ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 13 (2026) No. 3, pp.176-194
DOI:10.33168/JLISS.2026.0309

Artificial Intelligence–Driven Financial Fraud Identification in Informatics-Enabled Service Systems

Yonghong Wang*, Xiaomeng Zhang, Yong Yin

Gingko College of Hospitality Management, Chengdu 611743, Sichuan, China

13730879813@163.com (Corresponding author), xiaomeng.zhang@gingkoc.edu.cn, yong.yin@gingkoc.edu.cn

Abstract. In digital and intelligent service systems, financial fraud identification is not only a technical task for risk management but also a key information service supporting logistics finance, supply chain auditing, and compliance service operations. Existing methods are mostly independent of business processes and lack deep integration with organizational information systems and service ecosystems. Therefore, this paper constructs an AI-driven information and service fusion framework, repositioning financial fraud identification as an embedded decision support service. First, high-quality risk information input is constructed through multi-source heterogeneous information integration and feature engineering. Then, a gradient boosting decision tree (GBDT) model is used for fraud pattern identification, and pruning strategies are employed to optimize the model's service robustness in imbalanced data. Finally, the paper explains how this framework can be embedded as an intelligent information service component into enterprise compliance systems, supply chain finance risk control platforms, and regulatory technology processes. Experiments show that the proposed GBDT outperforms Random Forest (RF), Extreme Gradient Boosting (XGBoost), and Support Vector Machine (SVM), with GBDT's average Kappa coefficient being approximately 8.6%, 3.7%, and 10.9% higher, respectively, validating its effectiveness in information processing and classification decision-making. The conclusions show that this framework helps improve the accuracy of fraud identification. Through service-oriented, explainable, and auditable design, it enhances organizations' information adaptability and decision-making reliability in dynamic risk environments, thus providing a theoretical reference and a practical path for the construction and operation optimization of information systems in logistics, finance, and related service sectors.

Keywords: Financial Fraud Identification, Artificial Intelligence, Gradient Boosting Decision Tree, Financial Data Analysis, Machine Learning

1. Introduction

As global trade continues to become more and more digitalized, logistics services and supply chains are more important than ever (Kim & Ha, 2022). Financial fraud detection is not only an important part of a business's overall financial management strategy, but also a vital piece of the risk management framework for logistics financial services, supply chain services and digital platform operations. Financial fraud has serious financial implications for companies, including damaging the transparency of their finances, reputation with stakeholders, and investor confidence in their operations (Hashim et al., 2020; Dyck et al., 2024). In the context of supply chain finance, fraudulent activity (e.g., fictitious transactions or counterfeit documentation) disrupts the credit chain and increases the total costs of operations. Fraudulent activity within logistics service providers, such as fraudulent shipping charges or fraudulently filed claims against insurance coverage, directly negatively impacts the profitability of the logistics provider, as well as the integrity of the logistics ecosystem. Traditional rule-based identification methods have been difficult to cope with the increasingly complex fraud phenomenon (Rashid et al., 2022; Daraojimba et al., 2023). Such methods mostly rely on historical data or fixed patterns, cannot effectively analyze unbalanced data, and have the problem of low accuracy. As computer science continues to improve and develop, AI technology has been greatly developed and applied with high efficiency, self-adaptation and dynamic learning capabilities. Based on AI technology, large-scale and complex financial data can be automatically analyzed to dig out deep data rules that traditional methods cannot discover, and potential fraud patterns can be identified (Chirra, 2020; Gayam, 2021). By dynamically adapting to new fraud behaviors, it has important practical value in reducing the economic losses and legal risks caused by fraud and improving the transparency and compliance level of logistics companies.

At present, the research on fraud identification and prevention is mainly focused on how to improve accuracy. Mishra (2023) explored the use of Apache Flink to enhance anomaly detection and business process monitoring on a large scale. By combining rule-based methods with Flink's functions, fraud and anomalies can be detected in real-time. The results verified the effectiveness of the proposed method in improving decision-making and reducing risk. An & Suh (2020) proposed an identification method based on a rule classification model. Rules were extracted from the improved RF model to explain whether the company corresponding to the new instance may have fraud. The results showed that the proposed model performed better than the baseline model. Tumminello et al. (2023) formalized filtering rules through probability models and test-specific methods to evaluate out-of-sample fraud. Database test results presented that the proposed method could improve the fraud detection accuracy. Current research has significantly improved identification accuracy, but most of these methods are based on fixed rules. Behavior identification is limited, and it is difficult to adapt to rapidly changing environments.

The development of AI technology has provided more possibilities for adapting to the ever-changing fraud methods and providing real-time detection and identification (Johora et al., 2024). Specifically, machine learning (ML) techniques have the unique ability to adaptively optimize their parameters and structural designs through the use of feedback mechanisms, and tend to be extremely sensitive to changes in the patterns of fraudulent behavior (Islam et al., 2024; Njoku et al., 2024). According to Huang et al. (2024), it is possible to detect fraudulent activity more accurately and efficiently by using a K-Means clustering algorithm based on machine learning techniques, rather than through the conventional means of rule-based detection techniques. The ability to assess large volumes of financial transactions and identify abnormal behaviours through configuration inspection facilitates a level of adaptability for fraud detection that is superior to that associated with traditional rule-based systems. In addressing the issue of rapidly evolving threats that cannot be addressed through the use of traditional static models, Bello et al. (2024) advocate for the use of adaptive machine learning technologies that create elastic defenses against fraud schemes by continually learning from new data sources and continuously improving the detection of new fraudulent behaviours. The research

demonstrates the increase of flexibility in the detection of fraud and increases the credibility of the financial systems that have implemented this adaptive technique. Among other applications, the study of Immaneni (2021) discussed the use of integrated swarm intelligence and graph databases for real-time detection of fraudstealing. The researchers concluded that swarming allows fraud detection to be accomplished in real-time by using interactions of multiple agents in the swarm to learn and adapt to new fraud strategies developed by the perpetrators of fraud. Test results showed that the proposed method could achieve faster response time and strong defense against fraud. AI can dynamically adjust to new fraud behaviors to achieve more flexible and accurate identification and prevention (Bello et al., 2024; Kamuangu, 2024; Lin, 2024). However, most existing studies have overfitting problems in unbalanced data.

