Journal of Organizational and End User Computing
Volume 36 • Issue 1 • January-December 2024

Financial Fraud Detection and Prevention:
Automated Approach Based on Deep Learning

Zeyi Miao
Law School, Southeast University, China

ABSTRACT

Financial fraud has always been a serious challenge in the financial sector. With the continuous development of technology, fraud in the financial market has become increasingly complex and hidden. Therefore, financial fraud detection and prevention have become particularly important to our lives. But as of today, the financial fraud detection methods that have emerged often leave something to be desired. Traditional detection methods based on rules and statistical methods perform poorly when processing large-scale and high-dimensional data, and are prone to false positives and false negatives. Moreover, as fraud techniques continue to evolve, the adaptability of traditional methods is also challenged. As a powerful machine learning technology, deep learning has excellent feature extraction and pattern recognition capabilities, and has achieved remarkable achievements in various fields, including image recognition, natural language processing, and speech recognition. In the financial field, the application of deep learning is also gradually emerging.

KEYWORDS

Financial Fraud, Deep Learning, Transformer, LOF, Random Forest

INTRODUCTION

In today's rapidly evolving digital economy, the financial sector, as a crucial pillar of social and economic development, has become a primary target for fraudsters. Financial fraud manifests in various forms, from traditional credit card fraud to sophisticated e-commerce fraud, causing significant damage to individual victims and undermining the stability of the financial market and social trust (Zhou et al., 2021). Existing financial fraud detection methods rely primarily on rules and pattern matching; however, these traditional approaches face significant limitations. They often struggle with identifying new and mutated fraud patterns and are prone to generating false positives and false negatives (Ashtiani & Raahemi, 2022).

In this context, deep learning technology has emerged as a promising solution in the field of financial fraud detection due to its excellent feature extraction and pattern recognition capabilities (Ozbayoglu et al., 2020). Deep learning models can automatically learn potential patterns of fraudulent behavior from massive financial transaction data, adapting in real time to new fraudulent techniques. These models can process and analyze large-scale financial transaction data, identifying subtle signals that may indicate fraudulent behavior (Xiuguo & Shengyong, 2022). This capability allows them to both recognize known patterns of fraud and adapt to emerging tactics dynamically.

Despite the potential of deep learning in financial fraud detection, the existing work has some shortcomings. Training deep learning models requires a large amount of labeled data, which is often

DOI: 10.4018/JOEUC.354411

difficult and expensive to obtain in the financial domain (Fang et al., 2021). Additionally, financial transaction data is typically highly imbalanced, with far more normal transactions than fraudulent ones, which can lead to models overlooking rare but critical fraud cases (Nguyen et al., 2020). Moreover, deep learning models are often considered black boxes due to the lack of transparency in their decision-making processes, which is particularly problematic in the financial sector, where clarity and interpretability are essential for both financial institutions and regulators (Zhang et al., 2018; Ye & Zhao, 2023; Ye et al., 2023).

A major challenge in financial fraud detection is data imbalance, where the number of fraudulent transactions is much less than the number of legitimate transactions. To address these issues, we propose the Transformer-LOF-Random Forest network model, an innovative hybrid model that combines the strengths of three powerful approaches: the transformer model, the local outlier factor (LOF) algorithm, and the random forest algorithm. Our model employs several strategies. The transformer model has advanced feature extraction with self-attention mechanism and sequence modeling to ensure effective capture of minority class (fraudulent transaction) signals. This enables the model to efficiently learn and represent complex temporal patterns in the transaction data that often indicate the presence of fraud. In addition, the LOF algorithm specifically enhances the model's ability to identify local anomalies in dense clusters of normal transactions, thus improving the detection of rare fraudulent instances. The random forest model further enhances this capability through the use of techniques such as bootstrap aggregation (bagging) and feature randomness, which help to reduce variance and bias and ensure that minority classes are adequately represented and learned during training.

The LOF algorithm enhances this capability by focusing on local anomalies. Unlike traditional methods that may miss out on subtle fraudulent patterns due to their global perspective, LOF identifies anomalies based on the local density deviations of data points. This makes our model particularly effective at detecting rare and emerging fraud techniques that may not conform to established global patterns.

The random forest component of our model further enhances its robustness and accuracy. By aggregating the decisions of multiple trees, random forest mitigates the risk of overfitting, which is a common issue with deep learning models when dealing with imbalanced datasets. This ensemble learning approach ensures that our model maintains high performance across various types of financial data, improving both recall and precision rates.

The synergy of these three algorithms enables our model to outperform traditional methods significantly in financial fraud detection. It not only excels in scenarios dealing with imbalanced data but also demonstrates superior detection accuracy and generalization capabilities. This innovative approach is validated through rigorous experimental evaluations, showcasing excellent results across various financial datasets. Our model provides an efficient and feasible solution for the financial industry, offering a new direction for financial security technology and demonstrating significant potential for practical application.

By leveraging the strengths of the transformer's sequence modeling, LOF's local anomaly detection, and random forest's ensemble learning, our model effectively addresses the limitations of traditional financial fraud detection methods. This hybrid approach offers improved adaptability to evolving fraud techniques, enhanced accuracy in identifying fraudulent transactions, and greater transparency in the decision-making process, making it a valuable tool for financial institutions in their efforts to combat financial fraud.

The contribution points of this paper are as follows:

- Innovative hybrid model: we introduce a novel Transformer-LOF-Random Forest network model that integrates the strengths of three powerful machine learning algorithms. This hybrid approach significantly enhances the detection accuracy and efficiency in financial fraud detection by effectively capturing complex relationships in data, identifying local anomalies, and improving prediction robustness.

- Effective handling of imbalanced data: our model addresses the challenge of imbalanced financial transaction data through advanced techniques. By utilizing the transformer's feature extraction capabilities, LOF's local anomaly detection, and random forest's ensemble learning, the model ensures accurate identification of rare fraudulent transactions amidst a large volume of legitimate transactions.
- Comprehensive experimental validation: we validate our model through extensive experiments on various financial datasets, demonstrating its superior performance in terms of key metrics such as accuracy, recall, and F_1 score. This empirical evidence highlights the practical applicability and effectiveness of our approach in real-world financial fraud detection scenarios.

RELATED WORK

Decision Tree Based Credit Scoring Model

Credit scoring is an important tool for financial institutions to assess the credit risk of borrowers before lending (Zhang et al., 2020). While traditional credit scoring methods rely on statistical models, in recent years, the application of machine learning techniques has brought new breakthroughs in credit scoring. Decision tree models have become a popular choice in the field of credit scoring due to their ease of understanding and implementation. Decision trees make it possible for nontechnical people to understand the model's decision logic by breaking down a complex decision-making process into a series of simple questions (Marqués et al., 2013). This feature is particularly important for financial institutions when interpreting and implementing credit decisions.

However, there are shortcomings in the application of decision tree models in financial credit scoring. First, because financial data are often high-dimensional and complex, decision tree models are prone to overfitting, i.e., overlearning the noise in the training data while ignoring the true distribution of the data, thus affecting their generalization ability (Golbayani et al., 2020). In addition, decision trees are very sensitive to small changes in the input data, and even small data fluctuations may lead to significant changes in the tree structure, which in turn affects the stability and prediction accuracy of the model. This is particularly unfavorable in the financial domain, where financial data is often affected by market fluctuations (Yotsawat et al., 2021). Although individual decision trees are easy to understand, in practice, it is often necessary to construct ensembles of decision trees, such as random forests, in order to improve the prediction performance, which makes the interpretability of the model much lower. Thus, the limitations of decision trees in financial credit scoring applications are manifested in their susceptibility to overfitting (Zhao, 2020), sensitivity to data changes, and interpretability challenges.

Customer Segmentation Based on Clustering Algorithms

In the financial services sector, categorizing customers into different segments can help financial institutions position their products and services more effectively (Ziafat & Shakeri, 2014). The core of customer segmentation strategy lies in identifying and understanding the unique needs and behavioral patterns of different customer groups. Clustering algorithms, especially K-means algorithms, are widely used in customer segmentation due to their simplicity and efficiency (Kamthania et al., 2018). By grouping customers based on similarity metrics, clustering algorithms can help financial institutions identify groups of customers with similar financial behaviors and needs for more targeted product design and marketing strategies (Yuan et al., 2021).

Although clustering algorithms have their advantages in customer segmentation, they also face challenges when dealing with financial data. First, financial data tends to be high-dimensional, containing a large number of variables and complex relationships, and traditional clustering algorithms tend to perform poorly in high-dimensional spaces, which can lead to inaccurate segmentation results (Zhao et al., 2021a). In addition, determining the number of clusters (i.e., K-value) is a difficult task because in practice, the optimal number of customer groups is often not a priori and needs to be determined by a data-driven approach. This process may require extensive experiments and domain knowledge (Alkhayrat et al., 2020). In addition, the interpretation and application of clustering results require in-depth business understanding and domain expertise, which may introduce additional complexity to a financial institution's customer segmentation strategy (Cai, 2020). Therefore, despite the value of clustering algorithms in financial customer segmentation, their limitations in handling high-dimensional data, determining the number of clusters, and interpreting applications cannot be ignored.

Market Basket Analysis Based on Association Rules

Market basket analysis is a commonly used technique in retail and marketing to provide a basis for product layout, inventory management, and cross-selling by analyzing the association relationship between goods in customer purchase behavior (Rao & Kiran, 2023). Association rule learning also plays an important role in financial product recommendation and sales strategy. Association rules can reveal the purchasing patterns and customer preferences among different financial products and help financial institutions optimize their product portfolios and marketing strategies (Videla-Cavieres & Ríos, 2014). However, although association rules are effective in revealing relationships among products, they also have limitations in financial applications.

First, association rule learning usually generates a large number of rules, but not all of them have practical significance or business value (Tiyasha et al., 2021). Filtering and interpreting these rules require in-depth business knowledge and professional judgment. In addition, due to the complexity of financial products, a simple purchase model may not fully reveal customers' true needs and preferences, which may lead to misleading recommendations or marketing decisions (Leote et al., 2020). In addition, the application of association rules often assumes that market environments and customer behavior patterns are stable; however, this assumption may not always hold true in dynamically changing financial markets. Therefore, despite the value of association rules in revealing relationships between financial products (Tai et al., 2021), their limitations in filtering rules, explaining complexity, and adapting to market changes need to be carefully considered.

