

Received 2 June 2024, accepted 20 June 2024, date of publication 27 June 2024, date of current version 8 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3420243

## RESEARCH ARTICLE

# Intelligent BiLSTM-Attention-IBPNN Method for Anomaly Detection in Financial Auditing

SHUIXIANG WANG 

Department of Finance, China University of Mining and Technology, Xuzhou 221116, China

e-mail: 4977@cumt.edu.cn


This work was supported in part by the National Natural Science Foundation of China under Grant 52274161, and in part by the Higher Education Philosophy and Social Science Fund of Jiangsu under Grant 2021SJA1017.

**ABSTRACT** Anomaly detection is a fundamental requirement in financial auditing, its detecting results can be used to correct the defects and predict risks for audited enterprise. However, with the auditing data becoming very huge, the anomaly detection error probabilities and material misstatement risk will be significantly increased. In this case, it is essential to develop an intelligent anomaly detection technology to address above problems. For these reasons, this paper develops a new intelligent anomaly detection method that combines the advantages of bidirectional long-short term memory (BiLSTM), improved backpropagation neural network (IBPNN) and an attention mechanism, also it possesses the strong abilities of nonlinear predicting, long time series feature extracting and important information attention. Furthermore, we present a correlation analysis algorithm to process the various types of huge financial auditing data, which can effectively remove the irrelevant information and discover the correlation relationships in financial auditing data before the BiLSTM-Attention-IBPNN method runs on it. The experimental results proved that our proposed method has better performances and evaluation results in anomaly detection compared with the state-of-the-art methods, also significantly improves the anomaly detection quality and efficiency for financial auditing.

**INDEX TERMS** Anomaly detection, attention mechanism, bidirectional long-short term memory, financial auditing, improved backpropagation neural network.

## I. INTRODUCTION

Generally, the main purpose of financial auditing is to extract, analyze and evaluate the financial data of enterprise, so as to supervise the authenticity, reasonability and efficiency of its financial revenues and expenditures. To realize this goal, it requires the auditors possessing the ability of identifying, evaluating and detecting the anomaly of auditing material to produce and achieve a final auditing opinion about the credibility of financial statements. Similarity with the financial auditing goals, the auditing quality denotes the joint probability distribution density of detecting and reporting the material anomaly. Currently, how to effectively improve the financial auditing quality and efficiency, and quickly meet audit requirements and objectives have been become the focus of financial auditing researches [1], [2], [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Genoveffa Tortora .

Anomaly detection in financial auditing is a fundamental requirement of auditors reviewing financial material, which mainly includes (but not to be restricted), wrong accounting types combined, incorrect monetary value symbols, abnormal proportion of money, and wrong account patterns, etc. The anomaly detection results can be used for correcting audit defects and predicting financial risks, also can be applied to improve the levels of managements and operations for audited enterprises [4], [5], such as help company's managers to primary the current competition positions of the company, identify the differences with competitors, and draw up the best decisions and development plans, etc.

Normally, the experienced auditors can quickly find the anomalous information based on their professional knowledges, however, it is also considered time consuming and usually limited by the auditor's cognitive levels and scopes, the rules and regulations of government. Furthermore, the manual evaluating errors probability and material mistake

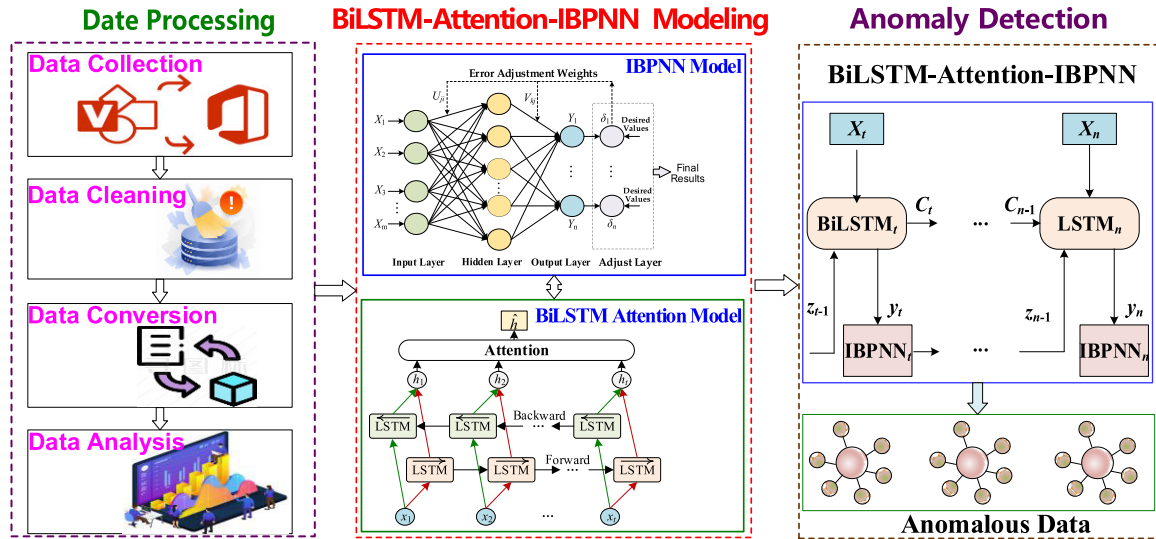


FIGURE 1. The overall architecture of our proposed method.

risks will be significantly increased when the financial auditing data become very huge. For these reasons, the anomalous information is not easy to be detected in the huge financial auditing data [6], [7], [8]. In addition, the traditional detection technology cannot simultaneously meet the requirements of quality and efficiency in current financial auditing conditions [9], [10].

In this case, it is essential to develop an intelligent detection technology for auditors to quickly find the anomalous information in financial auditing big-data environments and to decrease the misstatement risk probability. In recent years, the rapid developing artificial intelligence (AI) technology can provide a good tool for anomaly detection, which can be used to analyze and evaluate the huge data in the financial auditing and to help the auditors quickly discover the relationships and rules hidden in the auditing material [11], [12], [13]. Furthermore, the auditors can detect the anomalous information and perceive the unusual economic business, and judge the company future development situation according to the detection results of AI technology [14], [15].