To enhance financial transparency and improve the fraud identification and prevention, this paper combines AI technology and builds an identification model based on the GBDT algorithm. From a theoretical perspective, AI-based fraud detection systems are essentially enhanced decision support systems (DSS), and their improved performance can be explained by information processing theory and sociotechnical systems theory. According to information processing theory, organizations facing environmental uncertainty need to enhance their information acquisition, integration, and interpretation capabilities to maintain effective decision-making. Traditional rule engines with static knowledge bases cannot adequately process high-dimensional, nonlinear, and time-varying financial fraud signals. There are information processing bottlenecks in these systems. The analytical depth and noise resilience of the system will be improved by using a GBDT machine learning model through automatic feature interaction and residual learning mechanisms, thereby improving the quality of information that will be required to support anti-fraud decisions from complex financial data sources. The sociotechnical systems theory supports the co-evolution of both the technological and organizational subsystems. The AI-noise reduction-driven anti-fraud framework created here provides not only high-precision predictions but also the provision of structured decision-making support for auditors and risk control departments through interpretable feature importance ranking, thereby enhancing the organizational responsiveness of "human-machine collaboration" through improved overall reliability and compliance of services. The innovations of this paper are: 1) Service-oriented integration of multi-source heterogeneous data: A reusable process for fusion of financial, transactional, textual, and external data is proposed, and a feature engineering scheme oriented towards service scenarios is designed to enhance the completeness and interpretability of risk information; 2) Robust service modeling strategy for extreme imbalance scenarios: Through strategies such as post-system comparison pruning, resampling, and cost-sensitive learning, the advantages of imbalance processing paths guided by structure optimization in service sustainability are demonstrated under limited prior knowledge; 3) System integration and governance of decision support services: The fraud identification framework is defined as an intelligent service that can be embedded in organizational information systems and regulatory processes, and a comprehensive integration scheme covering technology deployment, process adaptation, and ethical governance is proposed, providing a reference for the cross-domain application of service science.

2. Financial Fraud Identification and Prevention Methods

2.1 Multi-source Heterogeneous Data Governance and Integration Architecture

This paper constructs a multi-layered information governance architecture for fraud detection, as shown in Figure 1. Through standardized data interfaces, it connects to the enterprise's internal financial system, external regulatory databases, and public judicial platforms to achieve real-time/ near-real-time data synchronization across systems. To address the issue of data structure heterogeneity, ontology mapping and a unified data model are employed to semantically align financial items, transaction types, and legal terms:

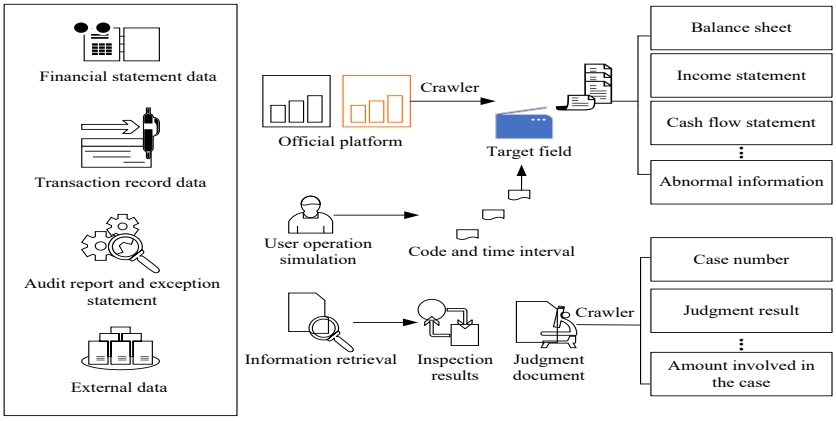

Fig.1: Data collection

In Figure 1, this paper uses two public websites, Dongfang Fortune Network and Juchao Information Network, as the main channels for data collection. In the specific collection process, a web crawler is compiled in Python language, and the target field is set, which includes financial reports such as balance sheet, income statement, cash flow statement, and some abnormal information about company announcements. Through user operation simulation, automatic access to the site is realized. The target data is captured according to the code and time interval, and the captured data is stored locally in the form of JSON. To prevent omissions, the application frequency is dynamically adjusted through the program to ensure comprehensive coverage of the target company and time period.

For tax data and related litigation information, the tax declaration information, tax audit results, and fraud case judgments of relevant companies are obtained by querying the public disclosure system and the public judgment document website. In the specific operation, a keyword-based database retrieval method is adopted, and the crawler is used to extract structured fields such as case number, judgment result, and amount involved, and match and integrate them by company name.

In the process of collection, different data are stored in a layered manner according to different data types and different time periods for further analysis. The basic situation of the collected sample data is presented in Table 1:

Table 1. Basic situation of sample data

Sample category	Number of samples	Time Span	Number of data fields	Data missing rate
Financial statement data	1029	2015-2022	48	2.40%
Transaction record data	150398	2015-2022	12	0.10%
Audit report and exception statement	926	2015-2022	8	1.80%
External data	83	2015-2022	15	0.50%

To further reveal the distribution characteristics of key financial features, Table 2 reports descriptive statistics of key continuous financial features:

Table 2. Key continuous financial characteristics descriptive statistics

Characteristics	Mean	Standard deviation	Min	25th percentile	Median	75th percentile	Max	Skewness
Current Ratio (x_1)	1.52	0.89	0.21	0.98	1.31	1.85	6.74	1.82
Liability Ratio (x_3)	0.49	0.18	0.11	0.36	0.48	0.61	0.92	0.31
Net Profit Margin (x_4)	0.07	0.15	-0.89	0.02	0.06	0.12	0.58	-1.24
Revenue Growth Rate (x_9)	0.12	0.23	-0.45	0.03	0.1	0.19	1.05	1.05
Frequency of Abnormal Transactions (x_{16})	0.03	0.06	0	0	0.01	0.03	0.35	3.41

Note: All ratio indicators have been normalized to the range [0,1]. The table above shows the original calculated values.

After the data is acquired, it is preprocessed. Preprocessing decisions were all based on domain knowledge and exploratory data analysis. Missing values were identified using linear interpolation based on time windows, limited to continuous variables with a missing value rate of less than 5%. Outlier removal employed the Local Outlier Factor (LOF) algorithm with a threshold of 2.5. This threshold was tested in pre-experiments to strike a balance between maintaining data integrity (removal rate <1.5%) and model stability.