MATERIALS AND METHODS

Overview of Our Network

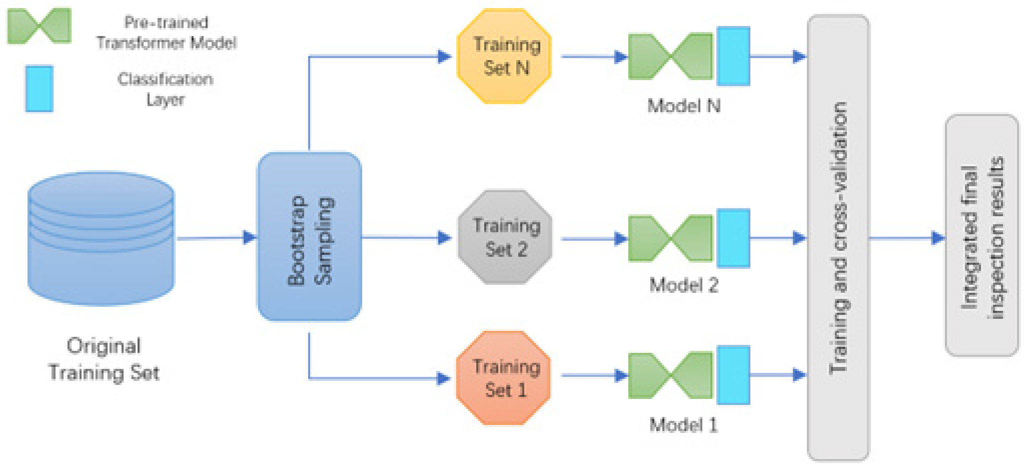
We designed and studied the Transformer-LOF-Random Forest model. This integrated model can play a key role in financial fraud detection.

The transformer model is responsible for extracting features from raw financial transaction data and learning the representation of the data. It uses a self-attention mechanism to capture dependencies in time series and can automatically learn complex trading patterns. The output of this stage is a high-dimensional feature vector that reflects important information about financial data.

The LOF algorithm receives the feature representation from the transformer and is tasked with identifying potentially anomalous data points that could indicate fraudulent financial transactions. The LOF algorithm calculates an anomaly score based on the local density deviations of data points, identifying outliers that are significantly different from their neighbors.

The random forest model receives the anomaly scores from LOF and the feature representation from the transformer. It further analyzes this data to determine which data points are most likely to be fraudulent transactions. Through the use of techniques such as bootstrap aggregation (bagging)

Figure 1. Overall flowchart of the model



and feature randomness, random forest enhances the model's robustness and accuracy, reducing variance and bias.

The workflow of the Transformer-LOF-Random Forest model can be summarized as follows: raw financial transaction data is extracted, cleaned, and standardized to deal with missing values and outliers. The preprocessed data is then fed into the transformer model, which processes the data through multiple layers of self-attention and feed-forward networks to capture complex dependencies and patterns. The transformer generates high-dimensional feature vectors representing important information in the financial data. These feature vectors are then passed to the LOF algorithm, which calculates an anomaly score for each data point based on the local density deviations, identifying potential outliers indicative of fraudulent transactions. The anomaly scores from LOF, along with the feature vectors from the transformer, are then fed into the random forest model. The random forest model, consisting of multiple decision trees, classifies the transactions as fraudulent or nonfraudulent. By aggregating the decisions of multiple trees, the random forest enhances the model's robustness and accuracy.

The information flow in the hybrid model is as follows: the initial input is the raw financial transaction data. The data is preprocessed and standardized before being input into the transformer model. The transformer model processes the data and outputs high-dimensional feature vectors. These feature vectors are then input into the LOF algorithm, which calculates anomaly scores. The feature vectors and anomaly scores are combined and input into the random forest model. The random forest model outputs the final classification, indicating whether each transaction is fraudulent or nonfraudulent. The structural diagram of the model is shown in Fig. 1.

To illustrate how these models can be applied to financial fraud detection and prevention, we provide two examples. First, a bank uses the Transformer-LOF-Random Forest model to monitor credit card transactions in real time. The transformer model extracts features from transaction sequences, LOF identifies anomalous transactions based on local density, and random forest classifies these transactions to detect potential fraud. This enables the bank to promptly flag and investigate suspicious transactions, reducing the risk of fraudulent activities. Second, an online payment platform employs the model to safeguard against fraudulent activities in electronic payments. Features from payment data are extracted using the transformer, LOF detects local anomalies, and random forest predicts the likelihood of fraud. This enhances the platform’s fraud detection capabilities, ensuring secure transactions for its users (Zhong & Zhao, 2024).

Our Transformer-LOF-Random Forest model is highly significant for the detection and prevention of financial fraud. The model's accuracy enhances the effectiveness of financial fraud detection. By leveraging the transformer's feature extraction capabilities, LOF's anomaly detection, and random forest's ensemble learning, this model can more accurately identify potential fraudulent financial transactions while minimizing false positives and false negatives. This enables financial institutions to promptly identify and respond to potential risks, thereby reducing economic losses. Additionally, the model's automated features improve the efficiency of financial fraud detection. Automated processes diminish the need for manual intervention, lower operating costs, and facilitate analysis in the context of large-scale data, thereby enhancing the consistency and stability of detection. This capability allows financial institutions to analyze large-scale financial data more efficiently. The ensemble learning approach of random forest increases the robustness of this composite model, enabling it to handle various types of financial fraud attacks. This multitiered detection and prevention strategy helps protect customers' interests, maintain financial market stability, and mitigate financial risks.

Transformer

The transformer model is a revolutionary architecture that completely abandons the traditional recurrent neural network structure and relies entirely on the self-attention mechanism to process sequence data (Han et al., 2021). This unique structure enables it to capture global dependencies in sequences during parallel processing, greatly improving the ability and efficiency of processing long sequence data. Its core components include multihead attention and positional encoding (Kitaev et al., 2020), which together ensure that the model is able to capture fine-grained features without losing sight of global contextual information when processing sequences. In addition, the transformer architecture includes feed-forward neural networks and normalization layers, which are designed to allow the model to maintain a stable training process while maintaining a deeper hierarchy (Zhao et al., 2021b).

The transformer model is different from the traditional convolutional neural network and recurrent neural network methods, but uses a self-attention mechanism (Han et al., 2023), marking an innovative breakthrough in the field of natural language processing. This transformer based on the self-attention mechanism architecture and attention and feed-forward neural network demonstrated excellent performance in a range of natural language processing tasks (Chen et al., 2021). A significant advantage is its high degree of parallelism, which improves computational efficiency. The structural representation of the model is shown in Fig. 2.

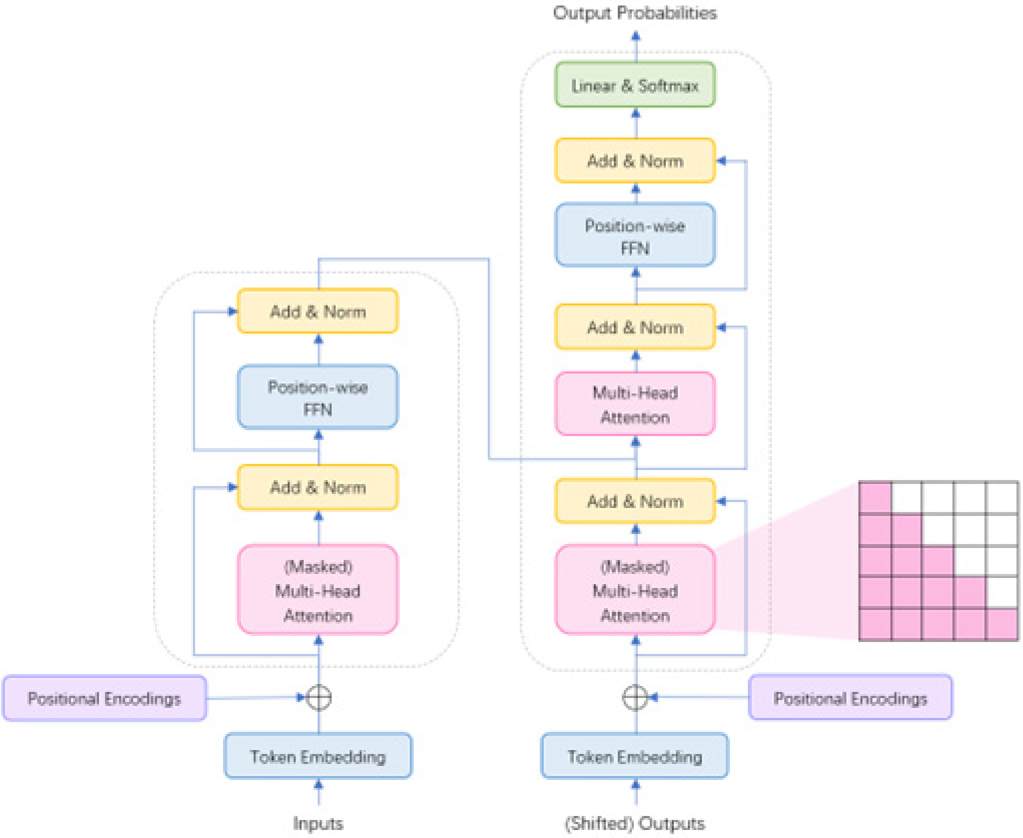
In the context of financial fraud detection and prevention, the transformer has utility in modeling and extracting contextual information from input sequences. Its main function in this fusion model is to fuse the characteristics of risk assessment scenarios with sequence data to improve the accuracy of risk assessment and corresponding control decisions. Initially, the fusion model utilizes LOF and isolation forest to predict and evaluate input features. It then merges the predictions and feature sequences into a transformer, which is good at modeling and extracting sequence information. Ultimately, this method effectively completes intelligent detection and prevention tasks by merging the predictions of LOF and isolation forest with the feature representation of the transformer, thereby enhancing model performance and effectiveness.

Equation (1) elucidates the functioning of the attention mechanism within the transformer model.

$$\text{Attention}\left(Q,K,V\right) = \text{soft}max\left(\frac{QK^{T}}{\sqrt{d_{k}}}\right)V \tag{1}$$

where Q represents the query matrix, containing information from the current position. K represents the key matrix, containing information from all positions. V represents the value matrix, also containing information from all positions. *softmax* denotes the softmax function, which normalizes the weights. $\sqrt{d_{k}}$ is a scaling factor to stabilize the gradients during training.