Now the AI technologies have been widely applied in different occasions, for example, traffic flows management, company risk, instrument life, etc. As for the financial audit field, the applications of AI techniques can improve the anomaly detection quality and efficiency, also it will be become an important tool in the future [16], [17]. The typical AI techniques [18], [19], [20] mainly include backpropagation neural network (BPNN), partial least squares (PLS), long-short term memory (LSTM), convolutional neural network (CNN), recurrent neural network (RNN), dynamic learning neural network (DLNN), and deep belief neural network (DBNN), etc. Among the above AI techniques, the LSTM and BPNN exhibits superior ability for anomaly detection. Currently, many researchers have used them into the financial field. For example, Raval et al. [21] developed a

trusted explainable LSTM model to classify fraud patterns on credit card transactions. Alghofaili et al. [22] presented a deep learning-based technique LSTM to detect the financial fraud, which enhances the current detection techniques as well as the detection accuracy in the light of big data. Alshingiti et al. [23] constructed a deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN. Jan [24] developed two powerful deep learning algorithms RNN and LSTM to detect the financial statement fraud for sustainable development of capital markets under information asymmetry. Dai and Zhu [25] developed an audit opinion prediction method using the combination of deep belief neural network and LSTM to predict the audit opinions in financial auditing statements. Chen [26] developed a network structure that integrates BPNN and PLS to analyze and process the financial and management accounting data. Liao et al. [27] used a Backpropagation (BP) neural network-based model to study corporate financial risk analysis and internal accounting management. Zhou et al. [28] presented a big data mining approach of Particle Swarm Optimization (PSO) BP neural network for financial risk management in commercial banks with internet of things (IoT) deployment. Bo et al. [29] built a BP neural network simulation model to predict the degree of synergy between financial innovation and economic growth based on the practice. Yang and Xi [30] presented a fast-warning method of financial risk behavior based on BP neural network.

Although the above-mentioned traditional LSTM and BPNN methods can be utilized to detect anomaly in financial auditing, they still exist some limitations [31], [32], [33]:

(1) The traditional LSTM method has a long-time memory capability but lacks the complex characteristics prediction ability, only uses the forward dependencies and cannot display the importance of different information in the training process.

(2) In spite of the conventional BPNN exhibits superior prediction ability among the above-mentioned AI techniques, but it has no long-time series feature extracting ability and easily falls into local optimization trap, also exhibits low convergence speed.

(3) Otherwise, the CNN, RNN, DLNN and DBNN methods only consider the local anomaly features, have no long-time series feature memory ability.

Generally, the bidirectional LSTM (BiLSTM) has a better capability to extract the contextual dependencies from both directions at the same time, also can provide more precise temporal sequential predictions. And the attention mechanism can increase the influence of important information by assigning greater weights for the importance information. Furthermore, the improve BPNN (IBPNN) by adding an adaptive error adjustment weight in the back propagation can greatly improve the convergence rate and avoid local minimum. For these reasons, this paper proposes a new intelligent anomaly detection method that combines the advantages of BiLSTM, IBPNN and attention mechanism, which can effectively overcome the weak nonlinear prediction property and unable attention important information for traditional LSTM, and greatly improve the convergence rate, long-time series memory capability and avoid local minimum for conventional BPNN. Moreover, the proposed BiLSTM-Attention-IBPNN method can simultaneously improve anomaly detection quality and efficiency for financial auditing. The main contributions of this study are summed up as:

(1) This paper develops a new intelligent method named BiLSTM-Attention-IBPNN to detect the anomalous information in financial auditing, which simultaneously possesses the strong nonlinear predicting characteristics, important information attention mechanism and long-time series feature extracting ability, significantly improves the anomaly detection quality and efficiency for financial auditing.

(2) This paper presents a correlation analysis algorithm to process the various types data for financial auditing, which can effectively remove the irrelevant information and discover the valid correlation relationships in the financial auditing before the BiLSTM-Attention-IBPNN method runs on it.

The overall architecture of this paper is illustrated in Figure 1, it mainly includes three stages: date processing stage, BiLSTM-Attention-IBPNN modeling stage, and anomaly detection stage. In the first stage, it is carried out through data collection, data cleaning, data conversion and data correlation analysis. During the second stage, the mathematic model of BiLSTM, IBPNN and attention mechanism will be established. Finally, in the third stage, the BiLSTM-Attention-IBPNN method will be proposed to detect the anomalous information in financial auditing.

The rest organizational structure of this paper is arranged as following: the methodology is given in Section II; and the experimental results and discussion is illustrated in Section III; following by the conclusions in Section IV.

## II. METHODOLOGY

The overall architecture of the proposed anomaly detection method is divided into three stages (see Figure 1) including: date processing stage, BiLSTM-Attention-IBPNN modeling stage and anomaly detection stage, which will be described in detail in the subsequent subsections.

### A. DATA PROCESSING

Before processed the anomaly detection in financial auditing, it is necessary to carry out the date processing for large amount of the financial auditing date. The date processing refers to collect, clean, convert and analyze the data from the financial auditing materials, and store into the database server according to the principle of audit classifications and hierarchies. The process of date processing mainly includes the data collection, data cleaning, data conversion and data correlation analysis.

#### 1) DATA COLLECTION

The data collection method for financial auditing is similar with the traditional financial collecting technique. The sources of auditing data mainly come from the financial auditing report or the internal network of the enterprise. After the auditing data is selected, it will be stored in the local temporary databases, and converted into standard format of requirements. During the data collection, it needs a detailed and in-depth understanding according to the regulations of financial auditing to decide the data collecting ways and objectives. Usually, these collected data mainly include financial statement auditing data, economic benefit auditing data, regularity auditing data, etc. Moreover, the data collecting should be complied with the following rules: (1) The collected data should be satisfied the requirements of auditing schemes; (2) Data selection should be followed a completely understanding for financial auditing process; (3) Data collection should not be restricted into the special auditors.

#### 2) DATA CLEANING

Generally, the number of input data is not equal to the amount of collected data, it must be carried out the process of data cleaning due to the complexity of financial auditing data, furthermore, the collected data always contains some redundant and duplicate information. The purpose of data cleaning is to eliminate the irrelevant attributes for financial auditing, and remove the redundant and duplicate information, also will be served for the following financial auditing process. Normally, the procedure of data cleaning mainly contains: confirmed inputting data; modified false values; replaced null values; eliminated redundant data; ensured auditing values within the definition domains. Based on the different financial auditing data conditions, now the commonly used data cleaning methods mainly include: (1) Ignored tuple method; (2) Filled missing value method; (3) Truth conversion method; (4) Data normalization method.

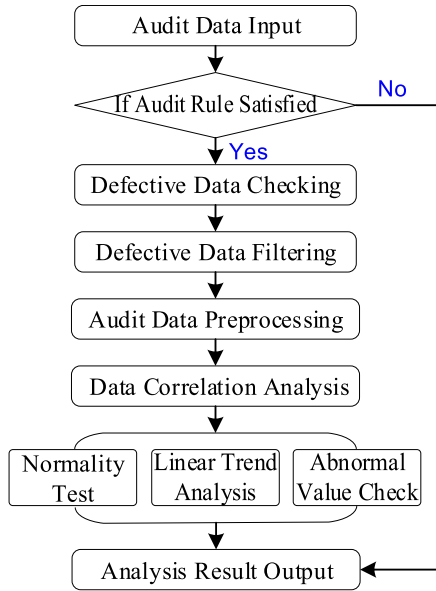


FIGURE 2. The procedure of data correlation analysis.