Then, it is normalized. Because the dimensions and ranges of financial indicators are very different, if they are directly input into the model, it is easy to cause training deviation. This paper uses the maximum and minimum value normalization method to unify all continuous type variables to the range of [0,1]:

$$x' = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

On this basis, for financial indicators with long-tail distribution characteristics, the logarithmic transformation method is used to normalize them to reduce the impact of outliers on the model.

When preprocessing time series data such as transaction records, the sliding window method is used to extract short-term volatility and long-term trends, and an indicator set that can reflect its time dynamic characteristics is constructed. The formula is:

$$S_t = \frac{\sum_{i=t-\omega+1}^{t} x_i}{\omega} \quad (2)$$

In formula 2, S_t is the smoothing value at the t-th moment, and ω is the window size.

To ensure the consistency and integration between multi-source data, the company name and equity code are uniformly used as index fields, and a data verification script is used to check whether the collected data has format errors, duplicate records, and other problems.

2.2 Definition of Fraud and Non-fraud Samples

After preprocessing the data, the information of financial report violation announcements, judicial decisions, and tax inspections are combined to accurately define fraud and non-fraud samples:

(1) Financial report violations

By searching the announcements disclosed by the China Securities Regulatory Commission and the Shanghai and Shenzhen Stock Exchanges, companies that are subject to supervision for illegal acts such as false statements, asset inflation, and profit inflation are screened. Samples that are found to have fraud behavior are regarded as fraud samples (Zhu et al., 2021; Obeng et al., 2024; IkbaL et al., 2020).

(2) Judicial judgment results

In the unstructured information, the judgments suspected of financial fraud are filtered to extract

the company name and fraud time. In the judgments, all cases that clearly mention false financial information and cause damage to stakeholders are classified as fraud samples (Ozili, 2020; Desai, 2020).

(3) Tax audit information

The tax audit announcement is queried through the public disclosure system. If there are obvious false declarations and tax evasion in the announcement, the corresponding annual company samples are also included in the fraud samples.

(4) Non-fraud samples

Non-fraud samples are randomly selected from companies that have not experienced the above-mentioned fraud incidents, and the industry distribution is guaranteed to match the fraud samples to avoid the impact of data bias on the analysis results.

Through the definition, the final analysis dataset is presented in Table 3:

Table 3. Analysis dataset

Classification	Fraud samples	Non-fraud samples
Sample quantity	95	631
Sample proportion (%)	13.1	86.9
Average total assets (in billions of yuan)	128.4	136.2
Average revenue (in billions of yuan)	87.6	92.3
Average net profit (in billions of yuan)	-3.2	6.8

In Table 3, the fraud samples are strictly defined and screened at multiple levels to ensure data quality and the significance of the fraud nature.

2.3 Feature Engineering

Before identification modeling, based on the collected multi-source heterogeneous data, features highly related to fraud behavior are extracted to form high-dimensional input variables for the training model, as shown in Figure 2.

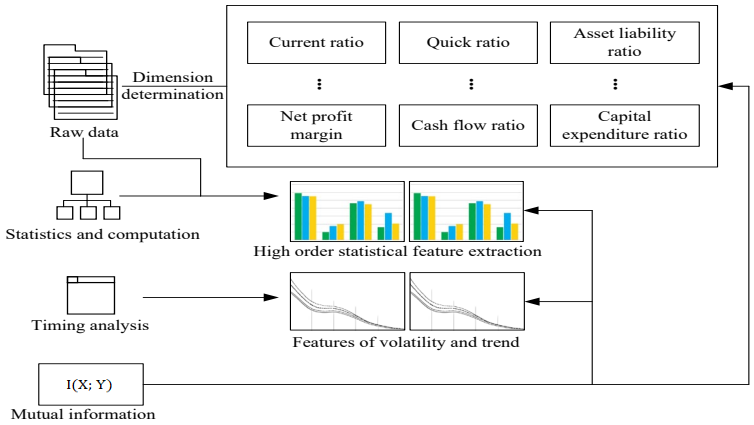

Fig.2: Feature extraction

(1) Determination of the dimension of the original data

The dimension of the original data is mainly determined by extracting key variables from financial statement data, transaction record data, audit reports and abnormal descriptions, and external data, mainly covering variables such as current ratio, quick ratio, debt-to-asset ratio, net profit margin, cash

flow ratio, and capital expenditure ratio.

(2) Statistics and calculation

Through statistical analysis of the original data, high-order statistical features with distinguishing power are extracted.

(3) Time series analysis

The volatility (standard deviation, coefficient of variation) and trend characteristics of corporate financial indicators are extracted using time series analysis methods. Taking net profit and operating income as an example, the net profit and operating income of the company in the past three years can be compared, and their change characteristics can be analyzed to determine whether there are sudden abnormal phenomena in the data.

(4) Feature selection

The feature selection adopts the method based on Mutual Information (MI). The specific calculation is expressed as:

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \quad (3)$$

High-contribution features are screened out, and the final extracted feature indicators include 19 items, as presented in Table 4:

Table 4. Feature extraction results

Dimension	Code	Feature indicators
Financial features	x1	Current ratio
	x2	Quick ratio
	x3	Asset liability ratio
	x4	Net profit margin
	x5	Change rate of accounts receivable turnover days
	x6	Standard deviation of inventory turnover times
	x7	Cash flow ratio
	x8	Capital expenditure ratio
	x9	Income growth rate
	x10	Cost growth rate
Timing features	x11	Maximum quarterly accounts receivable turnover days
	x12	Minimum quarterly inventory turnover times
	x13	Trend of cash flow
	x14	Change rate of return on equity
	x15	Abnormal fluctuations in profit margin
Derived features	x16	Abnormal transaction frequency
	x17	Proportion of related party transactions

	x18	Number of insider trading reports
	x19	Number of legal dispute cases

2.4 Model Construction

AI has been developed in the field of fraud identification, but the sparsity of fraud samples and the multicollinearity of financial indicators have posed new challenges to AI in processing unbalanced data and feature selection. To address this problem, this paper uses GBDT as the main algorithm. The core value of an AI anti-fraud system lies in transforming raw financial data into a decision information flow with a high signal-to-noise ratio. According to the DSS theory, an efficient DSS should have three capabilities (Gupta et al., 2022): (1) environmental perception capability; (2) cognitive computing capability; and (3) action support capability. This paper adopts GBDT as the core algorithm, mainly because GBDT naturally supports mixed-type feature inputs and can seamlessly integrate financial ratios (x1-x8), time-series trends (x9-x15), and derived behavioral indicators (x16-x19) to meet the environmental perception requirements; its additive modeling mechanism can effectively capture the high-order interaction effects between variables by iteratively fitting the residuals, thereby enhancing the cognitive computing depth (Zhang & Jung, 2020); and the local interpretability of the decision path based on GBDT can generate risk attribution reports for business personnel, supporting precise intervention and reflecting the value of action support.