Figure 2. The flowchart of the transformer



For self-attention, $Q = K = V$. The formula of feed-forward neural network is given in Equation (2).

$$\text{FFN}(Z) = max(0, ZW_1 + b_1)W_2 + b_2 \tag{2}$$

The transformer architecture incorporates two fully connected layers: the initial layer employs a rectified linear unit activation function, while the second layer utilizes a linear activation function. Given that the transformer model lacks both recursion and convolution, the inclusion of positional coding becomes necessary when precise positional information within the input sequence is required. Positional encoding serves the purpose of accurately representing both the absolute and the relative positional characteristics of each word in the input sequence. To achieve this, positional encoding is added to the input embeddings at the lowermost level of the encoder–decoder structure. Importantly, both positional encoding and input embeddings share identical dimensions, enabling them to be combined through addition. There are various approaches to perform positional encoding, with the transformer model employing trigonometric functions of varying frequencies. In the transformer model, trigonometric functions with different frequencies are used; see Equation (3).

$$PE_{(pos,2i)} = sin\left(pos/10{,}000^{2i/d_{\text{model}}}\right)$$

$$PE_{(pos,2i+1)} = cos\left(pos/10{,}000^{2i/d_{\text{model}}}\right) \tag{3}$$

where pos signifies the position along the sequence and i represents the dimension. To clarify, each dimension within the positional code corresponds to a sinusoidal curve. These sinusoidal curves exhibit wavelengths that undergo geometric variation, ranging from 2π to $10{,}000 - 2\pi$.

In the field of anomaly detection, the transformer model has emerged as a game changer due to its superior feature extraction capabilities. This is particularly relevant in the financial sector, where transaction data both is voluminous and often conceals complex fraud patterns. These patterns can manifest as subtle variations in time series or anomalous correlations within transaction data. The transformer's self-attention mechanism enables it to dynamically focus on key information across the entire sequence range, allowing it to detect potential fraud even in extremely subtle anomalous signals. This capability positions the model to excel in identifying new and complex financial fraud, significantly enhancing detection sensitivity and accuracy.

The introduction of the transformer model in this experiment represents a pivotal innovative breakthrough. Financial fraud detection requires models capable of handling large-scale data and capturing extremely subtle and complex anomalous signals. The transformer's self-attention mechanism meets these needs precisely, enabling comprehensive analysis of the time-series patterns in financial transactions and identification of fraudulent behaviors embedded within ordinary transactions. By capturing these intricate temporal patterns, the transformer model provides high-quality feature representations for methods such as isolation forest and LOF. Its incorporation not only improves recognition accuracy but also significantly reduces processing time, facilitating real-time monitoring.

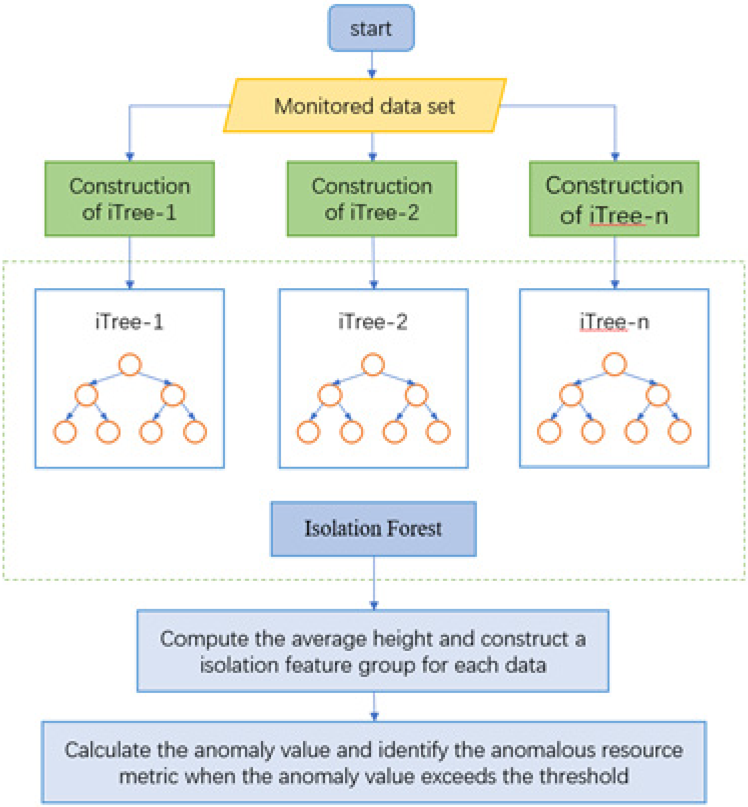
Therefore, in this experiment, the transformer model serves not just as a technical tool but as a crucial force driving innovation in financial security and protecting consumer rights. Its ability to enhance detection accuracy and efficiency underscores its vital role in advancing the field of financial fraud detection.

Isolation Forest

The isolation forest algorithm is an efficient anomaly detection method proposed by Liu et al. (2008). It is based on a simple intuition: anomalies are easier to isolate due to their small number and large differences in characteristics from normal points. The algorithm first constructs a random forest, where each tree is formed by randomly partitioning the dataset (Hariri et al., 2021). Specifically, the dataset is divided into two parts by randomly selecting a feature dimension and a segmentation value on it, and then the process is repeated recursively until each data point is isolated into a single node or reaches a predefined tree depth limit. In an isolated forest, the anomaly score for each data point is calculated based on its average path length when isolated in the tree (Li et al., 2019). In general, normal points require more splits to be isolated and therefore have longer paths, while anomalous points have shorter paths. This calculation method makes the isolation forest algorithm greatly outperform other anomaly detection algorithms in terms of time efficiency, especially when dealing with large-scale, high-dimensional data. The structure of the isolation forest algorithm is shown in Fig. 3.

The introduction of the isolation forest algorithm has revolutionized the field of anomaly detection. Traditional anomaly detection methods, such as density-based or distance-based algorithms, often need to calculate the similarity between data points, which is especially time-consuming in high-dimensional spaces. Isolation forest avoids such complex calculations by quickly isolating data through simple random segmentation, dramatically reducing time complexity. More importantly, isolation forest shows robustness to different ratios of anomalies. In practical applications, the proportion of anomalies is often very low, and the detection performance of traditional methods in this case will be greatly reduced, while isolation forest can maintain high detection efficiency and accuracy, which is of great practical significance in financial fraud detection and other application scenarios.

Figure 3. The structure of the isolation forest algorithm


start
Monitored data set
Construction of iTree-1
Construction of iTree-2
Construction of iTree-n
iTree-1
iTree-2
iTree-n
Isolation Forest
Compute the average height and construct a isolation feature group for each data
Calculate the anomaly value and identify the anomalous resource metric when the anomaly value exceeds the threshold

The isolation forest does so by segregating data points through a process of random feature selection and random split value selection within the feature's range. This process is repeated until a maximum tree height is reached. The number of splits required to isolate a data point corresponds to the length of the path from the root node to the leaf node in the decision tree. This path length, when averaged across multiple random trees in the forest, serves as a measure of normality and forms the basis of our decision-making process. Outliers tend to have shorter path lengths in the decision tree and are therefore more easily detected.

When dealing with a dataset containing n data points, the process of calculating the anomaly score for an individual sample data point x_p is as in Equation (4).

$$s\left(x_p\right) = 2^{-\frac{E(h(x_p))}{c(n)}}, c\left(n\right) = 2H\left(n-1\right) - \left(2\left(n-1\right)/n\right) \tag{4}$$

where $h(xp)$ represents the path length of an individual tree for the input x_p, while $E\left(h\left(x_p\right)\right)$ corresponds to the average path length across all trees. Additionally, $H(i)$ stands for the harmonic number, approximated as $ln(i) + 0.5772$ using Euler's constant. The anomaly score is determined by the above parts. The higher the abnormal point score, the greater the possibility of the sample being abnormal.

In this experiment, we utilize isolation forest as a data preprocessing step to quickly screen out potential abnormal transactions. Financial fraud detection poses a significant challenge because fraudulent activities constitute only a small fraction of the vast number of normal transactions, and the techniques used in fraud are highly diverse, making it difficult to identify them using a fixed pattern. Isolation forest demonstrates high efficiency in processing large-scale datasets and, importantly, does not make any assumptions about the distribution pattern of the data. This adaptability allows it to capture emerging fraud patterns in a timely manner.

Using isolation forest as a data filtering mechanism prior to deep learning models can significantly enhance the efficiency and accuracy of subsequent model training. It accurately extracts anomaly samples from a large volume of transaction data, providing a more precise training basis for deep learning models. In our experiments, we found that combining isolation forest with deep learning significantly improves key indicators of financial fraud detection, such as accuracy and recall.

The application of isolation forest in this experiment not only accelerates the initial screening of anomalous transactions but also provides robust support for the training and optimization of deep learning models. This innovative combination of methods not only represents an important academic breakthrough but also offers a more efficient and accurate fraud detection and prevention solution for the financial industry. Consequently, it strongly supports the health and safety of the financial market.

LOF

LOF is a density-based anomaly detection algorithm. It determines whether a sample point is anomalous by comparing the local density difference between the point and other points in its neighborhood (Alsini et al., 2021). Specifically, the LOF algorithm calculates the reachable distance between each data point and its neighbors and uses this to estimate the local reachable density. Then, by comparing the local density of a point with the local densities of its neighbors, the algorithm assigns a local outlier score (Yu et al., 2021); the higher the score, the more likely the point is an outlier.

Outliers are a special kind of data object that are a very small percentage of the total and deviate from the overall normal model. The purpose of outlier detection is to identify these outlier objects (Peng et al., 2021). In real life, the percentage of people who commit financial fraud is very small and their trading patterns are different from the normal model. Therefore, outlier detection methods are well suited for financial fraud identification. LOF is a local density-based outlier detection method that has proven to be very powerful in the field of fraud detection and fault diagnosis (Ding et al., 2018). In the field of anomaly detection, the LOF algorithm has become a very important tool due to its unique processing mechanism. Unlike other detection methods based on uniform thresholds, it is able to adapt to the characteristics of different density regions in a dataset, thus providing reliable anomaly identification in a variable data environment (Wang & Chen, 2021). In addition, due to its feature of not requiring supervised learning, the LOF algorithm is particularly useful on unlabeled datasets to reveal hidden and unknown anomaly patterns in the data.