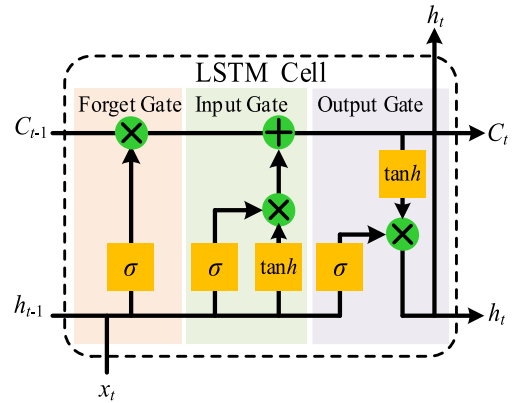
3) DATA CONVERSION

Before better carry out data analysis, we need to uniform the data format through data conversion. Generally, the date conversion is referred to convert the different types data into the unified data format, it mainly includes the dimensionality transformation, field constraint, dataset conversion. There are a variety of techniques used in the date conversion, the current commonly used methods mainly including: (1) Changed data format; (2) Adapted character encode; (3) Adjusted time format; (4) Changed measuring unit; (5) Converted number; (6) Converted data type.

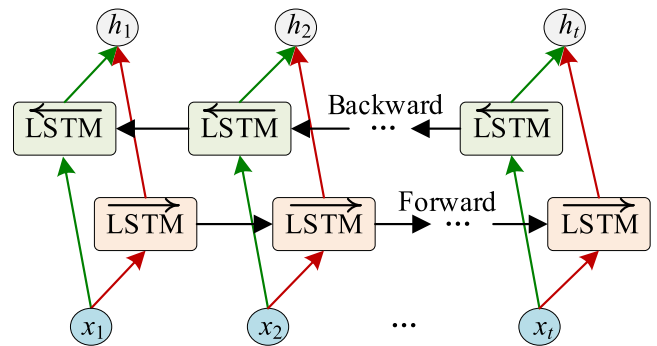
In addition, the data conversion process also can be summarized as: defining conversion requirements, evaluating the source data, extracting source data, data transformation, data loading, data validation, data maintenance, data testing, data deployment, etc.

4) DATA CORRELATION ANALYSIS

The data correlating analysis is regarded as a powerful data processing tool, which can be used to divert the financial auditing data. Its major purpose is to extract, transform, analyze, and process the huge amounts of data coming from financial auditing database, and dig out the defective data to help auditors making decisions. The procedure of correlation analysis for financial auditing data is illustrated in Figure 2. The first step is to build up the objective of correlation analysis and clarify the types of detection data; the second step is to establish the relevant algorithms including: defective data checking, defective data filtering and audit data preprocessing; the last step is to discover special correlation analysis through normality test, linear trend analysis and abnormal value check, and obtain the correlation relationships of auditing data.



(a) LSTM cell architecture



(b) BiLSTM architecture

FIGURE 3. The architecture of BiLSTM and an LSTM cell.

B. BiLSTM-ATTENTION-IBPNN MODELING

1) BiLSTM MODEL

The LSTM cell structure [19], [22] has been proved to be capable of capturing the long-term dependencies in sequences data (see Figure 3a), which includes input gate, forgotten gate, and output gate, moreover, these gates can effectively determine the information inflow and outflow. However, the conventional LSTM only can use of forward dependencies and inevitably filters out useful information due to the long-term gated memory chain. While the BiLSTM structure employs the hidden states of both forward and backward propagations of LSTM layers, it has a better capability to extract the contextual dependencies from both directions at the same time, also can provide more precise temporal sequential predictions for anomaly detection. The BiLSTM model architecture is illustrated in Figure 3b, it contains two parallel LSTM layers in both propagation directions. The mathematical definition of cell in the LSTM can be expressed as:

$$\begin{cases}
 f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \\
 i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \\
 o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \\
 \tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C) \\
 C_t = C_{t-1} \cdot f_t + i_t \cdot \tilde{C}_t \\
 h_t = o_t \tanh(C_t)
 \end{cases} \quad (1)$$



where  $W_f$ ,  $W_i$ ,  $W_o$ ,  $W_C$  and  $b_f$ ,  $b_i$ ,  $b_o$ ,  $b_C$  denote the weight and bias of forget gate, input gate, output gate and memory cell, respectively;  $f_t$ ,  $i_t$ ,  $o_t$  represent the states of the forget gate, input gate and output gate;  $C_t$  and  $C_{t-1}$  refer to the cell states at time  $t$  and  $t-1$ ;  $\hat{C}_t$  represent the candidate states.;  $\sigma$  and  $\tanh$  denote the non-linear activation functions.

For simple presentation, the Equation (1) can be abbreviated as:

$$h_t = f_{LSTM}(h_{t-1}, x_t) \quad (2)$$

where  $f_{LSTM}$  represents the operation of LSTM.

According to the mathematical model of LSTM, the expression of BiLSTM is calculated as:

$$\begin{cases} \bar{h}_t = \bar{f}_{LSTM}(\bar{h}_{t-1}, \bar{x}_t) \\ \tilde{h}_t = \tilde{f}_{LSTM}(\tilde{h}_{t-1}, \tilde{x}_t) \\ h'_t = (\bar{h}_t \oplus \tilde{h}_t) \end{cases} \quad (3)$$

where  $h'_t$  represents the final output of BiLSTM; “ $\rightarrow$ ” and “ $\leftarrow$ ” refer to the forward propagation and the backward propagation;  $\oplus$  represents the concatenation operation and uses to sum the forward and backward output components.

## 2) ATTENTION MECHANISM MODEL

Generally, the BiLSTM cannot display the importance of different information in the training process, and always loses some important information in anomaly detection when processing the long time series auditing data. Therefore, to strengthen the more important information and weaken other irrelevant information for anomaly detection in the long time series financial auditing, the attention mechanism model is selected to weight the different size for the BiLSTM outputs, which can focus on the more desirable information and dismisses unnecessary information. The attention mechanism originates from the simulation of human brain attentional characteristics, its basic principle is to assign the different weights according to the importance degree of the outputting information, that is to assign greater weights for the critical features and smaller weights for the other features, thereby increasing the influence of important information on the detection results. The structure of attention mechanism model is illustrated in Figure 4, suppose the output of BiLSTM is denoted as  $[h'_1, h'_2, \dots, h'_n]$ , during the vector  $h'_i$  training process, the attention mechanism dynamically modifies the weights of each time step and calculates the weight coefficients of each vector  $h'_i$ , the computation process for attention mechanism is expressed as follows:

$$\begin{cases} u_i = \tanh(w_s h'_i + b_s) \\ \lambda_i = \text{soft max}(u_i) = \frac{\exp(u_i^T)}{\sum_{i=1}^n (u_i^T)} \\ \hat{h} = \sum_{i=1}^n (\lambda_i h'_i) \end{cases} \quad (4)$$

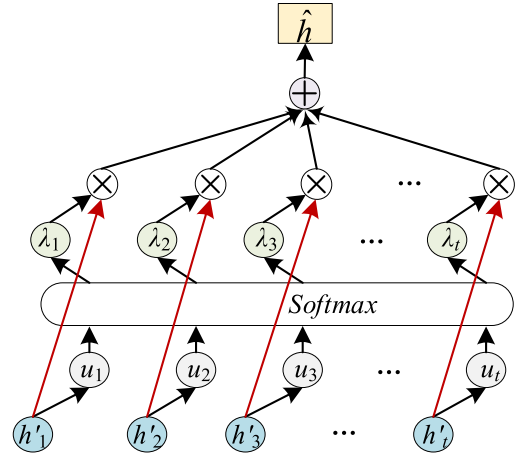


FIGURE 4. The structure of attention mechanism model.

where  $u_i$  denotes attention vector corresponding to the vector  $h'_i$ ;  $\lambda_i$  represents the weight coefficients of  $u_i$ ;  $\hat{h}$  denotes the attention vector;  $w_s$ ,  $b_s$  refer to the weight matrix and bias matrix of attention mechanism model, which can be continue to be optimized with the attention mechanism training process.