GBDT implements reinforcement learning based on multiple weak classifiers during training. When identifying fraud behavior, the constant model $F_0(x)$ is first initialized. This value represents the mean or appropriate reference value of all training samples, indicating the initial prediction of the model without learning (Sengupta & Das, 2023; Alothman et al., 2022):

$$F_0(x) = \arg\min_{\gamma} \sum_{i=1}^{N} L(y_i, \gamma) \quad (4)$$

Here, $L(y_i, \gamma)$ represents the loss function; y_i represents the true label of the sample; γ represents the current prediction result.

In each iteration, GBDT generates a new decision tree $h_t(x)$, and uses this tree to perform residual fitting on the prediction results of the previous stage, as shown in Figure 3:

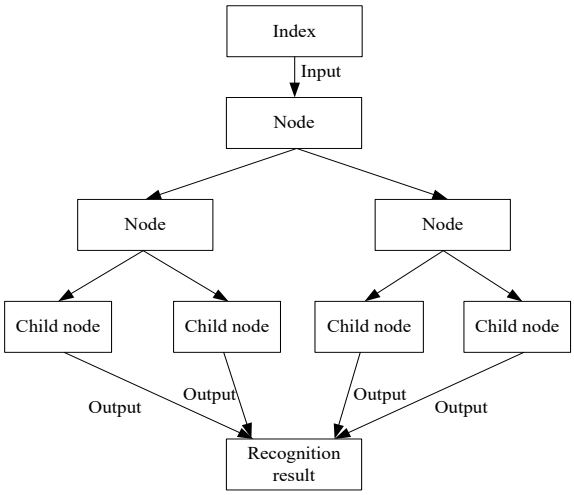

Fig.3: GBDT algorithm

GBDT's iterative learning mechanism enables it to adaptively focus on well-disguised fraudulent companies, thereby maximizing risk coverage with limited labeled data. During node splitting, the system selects optimal financial features such as "abnormal accounts receivable turnover" or "sudden changes in related-party transaction ratio" for splitting based on the information gain criterion. This process not only improves classification accuracy but also implicitly constructs an interpretable risk

discrimination path. If the model frequently splits at "x5 (accounts receivable growth rate) > 30%", it indicates that the indicator has strong discriminative power in distinguishing between fraudulent and legitimate companies, providing auditors with clear verification clues. For the complete mathematical form of the algorithm and training details, please refer to Appendix A.

High data imbalance is a core challenge in financial fraud detection. Common imbalance handling strategies include data-level resampling and algorithm-level cost-sensitive learning. However, resampling can introduce overfitting or information loss, while cost-sensitive learning relies on accurate prior knowledge of misclassification costs, which is often difficult to define precisely in fraud detection. In the model optimization training, to address the issue of overfitting caused by a large amount of noise in financial data, this paper optimizes the structure of each decision tree and uses a pruning algorithm to limit the maximum depth and minimum number of samples of the tree. By dynamically adjusting the depth of the decision tree, overfitting of the training samples is prevented.

This paper chooses a pruning-based imbalance handling strategy, primarily based on the following: GBDT, as an ensemble tree model, inherently possesses robustness to class imbalance due to its gradient boosting mechanism, as it iteratively focuses on difficult-to-classify samples. Furthermore, pruning, by controlling the tree's complexity, effectively suppresses overfitting to the majority class noise, thereby indirectly improving the generalization ability to recognize minority classes. The combination of pruning and GBDT eliminates the need for manual adjustments to the original sample distribution or pre-setting misclassification costs, reducing the method's reliance on prior domain knowledge and enhancing the model's applicability and stability.

During the training process of the tree, the tree structure is simplified, and redundant nodes are reduced to improve the model’s generalization ability. There are two common pruning methods: pre-pruning and post-pruning. Since the problem of fraud identification is characterized by large number and high complexity, pre-pruning (that is, constraining it when constructing the tree) causes the model to terminate its growth prematurely, making it unable to accurately discover the complex patterns hidden in the data. The post-pruning method is to first grow the decision tree to the maximum extent to obtain more implicit features, and then prune it to remove redundant information to maintain nodes with strong discriminative ability. Therefore, this paper adopts the post-pruning strategy.

Post-pruning is to use a recursive method to prune the generated tree. On this basis, by analyzing the importance of each branch, those branches that have an adverse effect on the model performance are removed. The steps include:

(1) Starting from the leaf node, all nodes in the tree are traversed.

(2) For each node, the performance change before and after node pruning is calculated, and the performance difference before and after pruning is mainly measured by cross-validation or other methods.

(3) If the performance of a node does not decrease significantly after pruning, the node and its child nodes are deleted.

The optimized GBDT model essentially constructs an adaptive learning system: it improves the quality of information representation of fraud risk by continuously integrating features from multiple sources; it balances the model's recognition accuracy and generalization ability through controllable complexity and pruning mechanisms; and it finally outputs risk labels with high confidence and interpretable feature contribution analysis, providing reliable support for risk decision-making. The post-pruning strategy can reduce the complexity of the algorithm while retaining the nodes that have a significant impact on the algorithm performance. On this basis, the pruned tree structure can identify fraud and precisely classify the two types of samples, fraud and non-fraud, which can provide a scientific basis for effectively identifying and preventing fraud behavior.

2.5 Integration and Application of Models in the Financial Services System

Based on information processing theory and DSS theory, the GBDT fraud identification model proposed in this paper not only possesses superior classification performance but can also be embedded into the workflows and logistics regulatory systems of financial service organizations, achieving closed-loop management from data to decision-making. The integration and application of the model in the financial service system mainly involves three levels: system integration architecture, operational process embedding, and human-machine collaboration mechanism.