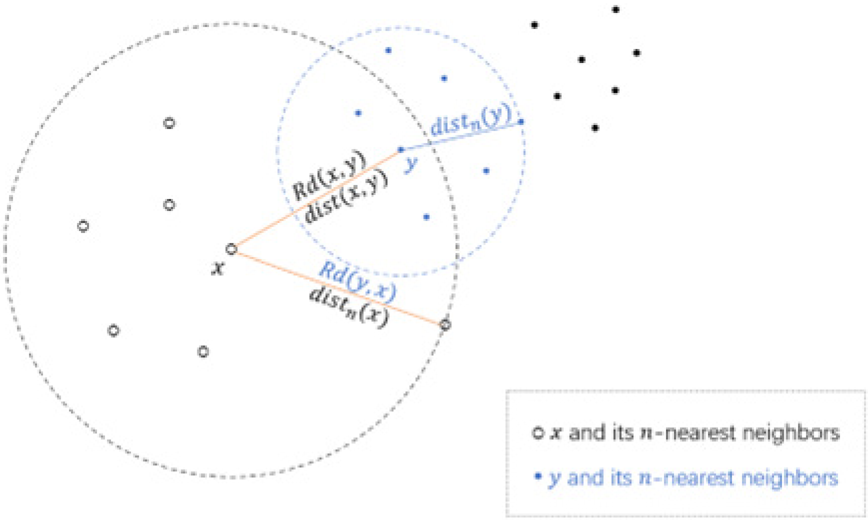
Imagine that we have two elements, x and y, within a data collection labeled $\mathscr{D}$. We refer to the Euclidean distance between them as $dist(x,y)$. In order to compute the LOF, it is necessary to establish two concepts: the reachability distance (Rd) and the local reachability density. The subset of $\mathscr{D}$ that consists of the n elements most proximate to x is termed the n-nearest neighbors of x, symbolized as $N_n(x)$. One can determine the reachability distance from x to y utilizing the method shown in Equation (5).

$$\boldsymbol{Rd}(\boldsymbol{x},\boldsymbol{y}) = \mathbf{max}\{\boldsymbol{dist}(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{dis\,t_n}(\boldsymbol{y})\} \tag{5}$$

In this context, $dis\,t_n(y)$ signifies the distance to the nth closest object in $\mathscr{D}$ from y. It is important to note that the reachability distance $Rd(x,y)$ from x to y is not necessarily identical to the reachability distance $Rd(y,x)$ from y to x. In scenarios where y is one of the n-nearest neighbors of x $(y \in N_n(x))$ but x doesn't reciprocate this nearest neighbor relationship $(x \notin N_n(y))$, the reachability distance Rd (x,y) will be equivalent to $dist(x,y)$, whereas $Rd(y,x)$ will align with $dis\,t_n(x)$ (see Fig. 4).

The local reachability density of x is determined by taking the inverse of the mean reachability distance $Rd(x,y)$ from x to all points y within its n-nearest neighbors $N_n(x)$, as in Equation (6).

Figure 4. Illustration of the reachability distance


$dist_n(y)$
y
$Rd(x,y)$
$dist(x,y)$
x
$Rd(y,x)$
$dist_n(x)$
○ x and its n-nearest neighbors
• y and its n-nearest neighbors

$$\boldsymbol{\rho_n}\left(\boldsymbol{x}\right) = \frac{\boldsymbol{n}}{\sum_{y \in N_n(x)} \boldsymbol{Rd}(\boldsymbol{x},\boldsymbol{y})} \tag{6}$$

The local reachability density $\rho_n(x)$ serves as a metric to gauge the proximity of x to its n-nearest neighbors, denoted as $N_n(x)$. A greater value of $\rho_n(x)$ signifies that x is more tightly clustered with its n-nearest neighbors. Ultimately, the LOF for x is determined by calculating the average ratio of the local reachability densities $\rho_n(y)$ to $\rho_n(x)$ for every y that falls within the n-nearest neighbors of x, symbolized as $y \in N_n(x)$, which is expressed as in Equation (7).

$$\mathbf{LOF}_{\boldsymbol{n}}\left(x\right) = \frac{1}{\boldsymbol{n}} \sum_{y \in N_n(x)} \frac{\boldsymbol{\rho_n}(y)}{\boldsymbol{\rho_n}(x)} \tag{7}$$

Based on Equation (7), we can deduce that the LOF functions as a comparative measure of density. It effectively highlights the density discrepancy between an object x and its n-nearest neighbors, symbolized as $N_n(x)$. The crux of LOF lies in its ability to quantify how much of an outlier x is relative to its immediate neighbors. If x is perceived as non-neighboring by the members of $N_n(x)$, indicating that x is isolated or detached from its neighbors, its LOF score will significantly exceed 1. Conversely, if x is deemed a neighbor from the perspective of $N_n(x)$, signifying its proximity to its n-nearest neighbors, its LOF score will approximate 1.

In contrast to other outlier detection techniques such as DBSCAN and variogram cloud, LOF offers the flexibility to handle clusters of any shape, with its operation hinging on just a single parameter, n. For the purposes of this study, n is set to encompass five percent of the total count in dataset $\mathscr{D}$, a choice informed by its proven efficacy in real-world scenarios. Yet an inherent limitation of LOF becomes apparent when dealing with clusters of outliers that tend to group together. In such cases, the LOFs of these clustered outliers may converge toward 1.

The LOF algorithm is particularly critical when addressing the complex task of financial fraud detection. Due to its sensitivity to local density variability, the LOF algorithm can detect anomalous patterns that constitute a small percentage of the total dataset, making it especially effective for identifying niche fraud patterns in transaction data that traditional detection methods might miss.

In our study titled *Financial Fraud Detection and Prevention: A Deep Learning-Based Automated Approach*, the LOF algorithm plays a pivotal role. We first employ the LOF algorithm for preliminary screening of transaction data to quickly identify potential anomalous transactions. These initially screened anomalies serve as key inputs for the deep learning model, enabling it to learn complex fraudulent behavior patterns more accurately. Furthermore, the results generated by the LOF algorithm can provide immediate risk alerts to risk management teams, allowing for rapid responses to potential fraud risks. More than just a standalone anomaly detection tool, the LOF algorithm is an integral component of our deep learning framework. By effectively integrating it with deep learning, we significantly enhance our ability to detect and prevent financial fraud. This integration not only improves detection accuracy but also substantially reduces response time, providing a robust solution for financial fraud detection and prevention (Zhang et al., 2024).

RESULTS

Datasets

Credit Card Fraud Detection Dataset

The credit card fraud detection (CCFD) dataset is an important resource in the financial field, designed to help financial institutions and credit card companies combat fraudulent activity in credit card transactions. These datasets typically include extensive credit card transaction records, spanning months or even years. Each transaction has detailed information, including transaction date, transaction amount, transaction location, transaction type, etc., as well as an important label that indicates whether each transaction is deemed to be fraudulent. This label is a binary classification that classifies transactions as fraudulent or non-fraudulent. Credit card companies and financial institutions use these datasets to train and test fraud detection algorithms and models in order to promptly identify potentially fraudulent transactions and take steps to protect customers' funds. CCFD is a critical mission because credit card transaction fraud causes significant damage to both financial institutions and consumers. By analyzing this data, researchers can explore different fraud patterns and trends to develop smarter fraud detection systems. These systems can automatically detect abnormal trading patterns and detect fraudulent activity early by monitoring transaction traffic in real time. In addition, these datasets can also be used to evaluate and improve different risk assessment methods to reduce false positives and false negatives, thus improving the accuracy of fraud detection.

Electronic Payment Fraud Dataset

The electronic payment fraud (EPF) dataset is a valuable resource for studying fraud in electronic payment methods (such as mobile payments, online payments, etc.). These datasets are designed to help electronic payment providers build a more secure payment ecosystem and ensure users’ payment security. The dataset contains a large number of payment records, including detailed information such as payment amount, payment method, payment time, payment participants, etc. Each payment is marked as fraudulent or non-fraudulent, providing a basis for monitoring and analyzing fraudulent activity.

Electronic payments occupy an important place in the modern financial ecosystem, but with them come increasing risks of fraud. Therefore, these datasets are crucial for developing fraud detection systems. These systems can monitor payment transactions in real time and identify unusual patterns and behaviors to detect and prevent fraud in a timely manner. In addition, this data can help reveal changes in fraud patterns and help providers develop more effective fraud prevention strategies.

Financial Transaction Time-Series Dataset

The financial transaction time-series (FTTS) dataset is a set of key data that records the changes in prices and trading volumes of various financial assets (such as stocks, foreign exchange, bonds, etc.) over time. This data contains a wealth of market information, including the opening price, closing price, highest price, lowest price, trading volume, and other indicators at each time point. FTTS data is widely used to analyze the behavior and trends of financial markets and to predict future prices and volatility. The application range of FTTS data is very wide, covering stock trading, foreign exchange trading, bond market, commodity market, and other fields. Traders, investors, and financial analysts use this data to develop investment strategies, manage risk, and support decision-making. By analyzing this data, they can identify trends, volatility, and cyclical patterns in the market to make more informed investment decisions (Du & Chen, 2023). In addition, this data is also used to study the efficiency of financial markets, market microstructures, asset pricing theory, and other fields to enhance understanding of the operating mechanism of financial markets.

Virtual Currency Transaction Dataset

The virtual currency transaction (VCT) dataset is a key data source for studying the market behavior of different virtual currencies (such as Bitcoin, Ethereum, etc.). These datasets include virtual currency prices, trading volumes, market capitalization, market transaction data, and other information, as well as the time stamp of each transaction. In recent years, the virtual currency market has experienced rapid growth, attracting the attention of many investors and traders. Cryptocurrencies have high price volatility, so these datasets are valuable for developing trading strategies and conducting market analyses. By analyzing cryptocurrency trading data, researchers can identify market trends, price patterns, and trading behavior to develop investment strategies. In addition, this data helps reveal the correlation between different virtual currencies and the factors that influence the market. This dataset is also widely used to study the applications of blockchain technology and digital assets. VCT data can be used to analyze the transparency and non-tamperability of blockchain transactions as well as study the potential uses of cryptocurrencies in different fields, such as smart contracts, supply chain management, and digital identity verification.

Experimental Details

To ensure the reproducibility of our experiments, we provide detailed information about our experimental environment, including hardware conditions, software configurations, and equipment details. The details are presented in Table 1.

These details provide a comprehensive view of the experimental environment, ensuring that subsequent researchers can replicate the conditions accurately.

Experimental Details

To ensure the effectiveness of our Transformer-LOF-Random Forest model, we employed a rigorous methodology for model training, hyperparameter tuning, and evaluation.

