on only some hidden layer nodes for encoding and decoding, resulting in more sparse extracted features. When adding sparsity constraints, regularization terms for activation levels must be added to the loss function to penalize excessive activation. L1 norm and KL divergence are two commonly used methods. When using L1 regularization, with $a_j(x_i)$ representing node j's activation value for input xi and λ representing the L1 regularization coefficient controlling penalty intensity, the sparse autoencoder's loss function is shown in Equation 6:

$$J_{SAE}(W,b) = J(x,\hat{x}) + \lambda \sum_{i,j} |a_j(x_i)| \quad (6)$$

Using KL divergence regularization, with sparsity parameter ρ, average activation level $\hat{\rho}_j$ for hidden layer node j, and KL regularization coefficient β, the sparse autoencoder's loss function is shown in Equation 7:

$$J_{SAE}(W,b) = J(x,\hat{x}) + \beta \sum_{j=1}^{m} KL(\rho|\hat{\rho}_j) \quad (7)$$

The KL divergence calculation is shown in Equation 8:

$$KL(\rho|\hat{\rho}_j) = \rho \log(\frac{\rho}{\hat{\rho}_j}) + (1-\rho)\log(\frac{1-\rho}{1-\hat{\rho}_j}) \quad (8)$$

The sparsity parameter ρ represents the ideal average activation level of hidden layer nodes, typically a small value close to 0 (e.g., ρ=0.05). $\hat{\rho}_j$ is calculated using Equation 9:

$$\hat{\rho}_j = \frac{1}{n}\sum i = 1^n [a_j(x_i)] \quad (9)$$

As the difference between ρ and $\hat{\rho}_j$ increases, KL divergence increases monotonically. Training the sparse autoencoder to make $\hat{\rho}_j$ approach ρ necessarily leads to more nodes $\hat{\rho}_j$ approaching 0, resulting in learned features with sparsity.

4.4 Generative Adversarial Network in AE-GAN

The generative adversarial network in AE-GAN is a conventional GAN that uses the hidden layer features encoded by the autoencoder's encoder from the training set samples as input. Based on the assumption that hidden layer features in latent space show more significant differences between normal and fraudulent transactions than original transaction data, the hidden layer features obtained through the autoencoder are used as input. The GAN generator generates variables approximating the hidden layer features of normal samples.

The AE-GAN model algorithm is described as follows:

(1) Set iteration counts for both autoencoder and generative adversarial network, initialize parameters for both networks;

(2) Randomly sample M normal transaction data as training samples;

(3) Train the autoencoder network, updating autoencoder parameters through backpropagation;

(4) Use the trained autoencoder's encoder network to compute sample latent variables, constructing a latent variable dataset $z_1, \ldots z_j, \ldots z_N$;

(5) Train the generative adversarial network, calculate loss functions for generator G and discriminator D based on z_j, compute gradients of loss functions, and update parameters of generator G and discriminator D respectively according to gradients.

After model training is complete, it can be used for financial fraud detection. During financial fraud detection, the autoencoder's encoder and the adversarial network's discriminator are needed: Input test samples to the autoencoder for feature extraction, use the autoencoder to compute hidden layer features for each sample, then input the extracted features to the trained GAN discriminator, which predicts sample labels.

5. Experiment

5.1 Dataset

The experiments in this section utilize real credit card transaction records collected during the research collaboration between the Machine Learning Group at Vrije Universiteit Brussel and the third-party payment company Worldline. The dataset comprises 284,807 credit card transactions made by consumers in a certain region of Europe over a two-day period. Out of these, there are 492 fraudulent transactions, accounting for 0.172%, with the remainder being normal transactions, resulting in a highly imbalanced dataset between the two types of data samples.

5.2 Experiment

Observations of the F1 score and Area Under the Curve (AUC) during training revealed that AE-GAN experienced greater fluctuations, while AE-G was relatively more stable.

This confirmed that AE-GAN's use of the original generative adversarial network to train generated data to approximate the latent variables of the original data led to model instability and greater fluctuation in training results. AE-G's generative adversarial network aimed to generate values different from the latent variables of normal samples, resulting in more stable training outcomes. The model evaluation metrics are shown in Table 1.