(1) System Integration Architecture

The model is deployed as a standalone fraud detection engine, connecting with logistics enterprise financial systems, transaction monitoring platforms, audit management systems, and regulatory reporting platforms via API interfaces. The system architecture employs a microservice design, supporting high-concurrency real-time queries and batch offline analysis. The model receives standardized data streams from multiple systems, outputs fraud risk scores and early warning signals, and presents feature contribution analysis through a visual dashboard to assist decision-makers in understanding the model's judgment basis.

(2) Embedding of Operational Processes

The model serves as a pre-screening mechanism for internal audits by providing automatic identification of high-risk companies in the annual audit planning phase and by providing guidance in determining priority allocations of audit resources or staff time to conduct audits. In addition, it provides real-time or near real-time alerts through the setting of dynamic threshold criteria in continuous monitoring situations. If a company's characteristic has significantly changed or the model score exceeds a certain threshold, the system creates a work order for an alert and sends it to the audit department or compliance group for manual verification of the event. It would be eligible for use under a regulatory technology "sandbox" and/or within an intelligent monitoring platform, in support of current regulatory agencies in performing supervisions, and would allow for the aggregation of risk view by industry, geographic area, and time period and to generate a structured report that would enhance the accuracy and extent of off-site supervision of companies.

(3) Human-machine collaboration mechanism

This model emphasizes the human-in-the-loop design principle. The system provides a tiered early warning mechanism: low-risk warnings are logged only; medium-to-high-risk warnings require manual review and confirmation; and extremely high-risk warnings automatically trigger a freeze or review process. Auditors or risk control experts can provide feedback on the model's early warning results. This feedback data is used for iterative model optimization, resulting in continuous improvement from monitoring to early warning, then to handling, and finally to learning, driving the dynamic evolution of the organization's anti-fraud capabilities.

3. Identification and Prevention of Financial Fraud

3.1 Experimental Indicators

To comprehensively evaluate the service quality of the model in fraud detection tasks, this paper uses five metrics: accuracy, precision, recall, AUC, and Kappa coefficient. Accuracy measures the overall classification correctness of the model; precision reflects the proportion of genuine fraud among samples identified as fraud by the model, directly affecting the reliability of the early warning system; recall assesses the model's ability to identify genuine fraudulent behavior, relating to the level of risk underreporting control. The AUC value comprehensively reflects the model's classification performance at different thresholds, and the Kappa coefficient is used to evaluate the model's classification consistency on imbalanced data. The calculation formulas for each metric are detailed in Appendix B.

3.2 Parameter Setting

This paper is mainly based on the GBDT algorithm and combines it with pruning technology to enhance the model's adaptability and fitting ability under unbalanced samples. Its parameter settings are displayed in Table 5:

Table 5. Algorithm parameter settings

Sequence	Parameter	Setting
1	Learning rate	0.05
2	Number of estimators	100
3	D_{max}	6
4	N_{min}	10
5	ΔI_{min}	0.01
6	Pruning strategy	Post-pruning

To comprehensively evaluate the effect of GBDT algorithm, it is compared with three advanced algorithms:

(1) RF

RF algorithm is an integrated learning algorithm that generates multiple decision trees and then averages the prediction values of each tree to improve the algorithm's stability and accuracy (Nhien et al., 2024).

(2) XGBoost

XGBoost algorithm achieves fine-tuning by performing gradient optimization at each step, and has the advantages of parallel computing and processing missing values.

(3) SVM

SVM is a classification model based on statistical learning. It divides different types of samples by searching for the best hyperplane and can maintain good identification effect in high-dimensional feature space (Singh et al., 2022).

The three comparison algorithms all use standard parameter settings.

3.3 Experimental Results

(1) Comparison of accuracy, precision, and recall

By rolling prediction of 19 input feature indicators under different models, the out-of-sample performance of each model in identification is obtained. The average results of accuracy, precision, and recall from 2015 to 2022 are shown in Figure 4:

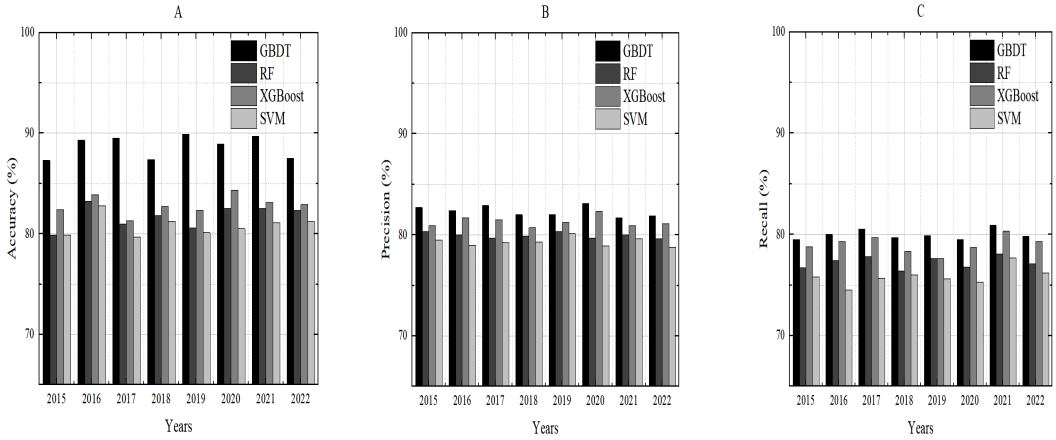

Fig.4. Accuracy, precision, and recall results

Fig.4A: Accuracy

Fig.4B: Precision

Fig.4C: Recall

In Figure 4, GBDT performs well in accuracy, precision, and recall, especially in accuracy, which is significantly higher than other control algorithms. In Figure 4A, the average accuracy of GBDT in the sample analysis of each year reaches 88.7%, while the average accuracy of RF, XGBoost, and SVM models are 81.7%, 82.9%, and 80.8%, respectively. In comparison, the average accuracy of GBDT is 7.0%, 5.8%, and 7.9% higher, respectively. In Figure 4B, the average precision of RF, XGBoost, and SVM models are 79.9%, 81.3%, and 79.3%, respectively, and the average precision of GBDT is 82.3%, which are 2.4%, 1.0%, and 3.0% higher than the control model, respectively. In Figure 4C, the average recall of GBDT in the sample analysis of each year is about 80.0%, and the average recall of the other three models are 77.2%, 79.0%, and 75.9%, respectively. The average recall of GBDT is 2.8%, 1.0%, and 4.1% higher than that of RF, XGBoost, and SVM models, respectively. From an operational perspective, the GBDT model's average accuracy of 88.7% means that, over long-term service operation, the vast majority of enterprise samples can be correctly classified for risk. This provides a reliable initial screening basis for resource-constrained risk control departments, reducing the operational burden of comprehensive manual verification. Its average precision of 82.3% indicates that when the system issues a fraud alert, over 80% of the risks are genuine, directly enhancing the credibility of the alert signals and avoiding "alarm fatigue" and wasted investigation resources caused by frequent false alarms. The average recall rate of 80.0% means that the system can capture over 80% of genuine fraudulent activities, thereby significantly reducing the possibility of significant financial losses or systemic regulatory risks due to missed reporting at the operational level, enhancing the service's foresight and defensive depth.