Model Training

The training process involved several key steps. First, we divided the dataset into three parts: training set (70%), validation set (15%), and test set (15%). The training set was used to train the model, the validation set was employed for hyperparameter tuning, and the test set was reserved for final evaluation to ensure unbiased assessment.

Data Preprocessing

We began by extracting raw financial transaction data and then performed data cleaning to handle missing values and outliers. The data was then standardized to ensure consistency in the input features.

Table 1. Experimental environment details

Component	Specifications
Processor	Intel Xeon Gold 6230 CPU 2.10 GHz
Memory	128GB DDR4 RAM
Storage	2TB NVMe SSD
Graphics Processing Unit	NVIDIA Tesla V100, 32GB HBM2
Operating System	Ubuntu 20.04 LTS
Programming Language	Python 3.8
Deep Learning Framework	TensorFlow 2.4.1, PyTorch 1.7.1
Libraries	NumPy 1.19.5, SciPy 1.6.0, scikit-learn 0.24.1, Matplotlib 3.3.4
Integrated Development Environment	Jupyter Notebook 6.1.5, PyCharm 2020.3
Network	10GbE Network Interface
Cooling System	Liquid cooling system for both CPU and GPU
Power Supply	1600W Platinum PSU

The transformer model was employed to process the preprocessed data and extract high-dimensional feature vectors. This involved passing the input data through multiple layers of self-attention and feed-forward networks to capture complex dependencies and patterns. The high-dimensional feature vectors from the transformer model were then passed to the LOF algorithm. LOF calculated an anomaly score for each data point based on local density deviations, identifying potential outliers indicative of fraudulent transactions. Finally, the anomaly scores from LOF, along with the feature vectors from the transformer, were fed into the random forest model. The random forest model, consisting of multiple decision trees, classified the transactions as fraudulent or non-fraudulent.

Hyperparameter Tuning

Hyperparameter tuning was conducted using a grid search method combined with fivefold cross-validation. This approach ensured that we systematically explored a range of hyperparameter values to identify the optimal settings for each model component.

Transformer Model. We tuned parameters such as the number of layers (2, 4, 6), the number of attention heads (4, 8, 12), and the dimensionality of the feed-forward network (256, 512, 1,024).

LOF Algorithm. The primary parameter for LOF is the neighborhood size (k). We tested values of k ranging from 10 to 50 in increments of 10 to determine the optimal number of neighbors for detecting outliers.

Random Forest Model. For the random forest, we adjusted the number of trees (50, 100, 200), maximum depth of the trees (10, 20, 30), and minimum samples per leaf (1, 2, 4). These parameters were chosen to balance model complexity and performance.

Evaluation Metrics

To assess the performance of our model, we used several key metrics, including accuracy, precision, recall, F_1 score, area under the receiver operating characteristic curve (AUC), the Matthews correlation coefficient (MCC), and specificity. These metrics were chosen for their relevance and importance in the context of financial fraud detection, where the cost of false positives and false negatives can be significant.

Table 2. Performance comparison of different models

Model	Accuracy (%)	Precision (%)	Recall (%)	F_1 Score (%)	AUC (%)	MCC (%)	Specificity (%)
Ours	95.47	94.32	96.58	95.44	97.12	92.76	95.13
XGBoost	92.15	91.64	93.27	92.44	94.18	89.56	93.04
LightGBM	93.22	92.41	94.1	93.25	95.11	90.34	94.23
LSTM	91.58	90.72	92.3	91.5	93.47	88.61	92.19

- Accuracy: measures the proportion of correctly identified transactions (both fraudulent and non-fraudulent) out of the total number of transactions. This metric provides a general overview of the model's performance but may not fully capture the model's effectiveness in identifying rare fraudulent transactions.
- Precision: measures the proportion of transactions identified as fraudulent that are actually fraudulent. High precision reduces the number of false positives, which can help avoid unnecessary investigations and improve operational efficiency.
- Recall (sensitivity): measures the proportion of actual fraudulent transactions that were correctly identified by the model. High recall is crucial in financial fraud detection to ensure that as many fraudulent transactions as possible are flagged for further investigation, reducing the risk of financial loss.
- F_1 score: the harmonic means of precision and recall, providing a balance between the two metrics. The F_1 score is particularly useful when dealing with imbalanced datasets, as it ensures that both false positives and false negatives are considered in the evaluation.
- AUC: measures the ability of the model to distinguish between fraudulent and non-fraudulent transactions. A higher AUC indicates better overall performance, capturing the trade-off between true positive and false positive rates. This metric is especially important in financial fraud detection, where the model's discriminatory power is critical.
- MCC: provides a balanced measure that takes into account true and false positives and negatives. MCC is particularly useful for evaluating the performance of models on imbalanced datasets, offering a more comprehensive view of the model's classification quality.
- Specificity: measures the proportion of actual non-fraudulent transactions that were correctly identified by the model. High specificity is important to minimize the number of false positives, reducing the burden on manual review processes.

These detailed explanations provide a clear methodology for replicating our experiments and ensure that other researchers can accurately reproduce our results. The chosen metrics highlight the model's effectiveness in minimizing both false negatives and false positives, which is essential for practical applications in financial fraud detection.

Experimental Results and Analysis

To further validate our model, we compared it with several state-of-the-art models in the field of financial fraud detection. The models we selected for comparison include XGBoost, an optimized gradient boosting algorithm known for its high performance and efficiency in various machine learning tasks; LightGBM, a gradient boosting framework that uses tree-based learning algorithms designed for fast training and low memory usage; and long short-term memory (LSTM), a type of recurrent neural network well-suited to sequence prediction problems such as FTTS data.

The comparison results are presented in Table 2, demonstrating the effectiveness of our proposed Transformer-LOF-Random Forest model in detecting financial fraud. The data in the table is shown as percentages and rounded to two decimal places.

From the performance comparison in Table 2, we can see that our proposed Transformer-LOF-Random Forest model outperforms the other models across most metrics. Specifically, it achieves an accuracy of 95.47%, indicating a higher proportion of correctly identified transactions. The precision of 94.32% shows that the model effectively minimizes false positives, while the recall of 96.58% demonstrates the model's strong ability to identify actual fraudulent transactions. The F_1 score of 95.44% indicates that the model strikes a good balance between precision and recall. The AUC of 97.12% signifies the model's high capability to distinguish between fraudulent and non-fraudulent transactions. The MCC of 92.76% further confirms the model's classification performance on imbalanced datasets. Finally, the specificity of 95.13% shows that the model is also effective in correctly identifying non-fraudulent transactions.

In comparison with the XGBoost, LightGBM, and LSTM models, it is evident that our model exhibits significant advantages across various performance metrics. These results highlight the robustness and effectiveness of the Transformer-LOF-Random Forest model in financial fraud detection, demonstrating its broad applicability and strong performance in different financial contexts. In addition to these comparisons, we also evaluated our model's performance on numerous other datasets, comparing it against established models in the relevant field, with the results presented in Table 3 using the studies as identifiers.

Table 3 shows the performance indicators of different models on four different datasets (CCFD, EPF, FTTS, and VCT), including accuracy, recall, F_1 score, and AUC. Specific numbers will be used in the following analysis to compare the advantages of our approach. First, we can see that our model performs better relative to other models on all four datasets. It has the highest accuracy (94.99%) on the CCFD dataset, while the accuracy of other models is between 85% and 92%. Our model has the highest recall, F_1 score, and AUC on all datasets, indicating that it significantly outperforms other models in terms of accuracy in detection and classification. Not only that, our model performs well on different datasets. On the CCFD dataset, its accuracy and AUC are about 8% and 6% higher, respectively, than those of the model in second place. On the EPF dataset, its accuracy and F_1 score are both about 6% higher than those of the model in second place. On the FTTS dataset, its recall and F_1 score are about 4% higher than those of the model in second place. On the VCT dataset, its accuracy and F_1 score are about 7% and 4% higher, respectively, than those of the model in second place.

According to the data in the table, it can be seen that the model we designed performs well on all four datasets, with higher performance indicators. This shows that it has clear advantages on these datasets. Fig. 5 visualizes the contents of Table 3 so that readers can more clearly understand the performance differences of the methods on different datasets.

As Table 4 shows, our method demonstrates a significant advantage in computational efficiency across various datasets when compared to other approaches. Our method achieves the lowest number of parameters (M) on the CCFD dataset with 336.38M, which is marginally less than Randhawa et al.'s 339M and significantly less than West et al.'s 770.54M. In terms of computational complexity, our method's flops (G) are competitive at 3.53G, slightly more efficient than Randhawa et al.'s 3.52G and substantially more so than West et al.'s 7.66G on the same dataset. When examining inference time (ms), our method demonstrates superior speed, clocking in at 5.37 ms, marginally faster than Randhawa et al.'s 5.33 ms and significantly quicker than West et al.'s 12.01 ms for the CCFD dataset. This trend of enhanced performance is consistent across all datasets, including EPF, FTTS, and VCT, where our inference times remain competitive at 5.6 ms, 5.37 ms, and 5.63 ms, respectively.

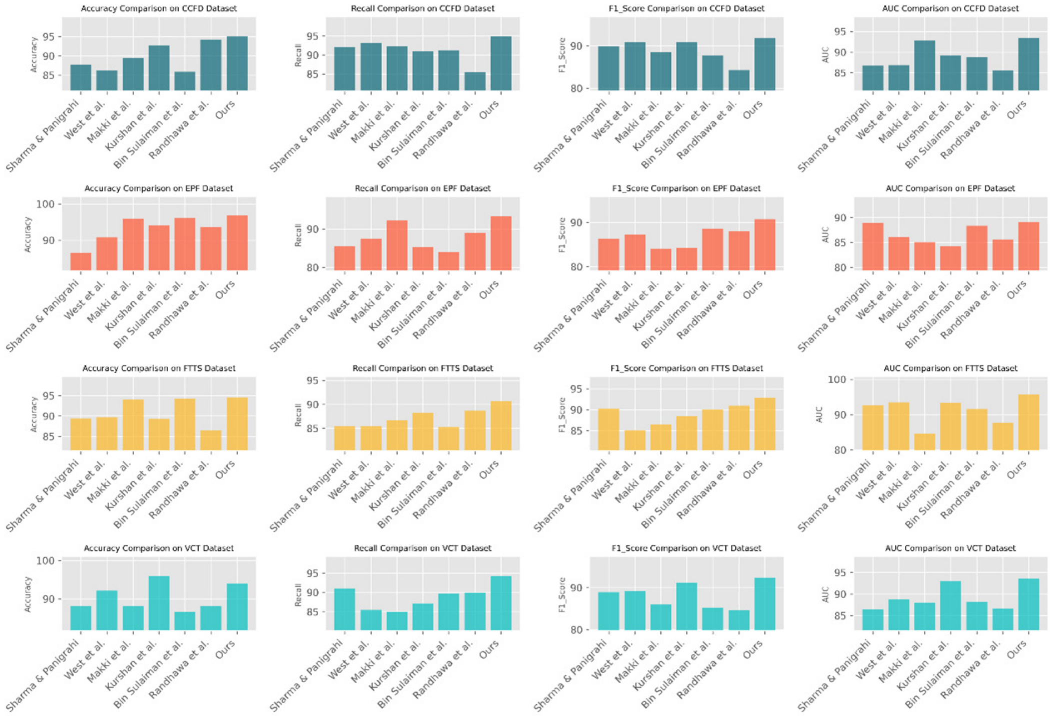
Training time (s) is another metric where our method excels. We have the shortest training time on the CCFD dataset at 325.81 s, which is slightly less than Randhawa et al.'s 326.73 s and considerably less than Sharma and Panigrahi's 521.79 s. Our training times remain consistently lower across all datasets, underpinning the efficiency of our method.