## 3) IBPNN MODEL

The traditional BPNN model is a multi-layer feedforward network with the reverse error propagation structure [25], and can solve a nonlinear problem. However, it also has some limitations such as low convergence speed and easily falls into local minimum. In addition, with different initial setting, the network converges to different local minima in the training process, which makes the performance of the BPNN unstable. For these reasons, this paper develops an improved BPNN model by adding an error adjustment weight with adaptive learning rate in back propagation, which can greatly improve the convergence rate and avoid local minimum. The basic structure of IBPNN is illustrated in Figure 5, it mainly includes input layer, output layer, hidden layer and error adjustment layer. suppose the IBPNN has  $m$  inputs  $x_i, i = 1, \dots, m$ ; and  $n$  outputs  $y_k, k = 1, \dots, n$ . The hidden layer has  $l$  neurons  $h_j, j = 1, \dots, l$ .

During IBPNN training process, it can be constantly adjusted the initial setting and threshold, and limited the expected error values within the designed ranges. When the goal is realized, the training procedure will be ended. Usually, the error function between expected and actual output of IBPNN can be expressed as:

$$e = \frac{1}{2} \sum_k (Y_k - \hat{Y}_k)^2 \quad (5)$$

where  $\hat{Y}_k$  denotes the expected value of output;  $Y_k$  represents the actual value of output.

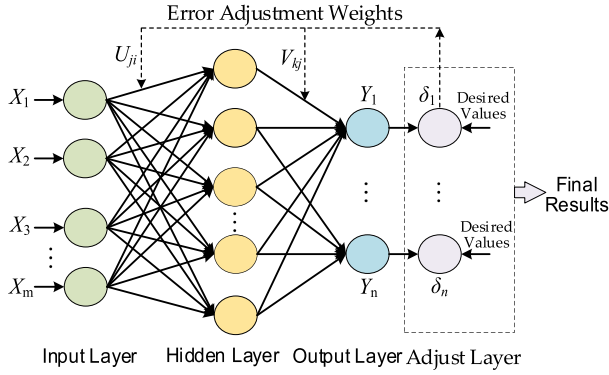


FIGURE 5. The structure of IBPNN model.

For the hidden layer, there are

$$\begin{cases} I_j = \sum_{i=1}^m \omega_{ji}x_i \\ H_j = f\left(\sum_{i=1}^m U_{ji}\omega_{ji}x_i\right) \end{cases} \quad (6)$$

where  $I_j$  and  $H_j$  refer to the input and output of  $j$  neuron at hidden layer;  $\omega_{ji}$  represents the weight from input layer to hidden layer;  $U_{ji}$  denotes the error adjustment weight between input and hidden layers;  $f(\cdot)$  represents the activation function of hidden layer neuron.

The  $k$  neuron output  $Y_k$  in output layer can be expressed as:

$$Y_k = g\left(\sum_{j=1}^m V_{kj}\omega_{kj}H_j\right) \quad (7)$$

where  $\omega_{kj}$  represents the middle from input layer to output layer,  $V_{kj}$  denotes the error adjustment weight between hidden and output layers;  $g(\cdot)$  denotes activation function of the output layer neuron.

According to the Equation (6) and (7), the Equation (5) can be rewritten as:

$$e = \frac{1}{2} \sum_k \left( g\left(\sum_{j=1}^m V_{kj}\omega_{kj}f\left(\sum_{i=1}^n U_{ji}\omega_{ji}x_i\right)\right) - \hat{Y}_k \right)^2 \quad (8)$$

The error adjustment weights  $U_{ji}$  and  $V_{kj}$  can be calculated as:

$$\begin{cases} U_{ji}(L+1) = U_{ji}(L) + \Delta U_{ji}(L+1) \\ V_{kj}(L+1) = V_{kj}(L) + \Delta V_{kj}(L+1) \end{cases} \quad (9)$$

where  $L$  denotes the learning times,  $\Delta U_{ji}(L+1) = \eta \frac{\partial^2 e}{\partial I_j \partial H_j}$  and  $\Delta V_{kj}(L+1) = \eta \frac{\partial^2 e}{\partial H_j \partial Y_k}$  represent the corrections for  $U_{ji}$  and  $V_{kj}$ ;  $\eta$  is the learning rate,  $\frac{\partial^2 e}{\partial I_j \partial H_j}$  denotes the negative gradient between input and hidden layers;  $\frac{\partial^2 e}{\partial H_j \partial Y_k}$  represents the negative gradient between hidden and output layers.

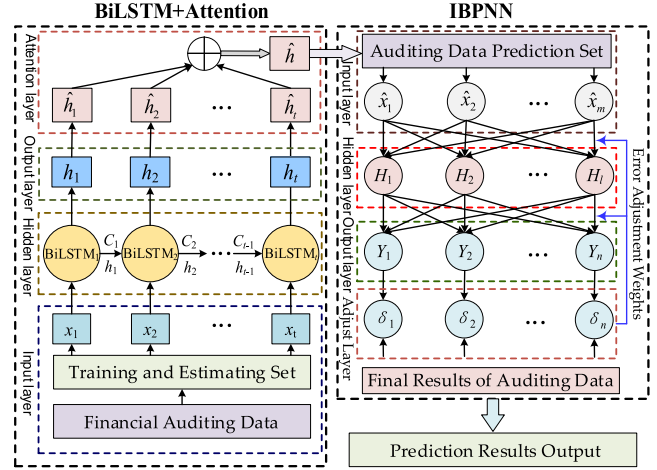


FIGURE 6. The structure of BiLSTM-Attention-IBPNN model.

#### 4) BILSTM-ATTENTION-IBPNN MODEL

Normally, the traditional BPNN has superior self-learning, self-adaptation and generalization ability, it is very suitable to predict the complex nonlinear characteristics for auditing data, however, it has no long-time series feature memory ability and easy fall into local optimization trap. While the conventional LSTM possess the advantage of long-time memory and training capabilities, but lacks the complex characteristics prediction ability and cannot display the importance of different information in the training process. In this case, the developed BiLSTM-Attention-IBPNN method can effectively overcome the weak nonlinear prediction property and unable attention important information for traditional LSTM, and greatly improve the convergence rate, long-time series memory capability and avoid local minimum for conventional BPNN. Also, it can effectively improve the anomaly detection quality and efficiency in financial auditing.