(2) AUC and ROC curve results

By comparing the AUC and ROC curves of different models, the sample identification effect of different models can be better evaluated. A larger AUC value indicates that the model has a better classification effect. The final result is shown in Figure 5:

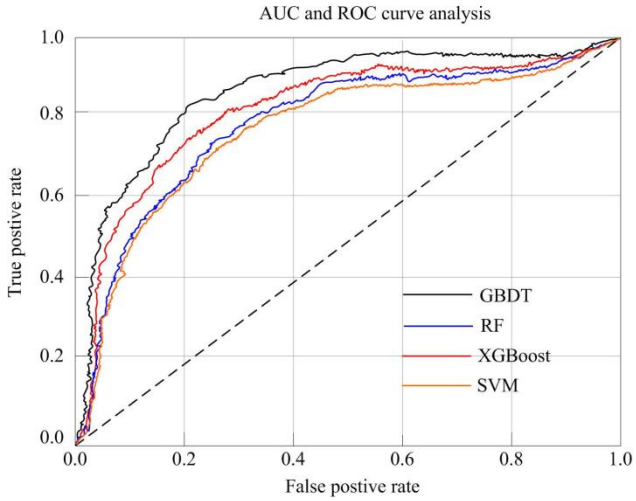

Fig.5: AUC and ROC curve results

From Figure 5, GBDT has a significant advantage in AUC and ROC curve results, with an AUC value of 0.912; the AUC values of RF, XGBoost, and SVM are 0.864, 0.881, and 0.827, respectively. Compared with RF, XGBoost, and SVM models, GBDT is the most ideal in distinguishing fraud and non-fraud samples. Based on the post-pruning strategy of GBDT, through repeated learning of the model, it achieves a good balance between the model's complexity and promotion ability. In the process of fraud behavior identification, it can extract valuable information from complex correlations through step-by-step error correction, thereby effectively coping with the challenges of high-dimensional features to fraud sample identification. This result demonstrates that the system maintains stable recognition performance across different risk assessment thresholds. This provides flexibility for operational decisions: during periods of low risk tolerance, the threshold can be lowered to improve recall and prevent risk omissions; while in routine monitoring, the threshold can be raised to improve accuracy and optimize the allocation of investigation resources.

(3) Kappa coefficient

By comparing the Kappa coefficient, the consistency level of different models in identification and their classification capabilities can be better understood. The final results are illustrated in Figure 6:

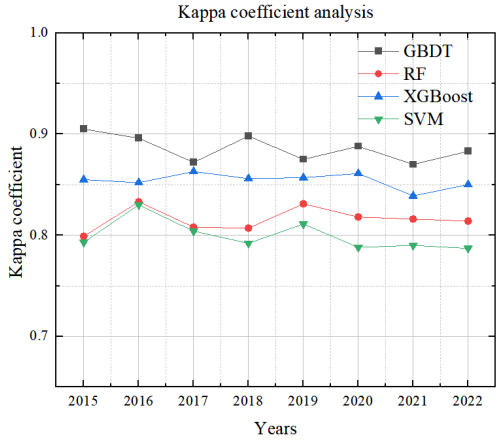

Fig.6: Kappa coefficient results

In Figure 6, the Kappa coefficients of the GBDT model in all years show strong classification consistency. From the specific comparison results, the average Kappa coefficient of GBDT in the sample analysis of each year reaches 0.886, while the average Kappa coefficients of RF, XGBoost, and

SVM models are 0.816, 0.854, and 0.799, respectively. In contrast, the average Kappa coefficient of GBDT is about 8.6%, 3.7%, and 10.9% higher, respectively. From the perspective of service reliability and trust building, a high Kappa coefficient signifies high stability and predictability of system output. For organizations relying on automated reporting for decision-making or as a regulatory technology tool, this consistency is a prerequisite for building internal trust and ensuring the acceptability of regulatory reviews. It reduces decision uncertainty caused by fluctuations in model output, supporting the long-term, deep embedding of automated services in critical business processes.

To further evaluate the effectiveness of the class imbalance handling strategy in the scenario presented in this paper, three typical schemes were compared under the same feature engineering and basic GBDT framework: 1) GBDT + post-pruning; 2) GBDT + SMOTE oversampling; and 3) GBDT + class weight adjustment. All comparative experiments used the same training/validation set splits, and AUC, recall, and Kappa coefficient were used as the main evaluation metrics to comprehensively measure the model's performance in balancing recognition performance and generalization ability. The results are shown in Table 6.

Table 6. Performance comparison of different imbalance handling strategies

Processing methods:	AUC	Recall	Precision	Kappa coefficient
GBDT + post-pruning	0.912	0.8	0.823	0.886
GBDT + SMOTE oversampling	0.887	0.821	0.794	0.852
GBDT + class weight adjustment	0.876	0.835	0.772	0.838

Table 6 shows that GBDT+post-pruning performs best in AUC, precision, and Kappa coefficient, demonstrating the best overall classification performance and prediction consistency. Although SMOTE and weight adjustment have a slight advantage in recall, their precision and Kappa coefficient both decrease to varying degrees, reflecting the risk of overfitting or blurred decision boundaries. This indicates that in the scenario based on multidimensional financial features, controlling model complexity through pruning can more effectively achieve a balance between accuracy and robustness in fraud detection without distorting data distribution or introducing additional parameters.