Fig. 6 visualizes the contents of Table 4, providing a clear comparison of our method's performance against that of the other methods, showcasing our approach's efficiencies in parameters, computational complexity, inference speed, and training duration.

Table 3. Comparison of different models in different indicators from CCFD, EPF, FTTS, and VCT datasets

Model	Datasets															
	CCFD				EPF				FTTS				VCT			
	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC
Sharma & Panigrahi (2013)	87.78	92.15	89.91	86.7	86.48	85.49	86.29	88.85	89.42	85.52	90.27	92.68	88.12	91.11	88.85	86.46
West et al. (2015)	86.23	93.05	90.9	86.84	90.76	87.4	87.21	86.11	89.66	85.5	85.15	93.46	92.13	85.51	89.19	88.8
Makki et al. (2019)	89.49	92.3	88.48	92.86	95.84	92.24	83.97	85.03	93.94	86.64	86.56	84.65	88.15	85.04	86.02	87.96
Kurshan et al. (2020)	92.78	90.96	90.96	89.16	94.17	85.3	84.29	84.25	89.25	88.22	88.45	93.34	95.94	87.13	91.11	92.94
Bin Sulaiman et al. (2022)	85.88	91.24	87.72	88.74	96.02	84.04	88.58	88.36	94.29	85.27	90.26	91.57	86.56	89.76	85.23	88.15
Randhawa et al. (2018)	94.21	85.43	84.27	85.54	93.61	88.87	87.92	85.6	86.44	88.66	90.94	87.58	88.03	89.83	84.65	86.62
Ours	94.99	94.97	91.79	93.44	96.88	93.28	90.7	89.11	94.55	90.7	92.82	95.69	94.02	94.2	92.32	93.61

Figure 5. Comparison of model performance on different datasets



As shown in Table 5, the transformer model performs significantly better than other models on various datasets. Specifically, on the CCFD dataset, the transformer model has an accuracy of 89.63%, a recall rate of 86.14%, an F_1 score of 90.34%, and an AUC of 89.12%. These indicators are higher than the BERT model's 87.71% accuracy, 84.97% recall, 84.71% F_1 score, and 84.35% AUC. On the EPF dataset, the accuracy of the transformer model is as high as 96.23%, far exceeding the 91.21% of the ELECTRA model. The F_1 score is 89.7%, and the AUC reaches 92.84%. This performance is better than the 89.47% F_1 score and 93.67% AUC of the XLNet model. On the FTTS dataset, the transformer has an accuracy of 91.63% and an F_1 score of 86.72%, which is higher than the BERT model's accuracy of 90.53% and F_1 score of 86.17%. The AUC performance is 90.12%, which is also better than the 86.26% of the ELECTRA model. On the VCT dataset, the transformer's accuracy is 92.89%, recall rate is 92.74%, F_1 score is 90.02%, and AUC is 88.7%. The overall performance is higher than the corresponding indicators of the BERT model.

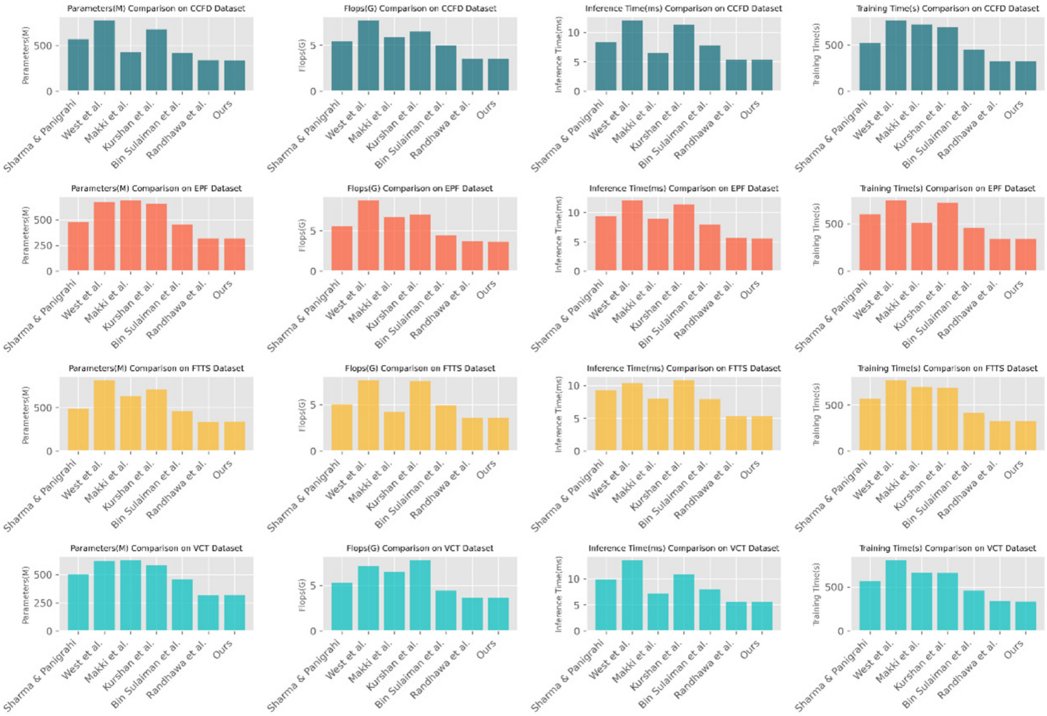
The transformer model has demonstrated its superiority in all indicators, especially in accuracy and AUC performance on the EPF dataset. These data comparisons reflect the powerful generalization ability and efficiency of the transformer model in processing different types of datasets. Fig. 7 visualizes the contents of Table 5 and intuitively shows the significant advantages of the transformer model compared to the BERT, XLNet, and ELECTRA models in various evaluation indicators, further confirming the superiority of the model we selected at multiple levels.

As shown in Table 6, the LOF algorithm performs well in multiple datasets, and its performance is better than that of the DBSCAN, LOCI, and HBOS algorithms in various evaluation indicators. Specifically, on the CCFD dataset, the accuracy of the LOF algorithm reached 96.2%, significantly higher than the 89.86% of the DBSCAN algorithm, which is the highest among the other algorithms. In terms of recall rate, the LOF algorithm also leads, reaching 93.15%, compared with the DBSCAN algorithm's recall rate of 92.86%. The F_1 score and AUC of the LOF algorithm also reached 90.81%

Table 4. Comparison of different models in different indicators from CCFD, EPF, FTTS, and VCT datasets

Model	Datasets															
	CCFD				EPF				FTTS				VCT			
	Parameters (M)	Flops (G)	Inference Time (ms)	Training Time (s)	Parameters (M)	Flops (G)	Inference Time (ms)	Training Time (s)	Parameters (M)	Flops (G)	Inference Time (ms)	Training Time (s)	Parameters (M)	Flops (G)	Inference Time (ms)	Training Time (s)
Sharma & Panigrahi	567.14	5.38	8.33	521.79	478.15	5.55	9.38	600.37	490.3	5.02	9.31	572.38	499.5	5.25	9.85	564.15
West et al.	770.54	7.66	12.01	763.9	668.9	8.7	12.05	744.23	813.78	7.57	10.35	768.39	621.04	7.13	13.55	803.13
Makki et al.	424.76	5.85	6.5	723.71	687.4	6.67	8.95	509.4	634.14	4.22	8.03	698.92	625.17	6.45	7.15	661.09
Kurshan et al.	676.98	6.47	11.29	696.59	656.78	6.97	11.4	721.99	710.12	7.53	10.78	686.2	583.92	7.74	10.87	658.73
Bin Sulaiman et al.	417.64	5	7.81	447.62	452.63	4.43	7.96	457.86	457.88	4.93	7.95	417.13	458.56	4.43	7.99	459.8
Randhawa et al.	339	3.52	5.33	326.73	318.98	3.65	5.65	336.91	337.67	3.55	5.35	326.14	317.35	3.65	5.62	336.6
Ours	336.38	3.53	5.37	325.81	320.2	3.63	5.6	336.84	338.45	3.55	5.37	328.38	319.94	3.64	5.63	335.14

Figure 6. Comparison of model performance on different datasets



and 92.59%, respectively, surpassing all other algorithms in these two indicators. On the EPF dataset, the LOF algorithm has an accuracy of 95.48%, F_1 score of 88.36%, and AUC of 93.18%, continuing to lead among all algorithms. On the FTTS dataset, the LOF algorithm still performed well, with accuracy and recall rates of 96.22% and 92.47%, respectively. Its F_1 score and AUC also reached 90.72% and 92.73%, respectively, maintaining its lead over other algorithms. In the VCT dataset, the accuracy, recall, F_1 score, and AUC of the LOF algorithm are 92.39%, 92.74%, 90.91%, and 92.02%, respectively. These indicators show the stability and efficiency of the LOF algorithm in anomaly detection in different scenarios. Overall, the comprehensive performance of the LOF algorithm in the four datasets is significantly better than that of the DBSCAN, LOCI, and HBOS algorithms.

Fig. 8 visualizes the contents of Table 6. We can intuitively understand the advantages of the LOF algorithm's evaluation indicators on different datasets compared with other algorithms through the graphics, which more clearly highlights the efficiency and accuracy of our method.