Table 1. Experiment Results

Model	F1	AUC	Recall	Precision	Acurracy
AE-G	0.8380	0.9538	0.7802	0.9052	0.9795
AE-GAN	0.8350	0.9649	0.7608	0.9251	0.9795
AE	0.7350	0.8749	0.7705	0.7027	0.9795

From Table 1, it can be observed that the AE-G model outperforms the other two models in multiple metrics, especially in the more critical evaluation indicators for financial fraud detection, such as recall and F1 score, where AE-G performs the best. An increase in recall rate may sacrifice precision to some extent, but for financial fraud detection, recall is more important than precision because the value of correctly identifying fraudulent transactions is greater than that of correctly identifying normal transactions. It is noteworthy that, in actual training, the average F1 score of AE-G is slightly lower than that of AE-GAN, but the AE-G model is more robust in the detection phase. This indicates that the improved generative adversarial network, by generating fraudulent transaction samples, enables the discriminator to learn more confident boundaries, thereby better enhancing the identification rate of fraudulent transaction samples.

Comparing AE-GAN with the traditional autoencoder model: the traditional anomaly detection method of autoencoders only learns from normal samples, which tends to classify fraudulent samples as normal, resulting in lower recall and AUC values in the experimental results. However, the accuracy value is relatively high. The proposed AE-GAN integrates the autoencoder network with the generative adversarial network, using the generative adversarial network to generate "fraudulent samples" to assist in classification training, which can alleviate the aforementioned issue to some extent. The discriminator learns to distinguish between the original data's latent variables and the generator's approximated generated variables, enhancing the ability to identify fraudulent transactions. The experimental results show that AE-GAN outperforms the autoencoder in all metrics, proving that AE-GAN has significantly improved performance compared to the autoencoder.

6. Conclusion

In conclusion, this paper presents a novel financial fraud detection model that leverages autoencoders and adversarial generative learning to address the challenges of sample imbalance and enhance detection capabilities. By training on normal samples and generating synthetic fraudulent samples, the model circumvents the need for actual fraudulent data, facilitating binary classification learning. The AE-GAN model, which integrates autoencoders with a generative adversarial network, not only mitigates class imbalance but also bolsters detection accuracy through adversarial learning. This approach represents a significant advancement in financial fraud detection, offering a robust solution to the complexities of modern financial crime.

References

[1] M. Jiang, Y. Liang, S. Han, K. Ma, Y. Chen, and Z. Xu, “Leveraging Generative Adversarial Networks for Addressing Data Imbalance in Financial Market Supervision,” arXiv preprint arXiv:2412.15222, 2024.

[2] X. Huang, Z. Zhang, X. Li, and Y. Li, “Reinforcement Learning-Based Q-Learning Approach for Optimizing Data Mining in Dynamic Environments.”

[3] Y. Wang, Z. Xu, Y. Yao, J. Liu, and J. Lin, “Leveraging Convolutional Neural Network-Transformer Synergy for Predictive Modeling in Risk-Based Applications,” arXiv preprint arXiv:2412.18222, 2024.

[4] W. Sun, Z. Xu, W. Zhang, K. Ma, Y. Wu, and M. Sun, “Advanced Risk Prediction and Stability Assessment of Banks Using Time Series Transformer Models,” arXiv preprint arXiv:2412.03606, 2024.

[5] X. Zhang, Z. Xu, Y. Liu, M. Sun, T. Zhou, and W. Sun, “Robust Graph Neural Networks for Stability Analysis in Dynamic Networks,” in Proc. 2024 3rd Int. Conf. Cloud Comput., Big Data Appl. Softw. Eng. (CBASE), 2024, pp. 806-811.

[6] J. Yao, Y. Dong, J. Wang, B. Wang, H. Zheng, and H. Qin, “Stock Type Prediction Model Based on Hierarchical Graph Neural Network,” in Proc. 2024 Int. Conf. Electron. Devices, Comput. Sci. (ICEDCS), 2024, pp. 426-430.

[7] S. Wang, C. Wang, J. Gao, Z. Qi, H. Zheng, and X. Liao, “Feature Alignment-Based Knowledge Distillation for Efficient Compression of Large Language Models,” arXiv preprint arXiv:2412.19449, 2024.

[8] X. Yan, J. Du, L. Wang, Y. Liang, J. Hu, and B. Wang, “The Synergistic Role of Deep Learning and Neural Architecture Search in Advancing Artificial Intelligence,” in Proc. 2024 Int. Conf. Electron. Devices, Comput. Sci. (ICEDCS), 2024, pp. 452-456.