4. Conclusions

This paper combines AI technology to study fraud identification and prevention. From the aspects of data collection, preprocessing, feature extraction, etc., based on GBDT, an identification model is established, and the model is further optimized using the pruning algorithm. Experiments have shown that GBDT is superior to RF, XGBoost, and SVM control models in terms of accuracy, precision, recall, and AUC values. In the comparison of Kappa coefficients, GBDT shows excellent consistency and stability, and its Kappa coefficient is about 8.6%, 3.7%, and 10.9% higher than the other three models. The model in this paper can effectively improve the accuracy of identification and provide more effective decision-making support for the prevention work of companies and regulatory authorities. However, the GBDT method is highly complex and requires high training time in sample classification. While the GBDT model possesses relative interpretability, its decision-making process still requires the integration of ex-post interpretation techniques such as SHAP to enhance transparency. Furthermore, a mechanism for manual review and decision log traceability should be established for high-risk warnings to clarify accountability. To mitigate potential false positives and implicit data bias, it is recommended to employ fairness audits and adversarial debiasing techniques. The data and conclusions in this paper rely on the specific institutional environment of Chinese listed companies, including their accounting standards, information disclosure regulatory framework, and corporate governance structure. Therefore, the model and conclusions are most directly applicable to scenarios with similar market systems and

data transparency. In regions with vastly different regulatory systems, lower data accessibility, or different corporate governance models, the feature set and threshold standards of this method need to be localized and adjusted for applicability. Future work will focus on building a governance framework that synergistically optimizes performance, interpretation, and fairness, ensuring that the application of the technology complies with logistics, financial regulatory compliance and social responsibility requirements. It will also consider combining the technology with other algorithms to further optimize computational efficiency, promote rapid real-time identification in large-scale data scenarios, and thus drive the healthy and scientific development of supply chain auditing and service operation risk control.

Data availability statement

The data used in this study are derived from publicly disclosed financial reports and regulatory penalty information, and have been processed for compliance before being used for modeling and analysis. The data sources, preprocessing methods, feature engineering processes, and model building techniques have been detailed in the main text and appendices to ensure full disclosure and understandability of the research methods. Scholars seeking reasonable academic purposes may contact the corresponding author for further information.

References

Alghofaili, Y., Albattah, A., & Rassam, M. A. (2020). A financial fraud detection model based on LSTM deep learning technique. Journal of Applied Security Research, 15(4), 498-516.

Alothman, R., AliTalib, H., & Mohammed, M. S. (2022). FRAUD DETECTION UNDER THE UNBALANCED CLASS BASED ON GRADIENT BOOSTING. Eastern-European Journal of Enterprise Technologies, 116(2), 6-12.

An, B., & Suh, Y. (2020). Identifying financial statement fraud with decision rules obtained from Modified Random Forest. Data Technologies and Applications, 54(2), 235-255.

Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences, 12(2), 21-34.

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer science & IT research journal, 5(6), 1505-1520.

Chirra, B. R. (2020). AI-Driven Fraud Detection: Safeguarding Financial Data in Real-Time. Revista de Inteligencia Artificial en Medicina, 11(1), 328-347.

Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention. Finance & Accounting Research Journal, 5(11), 342-360.

Dyck, A., Morse, A., & Zingales, L. (2024). How pervasive is corporate fraud?. Review of Accounting Studies, 29(1), 736-769.

Desai, N. (2020). Understanding the theoretical underpinnings of corporate fraud. Vikalpa, 45(1), 25-31.

Gayam, S. R. (2021). Artificial intelligence for financial fraud detection: advanced techniques for anomaly detection, pattern recognition, and risk mitigation. Afr J Artif Intell Sustain Develop, 1(2), 377-412.

Gupta, S., Modgil, S., Bhattacharyya, S., & Bose, I. (2022). Artificial intelligence for decision support systems in the field of operations research: review and future scope of research. Annals of Operations Research, 308(1), 215-274.

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: a management perspective. Journal of Financial Crime, 27(4), 1143-1159.

Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of machine learning-based k-means clustering for financial fraud detection. Academic Journal of Science and Technology, 10(1), 33-39.

IkbaL, M., Irwansyah, I., Paminto, A., Ulfah, Y., & Darma, D. C. (2020). Financial intelligence: Financial statement fraud in Indonesia. Journal of Intelligence Studies in Business, 10(3), 80-95.

Islam, S., Haque, M. M., & Karim, A. N. M. R. (2024). A rule-based machine learning model for financial fraud detection. International Journal of Electrical & Computer Engineering (2088-8708), 14(1), 759-771.

Immaneni, J. (2021). Using swarm intelligence and graph databases for real-time fraud detection. Journal of Computational Innovation, 1(1), 1-20.

Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-powered fraud detection in banking: Safeguarding financial transactions. The American journal of management and economics innovations, 6(6), 8-22.

Kamuangu, P. (2024). A review on financial fraud detection using ai and machine learning. Journal of Economics, Finance, and Accounting Studies, 6(1), 67-77.

Khamainy, A. H., Ali, M., & Setiawan, M. A. (2022). Detecting financial statement fraud through new fraud diamond model: the case of Indonesia. Journal of Financial Crime, 29(3), 925-941.

Kim, Y. J., & Ha, B. C. (2022). Logistics service supply chain model. Journal of Logistics, Informatics and Service Science, 9(3), 284-300.

Lin, A. K. (2024). The AI Revolution in Financial Services: Emerging Methods for Fraud Detection and Prevention. Jurnal Galaksi, 1(1), 43-51.

Mishra, S. (2023). Scaling rule based anomaly and fraud detection and business process monitoring through Apache Flink. International Journal of AI, BigData, Computational and Management Studies, 4(1), 108-119.

Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web base application. Machine Learning, 20(4), 01-12.

Nhien, C. T., Hung, D. N., & Bình, V. T. T. (2024). Using random forest and artificial neural network to detect fraudulent financial reporting: Data from listed companies in Vietnam. Calitatea, 25(202), 160-173.

Obeng, S., Iyelolu, T. V., Akinsulire, A. A., & Idemudia, C. (2024). Utilizing machine learning algorithms to prevent financial fraud and ensure transaction security. World Journal of Advanced Research and Reviews, 23(1), 1972-1980.

Ozili, P. K. (2020). Advances and issues in fraud research: a commentary. Journal of Financial Crime, 27(1), 92-103.

Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. Australasian Accounting, Business and Finance Journal, 16(1), 101-118.