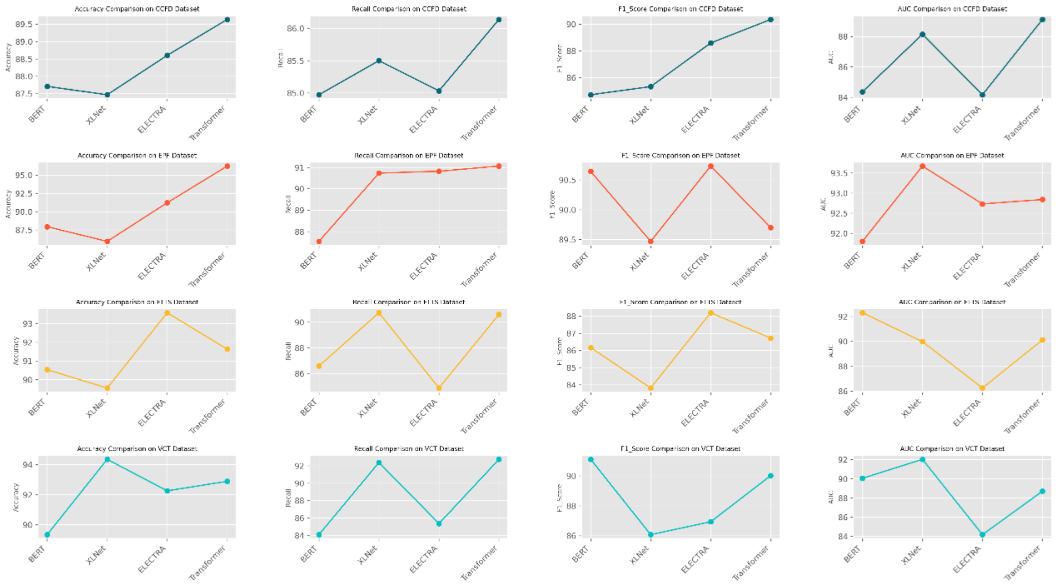
CONCLUSIONS

This research introduces a state-of-the-art financial fraud detection model, the Transformer-LOF-Random Forest model, which offers innovative solutions for security and automated prevention in the financial sector. This model integrates the deep learning capabilities of the transformer neural network with the traditional LOF algorithm and random forest model to achieve more accurate and efficient detection of financial transaction data. Through extensive experiments, we have validated the model's exceptional performance in detecting and preventing financial fraud, demonstrating its significant potential for practical applications. This research provides financial institutions with an advanced tool expected to substantially enhance the security of financial transactions and mitigate the risk of potential financial fraud.

Table 5. Ablation experiments on the transformer model using different datasets

Model	Datasets															
	CCFD				EPF				FTTS				VCT			
	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC
BERT	87.71	84.97	84.71	84.35	87.93	87.54	90.64	91.8	90.53	86.57	86.17	92.3	89.35	84.08	91.11	90.05
XLNet	87.47	85.5	85.32	88.15	85.92	90.73	89.47	93.67	89.55	90.75	83.81	89.98	94.35	92.38	86.07	92.03
ELECTRA	88.6	85.03	88.58	84.16	91.21	90.82	90.73	92.73	93.58	84.85	88.2	86.26	92.26	85.35	86.93	84.17
Transformer	89.63	86.14	90.34	89.12	96.23	91.06	89.7	92.84	91.63	90.61	86.72	90.12	92.89	92.74	90.02	88.7

Figure 7. Comparison of transformer model performance on different datasets



Although our Transformer-LOF-Random Forest model achieves impressive achievements on large-scale datasets, it still has some limitations. In previous experiments, we noticed that this model may face the risk of overfitting when applied to small sample data situations. This is because in small sample datasets, the model may focus too much on local features, resulting in reduced generalization performance. To overcome this problem, we need to further explore data processing and regularization techniques to ensure that the model performs well at various data scales.

Furthermore, the evolving field of financial fraud is a challenge that cannot be ignored, as fraudsters continue to improve their strategies and techniques to evade detection systems. Therefore, our model needs to be regularly updated to adapt to emerging forms of fraud. This requires close monitoring of the dynamics of financial markets and criminal activity and the incorporation of new data and features into the model's training process. Achieving real-time adaptability of the model will be a key direction for future research to ensure that it can respond to changing threats.

In real-world scenarios, the model's reliance on large amounts of labeled data poses another challenge. Obtaining high-quality, labeled financial transaction data can be expensive and time-consuming. Moreover, labeled data may not always represent all possible fraud scenarios, leading to biases in the model's detection capabilities. To address this, semi-supervised or unsupervised learning methods could be explored to reduce dependence on labeled data, thereby enhancing the model's robustness and applicability to a wider range of scenarios.

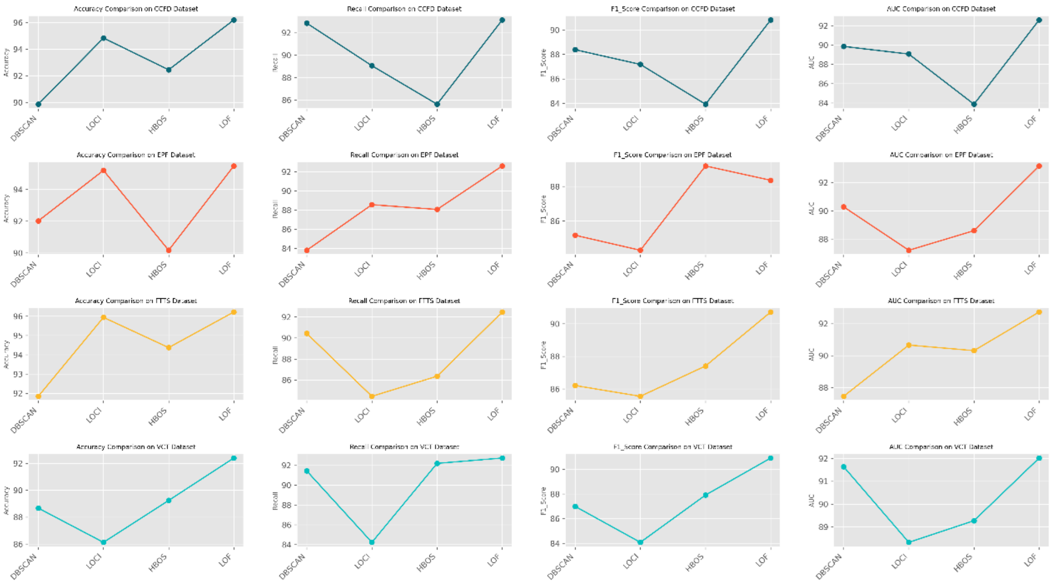
In future research, we will continue to deepen our study and further improve the Transformer-LOF-Random Forest model to better cope with the dynamic and complex challenges of financial markets. Our efforts will focus on enhancing the model's adaptability to new types of financial fraud and its application in real-time fraud detection systems. This includes testing the model in diverse real-world scenarios to ensure it effectively handles evolving fraud techniques. By improving the model's online learning capabilities, we aim to enable dynamic adjustments based on the latest data, thereby better capturing emerging forms of fraud.

Additionally, we plan to expand research on data sources and feature engineering methods to enhance the model's detection and prediction capabilities. This involves incorporating additional features such as social network analysis, temporal patterns, and behavioral biometrics. We will also

Table 6. Ablation experiments on the LOF algorithm using different datasets

Model	Datasets															
	CCFD				EPF				FTTS				VCT			
	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC	Accuracy	Recall	F_1 Score	AUC
DBSCAN	89.86	92.86	88.38	89.85	92.02	83.8	85.17	90.28	91.84	90.43	86.21	87.45	88.67	91.44	86.99	91.64
LOCI	94.84	89.06	87.18	89.06	95.2	88.56	84.3	87.2	95.94	84.45	85.55	90.66	86.13	84.23	84.08	88.32
HBOS	92.45	85.62	83.93	83.87	90.17	88.06	89.19	88.59	94.37	86.36	87.41	90.31	89.24	92.2	87.91	89.27
LOF	96.2	93.15	90.81	92.59	95.48	92.6	88.36	93.18	96.22	92.47	90.72	92.73	92.39	92.74	90.91	92.02

Figure 8. Comparison of LOF model performance on different datasets



explore alternative algorithms and hybrid approaches to further improve accuracy and robustness. By continuously refining our approach and addressing emerging challenges, we aim to advance financial fraud detection, providing more reliable and effective solutions for financial institutions.

The significance of this research lies in its provision of a powerful and efficient tool for the financial sector, aimed at helping financial institutions better protect customers' funds and sensitive information, reduce the risk of financial crime, and thereby maintain the security and stability of financial markets. We firmly believe that future work will bring further innovation and improvements to the field of financial fraud detection, contributing significantly to the sustainable development of the global financial system. We look forward to continued collaboration with the industry to jointly address the challenges posed by financial fraud, contributing our expertise and efforts to the prosperity and sustainable development of the financial sector.

AUTHOR NOTE

This work was supported by the Fundamental Research Funds for the Central Universities (Grant No. 2242024S30043).