[9] M. Jiang, Z. Xu, and Z. Lin, “Dynamic Risk Control and Asset Allocation Using Q-Learning in Financial Markets,” Transactions on Computational and Scientific Methods, vol. 4, no. 12, 2024.

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

[11] Y. Liang, E. Gao, Y. Ma, Q. Zhan, D. Sun, and X. Gu, “Contextual Analysis Using Deep Learning for Sensitive Information Detection,” in Proc. 2024 Int. Conf. Comput., Inf. Process. Adv. Educ. (CIPAE), 2024, pp. 633-637.

[12] S. Long, D. Yi, M. Jiang, M. Liu, G. Huang, and J. Du, “Adaptive Transaction Sequence Neural Network for Enhanced Money Laundering Detection,” in Proc. 2024 Int. Conf. Electron. Devices, Comput. Sci. (ICEDCS), 2024, pp. 447-451.

[13] Y. Wu, M. Sun, H. Zheng, J. Hu, Y. Liang, and Z. Lin, “Integrative Analysis of Financial Market Sentiment Using CNN and GRU for Risk Prediction and Alert Systems,” in Proc. 2024 Int. Conf. Electron. Devices, Comput. Sci. (ICEDCS), 2024, pp. 410-415.

[14] K. Xu, Y. Wu, M. Jiang, W. Sun, and Z. Yang, “Hybrid LSTM-GARCH Framework for Financial Market Volatility Risk Prediction,” Journal of Computer Science and Software Applications, vol. 4, no. 5, pp. 22-29, 2024.

[15] Y. Wang, Z. Xu, K. Ma, Y. Chen, and J. Liu, “Credit Default Prediction with Machine Learning: A Comparative Study and Interpretability Insights.”

[16] J. Gao, G. Liu, B. Zhu, S. Zhou, H. Zheng, and X. Liao, “Multi-Level Attention and Contrastive Learning for Enhanced Text Classification with an Optimized Transformer,” arXiv preprint arXiv:2501.13467, 2025.

[17] J. B. Heaton, N. G. Polson, and J. H. Witte, "Deep learning in finance", Proceedings of the 2017 Applied Stochastic Models in Business and Industry, vol. 33, no. 1, pp. 561-580, 2017.

[18] L. Yu, Z. Yang, and L. Tang, "A novel multistage deep belief network based extreme learning machine ensemble learning paradigm for credit risk assessment", Proceedings of the 2016 Flexible Services and Manufacturing Journal, vol. 28, no. 4, 2016.

[19] V. S. Ha and H. N. Nguyen, "Credit scoring with a feature selection approach based deep learning", Proceedings of the 2016 MATEC Web of Conferences, vol. 54, 2016.

[20] K. Tran, T. Duong, and Q. Ho, "Credit scoring model: A combination of genetic programming and deep learning", Proceedings of the 2016 Future Technology Conference, pp. 113-119, 2016.

[21] C. Luo, D. Wu, and D. Wu, "A deep learning approach for credit scoring using credit default swaps", Proceedings of the 2016 Engineering Applications of Artificial Intelligence, vol. 65, 2016.

[22] R. H. Hwang, M. C. Peng, C. W. Huang, P. C. Lin, and V. L. Nguyen, "An unsupervised deep learning model for early network traffic anomaly detection", Proceedings of the 2020 IEEE Access, vol. 8, 2020.

[23] K. Fu, D. Cheng, Y. Tu, et al., "Credit card fraud detection using convolutional neural networks", Proceedings of the 23rd International Conference on Neural Information Processing (ICONIP), pp. 483-490, 2016.

[24] Z.-H. Zhou and J. Feng, "Deep forest", Proceedings of the 2019 National Science Review, vol. 6, no. 1, pp. 74-86, 2019.

[25] Y. Abakarim, M. Lahby, and A. Attioui, "An efficient real-time model for credit card fraud detection based on deep learning", Proceedings of the 12th International Conference, 2018.

[26] A. Pumsirirat and Y. Liu, "Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine", Proceedings of the 2018 International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, 2018.

[27] I. Goodfellow et al., "Generative adversarial nets", Proceedings of the 2014 Advances in Neural Information Processing Systems, pp. 2672-2680, 2014.