Sengupta, K., & Das, P. K. (2023). Detection of financial fraud: Comparisons of some tree-based machine learning approaches. Journal of Data, Information and Management, 5(1), 23-37.

Singh, A., Jain, A., & Biable, S. E. (2022). Financial fraud detection approach based on firefly optimization algorithm and support vector machine. Applied Computational Intelligence and Soft Computing, 2022(1), 1-10.

Tumminello, M., Consiglio, A., Vassallo, P., Cesari, R., & Farabullini, F. (2023). Insurance fraud detection: A statistically validated network approach. Journal of Risk and Insurance, 90(2), 381-419.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. The Innovation, 2(4), 1-11.

Zhang, Z., & Jung, C. (2020). GBDT-MO: Gradient-boosted decision trees for multiple outputs. IEEE transactions on neural networks and learning systems, 32(7), 3156-3167.

Yonghong Wang is from Chengdu, Sichuan. Born in 1982, she is an associate professor at Gingko College of Hospitality Management. She holds a master's degree and obtained a bachelor's degree in management from Sichuan Normal University, and a master's degree from Chongqing University of Technology. The main research directions are project risk management, big data taxation
E-mail: 13730879813@163.com

Xiaomeng Zhang is from Chengdu, Sichuan Province. Born in 1989, she is an associate professor at Gingko College of Hospitality Management. She holds a master's degree and obtained a bachelor's degree in management from Zhengzhou University and a master's degree from Southwest Petroleum University. Her main research areas include management, big data finance, and project risk management.
E-mail: xiaomeng.zhang@gingkoc.edu.cn

Yong Yin is from Chengdu, Sichuan. Born in 1989. Worked in Chengdu Ginkgo Hotel Management College, associate professor title, master's degree, obtained a bachelor's degree in management from Xihua University, and a master's degree from Sichuan University. Her main research interests are management, project investment, and internal control.
E-mail: yong.yin@gingkoc.edu.cn

Appendix A: Formal Description of the GBDT Algorithm

The calculation of the residual r_i of each round of training is expressed as:

$$r_i = -\frac{\partial L(y_i, F_{t-1}(x_i))}{\partial F_{t-1}(x_i)} \quad (1)$$

On this basis, the decision tree is trained using the residual minimization method to optimize the model.

After the training is completed, the model is updated using the formula:

$$F_t(x) = F_{t-1}(x) + \eta \cdot h_t(x) \quad (2)$$

After multiple repetitions, the final model is the weighted sum of all decision trees:

$$F(x) = F_0(x) + \sum_{t=1}^{T} \eta \cdot h_t(x) \quad (3)$$

T is the number of iterations.

When determining the complexity of a decision tree, the depth of the tree is a very critical parameter. Increasing the depth of the tree can make the model have more understanding of the details of the data, but it also memorizes the noise and causes overfitting. A smaller tree depth cannot learn enough features from the data well, resulting in underfitting. To balance the two, a maximum depth D_{max} is set for each decision tree during training, and it satisfies:

$$Depth(T) \leq D_{max} \quad (4)$$

Here, $Depth(T)$ is the depth of the tree. This constraint can effectively mine important patterns of fraud samples from corporate sample data while maintaining a certain model complexity. The purpose of setting the maximum depth is to make the tree branching process have good generalization ability.

When each decision tree is divided, it generates a child node at a specific node until a certain termination condition is met. When the number of samples of a node in the network is too small, the model is too sensitive to a single sample or noise, resulting in a large deviation in the analysis results. To prevent overfitting, a minimum number of samples N_{min} is set on each leaf node:

$$N_{min} \leq sample\ size(R_j) \quad (5)$$

R_j represents the sample area of the j-th leaf node, and $sample\ size(R_j)$ represents the number of samples in this area. In a certain node, when the number of samples is lower than the preset minimum number of samples N_{min}, further division is stopped, and the node is used as a leaf node.

When constructing a tree, a feature must be selected for division at each division. At the same time, during the division process, a minimum information gain threshold ΔI_{min} is set to ensure that the amount of information generated by each division exceeds the threshold, otherwise no division is performed. This method can be used to measure the difference in data purity before and after the division. If the information gain is large enough, it means that the division effect is good.

The calculation formula of information gain is:

$$\Delta I = I(D) - \sum_{i=1}^{n} \frac{|D_i|}{|D|} I(D_i) \quad (6)$$

$I(D)$ represents the amount of information in the dataset D; D_i represents the subset obtained after D is divided according to a certain feature; n represents the number of subsets.

Splitting is allowed only when the information gain is above a set threshold ΔI_{min}:

$$\Delta I \geq \Delta I_{min} \quad (7)$$

Appendix B: Evaluation Index Calculation Formula

(1) Accuracy

Accuracy is a commonly used evaluation indicator, which is used to measure the correct proportion of model identification, that is, the proportion of correct classification in sample identification:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

In formula 1, TP represents the number of samples correctly identified as fraud; TN represents the number of samples correctly identified as non-fraud; FP represents the number of samples that identify non-fraud as fraud; FN represents the number of samples that identify fraud as non-fraud.

(2) Precision

Precision is used to measure the proportion of samples that are actually fraud among the samples that are judged as fraud by the model:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

The higher the Precision, the higher the proportion of real fraud samples when the model identifies fraud samples.

(3) Recall

Recall is utilized to evaluate the model's ability to identify fraud samples:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

In the identification task, a high recall rate can ensure that most fraud behaviors can be identified in a timely manner, thereby avoiding greater losses caused by fraud behaviors.

(4) AUC and ROC curve

The area under the ROC curve is AUC. The larger the AUC value, the stronger the model's ability to identify fraud and non-fraud samples:

$$FPR = \frac{FP}{FP+TN} \quad (4)$$

$$TPR = \frac{TP}{TP+FN} \quad (5)$$

In formulas 4 and 5, FPR represents the false positive rate, and TPR represents the true positive rate.

(5) Kappa coefficient

The Kappa coefficient is utilized to measure the degree of consistency between the model's predicted value and the true value, especially in the case of class imbalance. It is calculated as follows:

$$Kappa = \frac{P_o - P_e}{1 - P_e} \quad (6)$$

P_o is the observed accuracy; P_e is the expected accuracy, and its value is between -1 and 1. 0 means the same consistency as random prediction.