The integration model structure of BiLSTM-Attention-IBPNN is shown in Figure 6, it mainly includes BiLSTM-Attention module and IBPNN module, where the BiLSTM-Attention module contains the input layer, hidden layer, output layer, and attention layer. The final output of BiLSTM-Attention will be regarded as the initial input of IBPNN (including the input layer, hidden layer, output layer and adjust layer) to achieve the data transmitting from BiLSTM-Attention. By this way, the IBPNN could further predict the anomaly data coming from the BiLSTM-Attention and output the final detection results.

In the training process of the BiLSTM-Attention-IBPNN, the training dataset will be used to determine the hyperparameters for BiLSTM-Attention-IBPNN such as the neurons and network layers. Generally, the appropriate numbers of neurons and network layers have an important impact on the quality of the output of BiLSTM-Attention-IBPNN, for example, if the number is too small, the BiLSTM and IBPNN are not easy to fit; if the number is too large, the generalization ability of the BiLSTM-Attention-IBPNN will decrease. Therefore, in this paper, we adopt the cross-validation

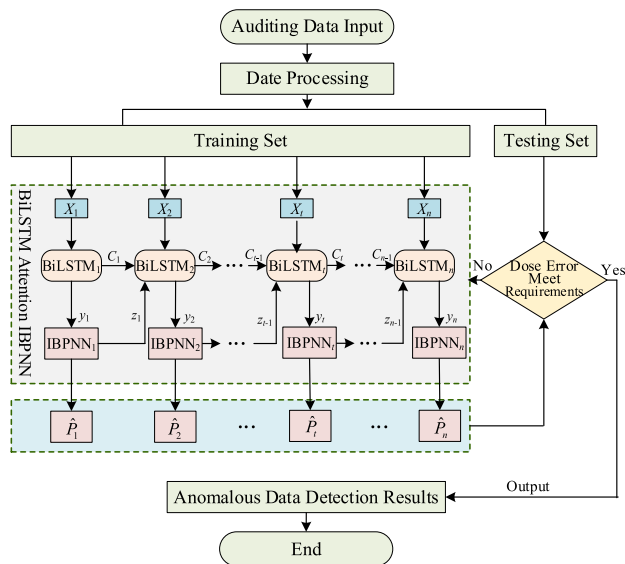


FIGURE 7. The detection process of anomalous data.

method [34] to determine the optimal hyperparameters for BiLSTM-Attention-IBPNN. Specifically, we validate 2 ~ 5 layers for BiLSTM model and 5 ~ 20 neurons for BiLSTM each layer; also try 2 ~ 5 layers for IBPNN model and 10 ~ 30 neurons for IBPNN each layer. During the cross-validation tests, we choose the activation function as sigmoid function, dropout parameter as 0.1, the maximum number of iterations as 100, learning rate as 0.001, batch-size as 50, and the data input and output dimensions as 1. According to the 200 cross-validation trials results between BiLSTM and IBPNN, we select the best combination as follows: the BiLSTM possesses 3 layers and 12 neurons per layer, while the IBPNN has 4 layers and 24 neurons per layer.

### C. ANOMALY DETECTION

The detailed detection process of anomalous data using BiLSTM-Attention-IBPNN method is illustrated as Figure 7.

(1) First of all, input the financial data of audited enterprise, then perform the data processing operations.

(2) Build the training set  $X = \{x_1, x_2, \dots, x_t\}$ , where  $t = \{1, \dots, n\}$ .

(3) Initialize the BiLSTM which mainly includes the initialization of weight matrix, maximum iterations, minimum error values, where the weight matrix is generated based on the uniformly distributed, the maximum iteration and minimum error values are determined according to the financial auditing requirements.

(4) Input the  $x_t$  into BiLSTM, then the time characteristics of data will be extracted by the BiLSTM memory unit, where the BiLSTM hidden layer includes  $t$  time series LSTM cells, and the final output of each LSTM memory cell to the output layer is  $h_t$ . After training by attention layer then the attention results  $\hat{h}_t$  will be used as the initial input  $\hat{x}_t$  of IBPNN, where  $\hat{X} = (\hat{x}_1, \hat{x}_2, \dots, \hat{x}_t, \dots, \hat{x}_n)$ ,  $\hat{x}_t = \hat{h}_t$ . During the BiLSTM-Attention-IBPNN iterative integration, the short memory

$z_t = \frac{1}{2} \sum_k \left( g \left( \sum_{j=1}^m V_{kj} \omega_{kij} f \left( \sum_{i=1}^n U_{ji} \omega_{ji} x_i \right) \right) - \hat{Y}_k \right)^2$  will be input into the BiLSTM to obtain the final results  $\hat{P} = (\hat{P}_1, \hat{P}_2, \dots, \hat{P}_t, \dots, \hat{P}_n)$ .

(5) Finally, the output of  $\hat{P}$  will be input into the training set and compare with the designed threshold values, if the errors meet the requirements, the detection results of anomalous data  $\hat{P}$  will be output. Otherwise, go back to the step 4 and continue re-performed these procedures.

## III. RESULTS AND DISCUSSIONS

### A. DATASET DESCRIPTION

To evaluate the effectiveness of the proposed method in anomaly detection, we chose three kinds typical financial auditing data, which are the education auditing database, credit card auditing database and insurance auditing database (see Table 1 ~ 3). Note that the datasets in selected auditing database are randomly divided into the two parts by assigning 70% for training set, and keeping 30% for testing set. The training samples are used to build up the prediction models, while the testing samples are then conducted to assess the performance of the proposed method. However, it can be found that the above selected auditing datasets for training are extremely imbalanced; specifically, the ratio of negative samples in all instances is less than 1%. In order to alleviate the imbalanced-sample problem, we used the well-known classification method (Synthetic Minority Oversampling Technique (SMOTE), eXtreme Gradient Boosting (XGBoost) [35] and light gradient boosting machines (LGBM) [36]) to balance the majority and minority samples in the training dataset. Furthermore, we combine the stratified fivefold cross-validation and a pairwise  $t$ -test algorithm to improve the training accuracy and preventing bias introduction during model classification. The combinations can effectively solve the imbalanced-sample problem in anomaly detection for financial auditing data. The brief descriptions for each auditing database are given as follows:

#### 1) EDUCATION AUDITING DATABASE

As shown in Table 1, this database is collected from the finance department of China University of Mining and Technology within six months, it contains total 53,279 transaction instances of financial reimbursement where 53,067 transactions are positive samples and 212 transactions are negative samples. Specially, the training dataset has 37,300 positive samples and 150 negative samples, and the testing dataset composes of 15,917 positive samples and 62 negative samples. Note that, the above each transaction record has 30 transaction attributes and 3 transaction class.