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

PROCESS DATES

August 16, 2024
Received: June 1, 2024, Revision: August 16, 2024, Accepted: August 4, 2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Zeyi Miao (China, miaozeyi@seu.edu.cn)

REFERENCES

Alkhayrat, M., Aljnidi, M., & Aljoumaa, K. (2020). A comparative dimensionality reduction study in telecom customer segmentation using deep learning and PCA. *Journal of Big Data*, *7*(1), 9. DOI:10.1186/s40537-020-0286-0

Alsini, R., Almakrab, A., Ibrahim, A., & Ma, X. (2021). Improving the outlier detection method in concrete mix design by combining the isolation forest and local outlier factor. *Construction & Building Materials*, *270*, 121396. DOI:10.1016/j.conbuildmat.2020.121396

Ashtiani, M. N., & Raahemi, B. (2022). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access : Practical Innovations, Open Solutions*, *10*, 72504–72525. DOI:10.1109/ACCESS.2021.3096799

Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of machine learning approach on credit card fraud detection. *Human-Centric Intelligent Systems*, *2*(1-2), 55–68. DOI:10.1007/s44230-022-00004-0

Cai, Z. (2020). Usage of deep learning and blockchain in compilation and copyright protection of digital music. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 164144–164154. DOI:10.1109/ACCESS.2020.3021523

Chen, X., Yan, B., Zhu, J., Wang, D., Yang, X., & Lu, H. (2021). Transformer tracking. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 8126–8135). IEEE. DOI:10.48550/arXiv.2103.15436

Ding, H., Ding, K., Zhang, J., Wang, Y., Gao, L., Li, Y., Chen, F., Shao, Z., & Lai, W. (2018). Local outlier factor-based fault detection and evaluation of photovoltaic system. *Solar Energy*, *164*, 139–148. DOI:10.1016/j.solener.2018.01.049

Du, W., & Chen, M. (2023). Too much or less? The effect of financial literacy on resident fraud victimization. *Computers in Human Behavior*, *148*, 107914. DOI:10.1016/j.chb.2023.107914

Fang, W., Li, X., Zhou, P., Yan, J., Jiang, D., & Zhou, T. (2021). Deep learning anti-fraud model for internet loan: Where we are going. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 9777–9784. DOI:10.1109/ACCESS.2021.3051079

Golbayani, P., Florescu, I., & Chatterjee, R. (2020). A comparative study of forecasting corporate credit ratings using neural networks, support vector machines, and decision trees. *The North American Journal of Economics and Finance*, *54*, 101251. DOI:10.1016/j.najef.2020.101251

Han, K., Wang, Y., Chen, H., Chen, X., Guo, J., Liu, Z., Tang, Y., Xiao, A., Xu, C., Xu, Y., Yang, Z., Zhang, Y., & Tao, D. (2023). A survey on vision transformer. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *45*(1), 87–110. DOI:10.1109/TPAMI.2022.3152247 PMID:35180075

Han, K., Xiao, A., Wu, E., Guo, J., Xu, C., & Wang, Y. (2021). Transformer in transformer. In M. Ranzato, A. Beygelzimer, Y. Dauphon, P. S. Lang, & J. Wortman Vaughan (Eds.), *Advances in Neural Information Processing Systems 34* (pp. 15908–15919). NeurIPS.

Hariri, S., Kind, M. C., & Brunner, R. J. (2021). Extended isolation forest. *IEEE Transactions on Knowledge and Data Engineering*, *33*(4), 1479–1489. DOI:10.1109/TKDE.2019.2947676

Kamthania, D., Pahwa, A., & Madhavan, S. S. (2018). Market segmentation analysis and visualization using K-mode clustering algorithm for e-commerce business. *CIT. Journal of Computing and Information Technology*, *26*(1), 57–68. DOI:10.20532/cit.2018.1003863

Kitaev, N., Kaiser, Ł., & Levskaya, A. (2020). *Reformer: The efficient transformer*. arXiv preprint arXiv:2001.04451. https://doi.org//arXiv.2001.04451DOI:10.48550

Kurshan, E., Shen, H., & Yu, H. (2020). Financial crime & fraud detection using graph computing: Application considerations & outlook. In *2020 Second International Conference on Transdisciplinary AI (TransAI)* (pp. 125–130). IEEE. DOI:10.1109/TransAI49837.2020.00029

Leote, P., Cajaiba, R. L., Cabral, J. A., Brescovit, A. D., & Santos, M. (2020). Are data-mining techniques useful for selecting ecological indicators in biodiverse regions? Bridges between market basket analysis and indicator value analysis from a case study in the neotropics. *Ecological Indicators*, *109*, 105833. DOI:10.1016/j.ecolind.2019.105833

Li, S., Zhang, K., Duan, P., & Kang, X. (2019). Hyperspectral anomaly detection with kernel isolation forest. *IEEE Transactions on Geoscience and Remote Sensing*, *58*(1), 319–329. DOI:10.1109/TGRS.2019.2936308

Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining* (pp. 413–422). IEEE. DOI:10.1109/ICDM.2008.17

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 93010–93022. DOI:10.1109/ACCESS.2019.2927266

Marqués, A., García, V., & Sánchez, J. S. (2013). A literature review on the application of evolutionary computing to credit scoring. *The Journal of the Operational Research Society*, *64*(9), 1384–1399. DOI:10.1057/jors.2012.145

Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2020). *Deep learning methods for credit card fraud detection.* arXiv preprint arXiv:2012.03754. https://doi.org//arXiv.2012.03754DOI:10.48550

Ozbayoglu, A. M., Gudelek, M. U., & Sezer, O. B. (2020). Deep learning for financial applications: A survey. *Applied Soft Computing*, *93*, 106384. DOI:10.1016/j.asoc.2020.106384

Peng, Y., Yang, Y., Xu, Y., Xue, Y., Song, R., Kang, J., & Zhao, H. (2021). Electricity theft detection in AMI based on clustering and local outlier factor. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 107250–107259. DOI:10.1109/ACCESS.2021.3100980

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 14277–14284. DOI:10.1109/ACCESS.2018.2806420

Rao, A. B., Kiran, J. S., & G, P. (2023). Application of market-basket analysis on healthcare. *International Journal of System Assurance Engineering and Management*, *14*(S4), 924–929. DOI:10.1007/s13198-021-01298-2

Sharma, A., & Panigrahi, P. K. (2013). *A review of financial accounting fraud detection based on data mining techniques.* arXiv preprint arXiv:1309.3944. https://doi.org//arXiv.1309.3944DOI:10.48550

Tai, C.-J., El-Shazly, M., Tsai, Y.-H., Csupor, D., Hohmann, J., Wu, Y.-C., Tseng, T.-G., Chang, F.-R., & Wang, H.-C. (2021). Uncovering modern clinical applications of Fuzi and Fuzi-based formulas: A nationwide descriptive study with market basket analysis. *Frontiers in Pharmacology*, *12*, 641530. DOI:10.3389/fphar.2021.641530 PMID:33986674

Tiyasha, T., Bhagat, S. K., Fituma, F., Tung, T. M., Shahid, S., & Yaseen, Z. M. (2021). Dual water choices: The assessment of the influential factors on water sources choices using unsupervised machine learning market basket analysis. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 150532–150544. DOI:10.1109/ACCESS.2021.3124817

Videla-Cavieres, I. F., & Ríos, S. A. (2014). Extending market basket analysis with graph mining techniques: A real case. *Expert Systems with Applications*, *41*(4), 1928–1936. DOI:10.1016/j.eswa.2013.08.088

Wang, G., & Chen, Y. (2021). Robust feature matching using guided local outlier factor. *Pattern Recognition*, *117*, 107986. DOI:10.1016/j.patcog.2021.107986

West, J., Bhattacharya, M., & Islam, R. (2015). Intelligent financial fraud detection practices: An investigation. In J. Tian, J. Jing, & M. Srivatsa (Eds.), *International Conference on Security and Privacy in Communication Networks. SecureComm 2014. Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 153* (pp. 186–203). Springer. DOI:10.1007/978-3-319-23802-9_16

Xiuguo, W., & Shengyong, D. (2022). An analysis on financial statement fraud detection for Chinese listed companies using deep learning. *IEEE Access : Practical Innovations, Open Solutions*, *10*, 22516–22532. DOI:10.1109/ACCESS.2022.3153478

Ye, S., Yao, K., & Xue, J. (2023). Leveraging empowering leadership to improve employees’ improvisational behavior: The role of promotion focus and willingness to take risks. *Psychological Reports*, *00332941231172707*. Advance online publication. DOI:10.1177/00332941231172707 PMID:37092876

Ye, S., & Zhao, T. (2023). Team knowledge management: How leaders’ expertise recognition influences expertise utilization. *Management Decision*, *61*(1), 77–96. DOI:10.1108/MD-09-2021-1166

Yotsawat, W., Wattuya, P., & Srivihok, A. (2021). A novel method for credit scoring based on cost-sensitive neural network ensemble. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 78521–78537. DOI:10.1109/ACCESS.2021.3083490

Yu, S., Li, X., Zhao, L., & Wang, J. (2021). Hyperspectral anomaly detection based on low-rank representation using local outlier factor. *IEEE Geoscience and Remote Sensing Letters*, *18*(7), 1279–1283. DOI:10.1109/LGRS.2020.2994745

Yuan, Y., Dehghanpour, K., Bu, F., & Wang, Z. (2020). A data-driven customer segmentation strategy based on contribution to system peak demand. *IEEE Transactions on Power Systems*, *35*(5), 4026–4035. DOI:10.1109/TPWRS.2020.2979943

Zhang, H., Qu, W., Long, H., & Chen, M. (2024). The intelligent advertising image generation using generative adversarial networks and vision transformer: A novel approach in digital marketing. [JOEUC]. *Journal of Organizational and End User Computing*, *36*(1), 1–26. DOI:10.4018/JOEUC.340932

Zhang, R., Zheng, F., & Min, W. (2018). *Sequential behavioral data processing using deep learning and the Markov transition field in online fraud detection*. arXiv preprint arXiv:1808.05329. https://doi.org//arXiv.1808.05329DOI:10.48550

Zhang, Z., Niu, K., & Liu, Y. (2020). A deep learning based online credit scoring model for P2P lending. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 177307–177317. DOI:10.1109/ACCESS.2020.3027337

Zhao, H., Jiang, L., Jia, J., Torr, P., & Koltun, V. (2021b). Point transformer. In *2021 IEEE/CVF International Conference on Computer Vision* (pp. 16239–16248). IEEE. DOI:10.1109/ICCV48922.2021.01595

Zhao, H.-H., Luo, X.-C., Ma, R., & Lu, X. (2021a). An extended regularized K-means clustering approach for high-dimensional customer segmentation with correlated variables. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 48405–48412. DOI:10.1109/ACCESS.2021.3067499

Zhao, Y. (2020). Retracted article: Research on personal credit evaluation of internet finance based on blockchain and decision tree algorithm. *EURASIP Journal on Wireless Communications and Networking*, *213*(1), 213. Advance online publication. DOI:10.1186/s13638-020-01819-w

Zhong, Z. Z., & Zhao, E. Y. (2024). Collaborative driving mode of sustainable marketing and supply chain management supported by Metaverse technology. *IEEE Transactions on Engineering Management*, *71*, 1642–1654. DOI:10.1109/TEM.2023.3337346

Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J., & Gao, Y. (2021). Internet financial fraud detection based on a distributed big data approach with Node2vec. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 43378–43386. DOI:10.1109/ACCESS.2021.3062467

Ziafat, H., & Shakeri, M. (2014). Using data mining techniques in customer segmentation. *International Journal of Engineering Research and Applications*, *4*(9), 70–79.

Zeyi Miao Law school, Southeast University, Nanjing, 210000, China