#### 2) CREDIT CARD AUDITING DATABASE

The database for the credit card auditing as Table 2 is come from the Bank of China credit card department within one month, which contains total 62,578 transaction instances of

**TABLE 1. Education auditing database.**

Description	Training Dataset	Testing Dataset
Number of instances	37300	15979
Number of attributes	30	30
Number class	3	3
Number of positive samples	37150	15917
Number of negative samples	150	62

**TABLE 2. Credit card auditing database.**

Description	Training Dataset	Testing Dataset
Number of instances	43900	18676
Number of attributes	28	28
Number class	2	2
Number of positive samples	43660	18600
Number of negative samples	240	76

**TABLE 3. Insurance card auditing database.**

Description	Training Dataset	Testing Dataset
Number of instances	41100	17553
Number of attributes	20	20
Number class	2	2
Number of positive samples	40900	17465
Number of negative samples	200	88

credit cardholders, the positive and negative samples are 62,262 and 316, respectively. Specially, the training dataset composes of 43,900 positive samples and 240 negative samples, and the testing dataset has 18,676 positive samples and 76 negative samples. To protect personal privacy, each transaction record only consists of 28 transaction attributes and 2 transaction class.

**3) INSURANCE AUDITING DATABASE**

As shown in Table 3, the insurance auditing database is come from the China Life Insurance Company Ltd. within one year, which has 20 transaction attributes and 2 transaction class for each transaction record. The total transaction instances of the database are 58,653, where the positive and negative samples are 58,365 and 288, respectively. Specially, the training dataset has 41,100 positive samples and 200 negative samples, and the testing dataset composes of 17,533 positive samples and 88 negative samples.

**B. ANOMALY DETECTION RESULTS**

Generally, the commonly used types of anomaly detection in financial auditing mainly include the wrong account patterns, understatement/overstatement of income, abnormal proportion of money, incorrect monetary value, misrepresentations or omissions in financial, etc. Please refer to the details of 30 independent variables and definitions for financial auditing in [37]. Normally, the process of anomaly detection in financial auditing can be regarded as a binary classification

**TABLE 4. Confusion matrix.**

		Predicted Class (%)	
		Non-anomaly (0)	Anomaly (1)
Actual Class (%)	Non-anomaly (0)	True Negative (TN)	False Positive (FP)
	Anomaly (1)	False Negative (FN)	True Positive (TP)

problem with four possible classification outcomes are shown in Table 4: (1) True Negative (TN), it denotes a non-anomaly data correctly classified as a non-anomaly data. (2) False Negative (FN), it represents an anomaly data incorrectly classified as a non-anomaly data. (3) True Positive (TP), it denotes an anomaly data correctly classified as an anomaly data. (4) False Positive (FP), it represents a non-anomaly data incorrectly classified as an anomaly data. In this paper, we regard the anomaly class as positive (1) and non-anomaly class as negative (0). The five typical performance evaluation metrics (accuracy, specificity, sensitivity, type I and type II error) based on the confusion matrix are illustrated as follows:

**1) ACCURACY**

The accuracy refers to the percentage of non-anomaly predicted classes, both positive and negative, which can be applied to the balancing dataset when true positives and negatives are important.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

**2) SENSITIVITY AND SPECIFICITY**

Specificity denotes the numbers of non-anomaly auditing opinions instance that are rightly assign as non-anomaly opinions, whereas the sensitivity represents the number of auditing opinions correctly classified as anomaly.

$$\begin{cases} Specificity = \frac{TN}{TN + FP} \\ Sensitivity = \frac{TP}{TP + FN} \end{cases} \tag{11}$$

**3) TYPE I AND TYPE II ERROR**

Type I Error (false positive) represents the percentage of unqualified enterprises that are incorrectly denoted as another class, while Type II Error (false negative) refers to the number of the incorrectly qualified enterprises regarded as unqualified class.

$$\begin{cases} TypeI = \frac{FP}{FN + FP} \\ TypeII = \frac{FN}{FN + TP} \end{cases} \tag{12}$$

The effectiveness of our proposed method is compared with the state-of-the-art methods: RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression methods. Note that the logistic regression method has been regarded as a typical statistical approach for financial auditing [38]. After the training models have been established based on



**TABLE 5.** The comparison results of anomalous data detection for education auditing data.

Method	Accuracy (%)	Specificity (%)	Sensitivity (%)	TypeI Error (%)	TypeII Error (%)
Proposed method	<b>97.81%</b>	<b>97.13%</b>	<b>92.32%</b>	<b>1.32%</b>	<b>6.52%</b>
RNN-LSTM [24]	91.43%	88.35%	84.47%	2.85%	9.13%
BPNN-PLS [26]	88.65%	88.67%	83.28%	3.37%	11.76%
DLNN [25]	86.12%	84.23%	80.62%	5.66%	13.18%
DBNN [11]	81.33%	79.61%	75.83%	7.35%	14.65%
RNN [6]	77.56%	76.35%	72.51%	8.92%	17.16%
CNN [1]	78.82%	77.74%	73.26%	8.74%	18.98%
Logistic Regression [36]	82.25%	80.73%	78.23%	6.16%	15.62%

**TABLE 6.** The comparison results of anomalous data detection for credit card auditing data.

Method	Accuracy (%)	Specificity (%)	Sensitivity (%)	TypeI Error (%)	TypeII Error (%)
Proposed method	<b>93.53%</b>	<b>92.84%</b>	<b>88.66%</b>	<b>1.41%</b>	<b>7.09%</b>
RNN-LSTM [24]	87.12%	84.06%	80.12%	3.06%	9.88%
BPNN-PLS [26]	84.34%	84.33%	78.94%	3.88%	13.13%
DLNN [25]	81.86%	81.91%	78.37%	6.27%	14.39%
DBNN [11]	78.53%	78.37%	75.52%	8.12%	15.26%
RNN [6]	73.29%	72.05%	69.29%	9.76%	18.89%
CNN [1]	74.55%	73.47%	70.95%	9.27%	18.26%
Logistic Regression [36]	79.31%	78.32%	74.18%	8.86%	17.12%

**TABLE 7.** The comparison results of anomalous data detection for insurance auditing data.

Method	Accuracy (%)	Specificity (%)	Sensitivity (%)	TypeI Error (%)	TypeII Error (%)
Proposed method	<b>94.05%</b>	<b>93.33%</b>	<b>91.55%</b>	<b>1.38%</b>	<b>6.87%</b>
RNN-LSTM [24]	87.62%	84.56%	80.66%	3.04%	9.12%
BPNN-PLS [26]	84.81%	84.82%	81.43%	3.76%	12.68%
DLNN [25]	82.37%	81.47%	78.85%	6.05%	14.11%
DBNN [11]	79.56%	78.82%	76.53%	7.98%	15.35%
RNN [6]	73.74%	72.56%	71.76%	9.52%	18.16%
CNN [1]	72.83%	71.94%	70.47%	9.11%	18.01%
Logistic Regression [36]	79.27%	78.13%	77.03%	8.17%	16.06%

**TABLE 8.** The detection efficiency comparison among RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN, logistic regression and our proposed method based on education auditing database.

Methods	Mean Detecting Time (s)
Proposed method	<b>126.7</b>
RNN-LSTM [24]	148.9
BPNN-PLS [26]	157.2
DLNN [25]	198.3
DBNN [11]	213.6
RNN [6]	236.8
CNN [1]	221.5
Logistic Regression [36]	332.5

the training datasets, next we will use the testing datasets to assess the generalization capability of our proposed method with the metrics of accuracy, specificity, sensitivity, type I and type II error, the comparison results are shown in Table 5 ~ 7.

Table 5 gives the comparison results of RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression with the proposed method using education auditing testing dataset. It can be seen that based on the selected evaluation

criteria our proposed method shown the best performances for anomalous data detection, it achieves a full detecting and predicting coverage of the anomalous data. Compared with the RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression methods, the overall accuracy, specificity, sensitivity have improved “6.54%, 10.38%, 11.96%, 16.87%, 20.76%, 19.43%, 15.91%”, “9.06%, 9.59%, 13.29%, 18.02%, 21.42%, 19.98%, 16.88%”, and “8.56%, 10.94%, 12.68%, 17.88%, 21.45%, 20.69%, 15.26%”, respectively. Simultaneously, the type I and type II error have decreased “1.53%, 2.05%, 4.34%, 6.03%, 7.60%, 7.42%, 5.43%,” and “2.61%, 5.24%, 6.66%, 8.13%, 10.64%, 12.46%, 7.35%”.

Table 6 illustrates the results achieved from of RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression with the proposed method using credit card auditing testing dataset. Also the selected five estimation criteria were used to evaluate the detection performances, the comparison results shown that our proposed method shown the best performances for anomalous data detection, Compared with the RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression methods, the overall accuracy,

specificity, sensitivity have improved “6.84%, 10.91%, 12.51%, 16.04%, 21.71%, 20.32%, 15.21%”, “9.48%, 10.08%, 11.75%, 15.63%, 22.41%, 20.91%, 15.64%”, and “9.59%, 12.29%, 11.63%, 14.79%, 21.90%, 19.98%, 16.33%”, respectively. Simultaneously, the type I and type II error have decreased “1.65%, 2.47%, 4.86%, 6.71%, 8.35%, 7.86%, 7.15%” and “2.79%, 6.04%, 7.30%, 8.17%, 11.80%, 11.17%, 9.47%”.

Table 7 depicts the detection results of RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN, logistic regression and our proposed method based on the insurance auditing testing dataset. According to the selected evaluation criteria, we can see that the proposed method achieves the best performances for anomalous data detection, compared with the RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression methods, the overall accuracy, specificity, sensitivity have improved “6.81%, 10.85%, 12.45%, 15.43%, 21.60%, 22.55%, 15.71%”, “9.43%, 10.02%, 12.77%, 15.54%, 22.29%, 22.94%, 16.29%”, and “11.91%, 12.41%, 13.88%, 16.39%, 21.64%, 23.06%, 15.87%”, respectively. Simultaneously, the type I and type II error have decreased “1.66%, 2.38%, 4.67%, 6.60%, 8.14%, 7.73%, 7.12%” and “2.25%, 5.81%, 7.24%, 8.48%, 11.29%, 11.14%, 9.78%”.

To show the superiority of our presented method in anomalous data detection efficiency, we also conducted the tests of the detecting efficiency based on the education auditing database. The comparison results are given in Table 8, it proves that the presented method produces faster computational efficiency than that of the other methods, the mean computing time using the proposed method reduces by 14.91%, 19.40%, 36.11%, 40.68%, 46.49%, 42.80% and 62.05% against the RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN and logistic regression methods, respectively. The reasons mainly due to that our proposed method is embedded the attention mechanism module and the adjustment layer in IBPNN, which makes the anomalous data detection most efficient.

#### IV. CONCLUSION

To improve anomaly detection efficiency and decrease error probabilities for huge financial auditing data, this paper develops an intelligent anomaly detection method that combines the advantages of BiLSTM, IBPNN and attention mechanism, and simultaneously possesses the strong abilities of nonlinear predicting, long time series feature extracting and important information attention. In addition, we present a correlation analysis algorithm to process the various types of huge financial auditing data, which can effectively remove the irrelevant information and discover the correlation relationships in financial auditing data before the BiLSTM-Attention-IBPNN method runs on it. The evaluation results demonstrate that the proposed method has better performances in anomalous data detection quality and efficiency compared with the RNN-LSTM, BPNN-PLS, DLNN, DBNN, RNN, CNN, and logistic regression methods.

Although the anomaly detection quality and efficiency for financial auditing has been improved utilizing our proposed method, there are still some issues that should be addressed in the future plan; we outline some of them as follows: (1) Exploring and applying few data pre-processing technologies for the financial auditing dataset, such as, feature selected algorithm or data-filtering approaches, and accordingly define how these technologies could be reflected on the BiLSTM-Attention-IBPNN model performances. For example, the filtering-condensing method can remove outlier entries, avoiding non-informative entries negatively affecting the training procedure. (2) In addition to the commonly used variables in anomaly detection, it is necessary to consider other non-financial variables when evaluating detection quality and efficiency, for example, average accuracy ratio, F-measure, area under curve, etc. then the financial and non-financial variables should be combined to reflecting anomalous data detection performances.

#### REFERENCES

- [1] H. Zhao and Y. Wang, “A big data-driven financial auditing method using convolution neural network,” *IEEE Access*, vol. 11, pp. 41492–41502, 2023.
- [2] Y. Ma, “Deep learning-based image processing for financial audit risk quantification in healthcare,” *Expert Syst.*, Jun. 2023, doi: 10.1111/exsy.13355.
- [3] X. Zhu, “Construction of financial auditing teaching mode based on artificial intelligence expert system,” *Boletín Técnico*, vol. 55, pp. 743–747, Nov. 2017.
- [4] M. N. Ashtiani and B. Raahemi, “Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review,” *IEEE Access*, vol. 10, pp. 72504–72525, 2022.
- [5] W. Xiguoguo and D. Shengyong, “An analysis on financial statement fraud detection for Chinese listed companies using deep learning,” *IEEE Access*, vol. 10, pp. 22516–22532, 2022.
- [6] C. Estep, E. E. Griffith, and N. L. MacKenzie, “How do financial executives respond to the use of artificial intelligence in financial reporting and auditing?” *Rev. Accounting Stud.*, May 2023, doi: 10.1007/s11142-023-09771-y.
- [7] H. Zhou, “Innovation strategy of enterprise’s financial audit informatisation in the era of industry 4.0,” *Int. J. Technol. Manage.*, vol. 84, nos. 3–4, pp. 157–176, 2020.
- [8] A. A. Almazroi and N. Ayub, “Online payment fraud detection model using machine learning techniques,” *IEEE Access*, vol. 11, pp. 137188–137203, 2023.
- [9] Y. Zhao and Y. Fang, “Financial account audit early warning based on fuzzy comprehensive evaluation and random forest model,” *J. Math.*, vol. 2022, pp. 1–10, Mar. 2022.
- [10] M. Xiong and L. Chen, “Financial risk control and audit of supply chain under the information technology environment,” *Sci. Program.*, vol. 2022, Apr. 2022, Art. no. 6157740.
- [11] Y. Chen and Z. Wu, “Financial fraud detection of listed companies in China: A machine learning approach,” *Sustainability*, vol. 15, no. 1, p. 105, Dec. 2022.
- [12] M. Werner, M. Wiese, and A. Maas, “Embedding process mining into financial statement audits,” *Int. J. Accounting Inf. Syst.*, vol. 41, Jun. 2021, Art. no. 100514.
- [13] T. Xie and J. Zhang, “Data-driven intelligent risk system in the process of financial audit,” *Math. Problems Eng.*, vol. 2022, Apr. 2022, Art. no. 9054209.
- [14] R. Shan, X. Xiao, J. Che, J. Du, and Y. Li, “Data mining optimization software and its application in financial audit data analysis,” *Mobile Inf. Syst.*, vol. 2022, Jul. 2022, Art. no. 6851616.
- [15] G. L. Gray and R. S. Debreceeny, “A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits,” *Int. J. Accounting Inf. Syst.*, vol. 15, no. 4, pp. 357–380, Dec. 2014.

- [16] M. A. Fernández-Gómez, F. García-Lagos, and J. R. Sánchez-Serrano, "Integrating corporate governance and financial variables for the identification of qualified audit opinions with neural networks," *Neural Comput. Appl.*, vol. 27, no. 5, pp. 1427–1444, Jul. 2016.
- [17] M. Cao, R. Chychyła, and T. Stewart, "Big data analytics in financial statement audits," *Accounting Horizons*, vol. 29, no. 2, pp. 423–429, Jun. 2015.
- [18] J. R. Sánchez-Serrano, D. Alaminos, F. García-Lagos, and A. M. Callejón-Gil, "Predicting audit opinion in consolidated financial statements with artificial neural networks," *Mathematics*, vol. 8, no. 8, p. 1288, Aug. 2020.
- [19] P. Ray, B. Ganguli, and A. Chakrabarti, "A hybrid approach of Bayesian structural time series with LSTM to identify the influence of news sentiment on short-term forecasting of stock price," *IEEE Trans. Computat. Social Syst.*, vol. 8, no. 5, pp. 1153–1162, Oct. 2021.
- [20] S. He, X. Sang, J. Yin, Y. Zheng, and H. Chen, "Short-term runoff prediction optimization method based on BGRU-BP and BLSTM-BP neural networks," *Water Resour. Manage.*, vol. 37, no. 2, pp. 747–768, Jan. 2023.
- [21] J. Raval, P. Bhattacharya, N. K. Jadav, S. Tanwar, G. Sharma, P. N. Bokoro, M. Elmorsy, A. Tolba, and M. S. Raboaca, "RaKShA: A trusted explainable LSTM model to classify fraud patterns on credit card transactions," *Mathematics*, vol. 11, no. 8, p. 1901, Apr. 2023.
- [22] Y. Alghofaili, A. Albattah, and M. A. Rassam, "A financial fraud detection model based on LSTM deep learning technique," *J. Appl. Secur. Res.*, vol. 15, no. 4, pp. 498–516, Oct. 2020.
- [23] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN," *Electronics*, vol. 12, no. 1, p. 232, Jan. 2023.
- [24] C.-L. Jan, "Detection of financial statement fraud using deep learning for sustainable development of capital markets under information asymmetry," *Sustainability*, vol. 13, no. 17, p. 9879, Sep. 2021.
- [25] X. Dai and W. Zhu, "Intelligent financial auditing model based on deep learning," *Comput. Intell. Neurosci.*, vol. 2022, Aug. 2022, Art. no. 8282854.
- [26] X. Chen, "The fusion model of financial accounting and management accounting based on neural networks," *Mobile Inf. Syst.*, vol. 2022, Jul. 2022, Art. no. 1587274.
- [27] H. Liao, H. Yue, Y. Lin, D. Li, and L. Zhang, "Enterprise financing risk analysis and internal accounting management based on BP neural network model," *Math. Problems Eng.*, vol. 2022, May 2022, Art. no. 8627185.
- [28] H. Zhou, G. Sun, S. Fu, J. Liu, X. Zhou, and J. Zhou, "A big data mining approach of PSO-based BP neural network for financial risk management with IoT," *IEEE Access*, vol. 7, pp. 154035–154043, 2019.
- [29] W. Bo, F. Tianyu, L. Zhiyong, and N. Xiangtian, "Research and analysis on the coordination mechanism of financial innovation and economic growth based on BP neural network," *J. Intell. Fuzzy Syst.*, vol. 37, no. 5, pp. 6177–6189, Nov. 2019.
- [30] Q. Yang and Z. Xi, "A fast-warning method of financial risk behavior based on BP neural network," *J. Circuits, Syst. Comput.*, vol. 33, no. 1, Jan. 2024, Art. no. 2450008.
- [31] P. Kavianpour, M. Kavianpour, E. Jahani, and A. Ramezani, "A CNN-BiLSTM model with attention mechanism for earthquake prediction," *J. Supercomput.*, vol. 79, no. 17, pp. 19194–19226, Nov. 2023.
- [32] H. Wei, M. Gao, A. Zhou, F. Chen, W. Qu, C. Wang, and M. Lu, "Named entity recognition from biomedical texts using a fusion attention-based BiLSTM-CRF," *IEEE Access*, vol. 7, pp. 73627–73636, 2019.
- [33] Y.-J. He, J.-S. Zhang, and C.-G. Pan, "An improved BP neural network algorithm for prediction of roadway support," *Int. J. Circuits, Syst. Signal Process.*, vol. 15, pp. 393–399, Apr. 2021.
- [34] H. Xu, B. Lv, J. Chen, L. Kou, H. Liu, and M. Liu, "Research on a prediction model of water quality parameters in a marine ranch based on LSTM-BP," *Water*, vol. 15, no. 15, p. 2760, Jul. 2023.
- [35] S. He, B. Li, H. Peng, J. Xin, and E. Zhang, "An effective cost-sensitive XGBoost method for malicious URLs detection in imbalanced dataset," *IEEE Access*, vol. 9, pp. 93089–93096, 2021.
- [36] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine," *IEEE Access*, vol. 8, pp. 25579–25587, 2020.
- [37] S. Chen, "Detection of fraudulent financial statements using the hybrid data mining approach," *SpringerPlus*, vol. 5, no. 1, pp. 1–16, Dec. 2016.
- [38] P. Hajek and R. Henriques, "Mining corporate annual reports for intelligent detection of financial statement fraud—A comparative study of machine learning methods," *Knowl.-Based Syst.*, vol. 128, pp. 139–152, Jul. 2017.



**SHUOXIANG WANG** received the B.S. degree in accounting engineering from Henan Polytechnic University, Henan, China, in 2006. She has joined the Department of Finance, China University of Mining and Technology. Her research interests include machine learning, deep learning, financial risk management, big data mining, and anomaly detection.

...