Hindawi
Mobile Information Systems
Volume 2022, Article ID 7358383, 8 pages
https://doi.org/10.1155/2022/7358383

Research Article

Financial Abnormal Data Detection System Based on Reinforcement Learning

Xuechen Hou

Xi'an Peihua University, Xi'an, China

Correspondence should be addressed to Xuechen Hou; hxc@peihua.edu.cn

Received 14 May 2022; Revised 3 July 2022; Accepted 12 July 2022; Published 2 August 2022

Academic Editor: Ateeq Ur Rehman

The fraud of financial data has seriously damaged the interests of stakeholders and hindered the healthy development of the economy. Based on the reinforcement learning theory, this paper proposes a model of intelligent analysis of enterprise financial data anomalies, constructs the difference method, and transforms nontemporal indicators into temporal indicators. The proposed model uses a convolution neural network with four hidden layers to classify, evaluate, and analyze the constructed temporal indicators of financial data. The main objective is a more effective and accurate identification of the issue. The test results show that the intelligent analysis method of financial abnormal data based on deep learning has ideal effectiveness and accuracy.

1. Introduction

Artificial intelligence technology is advancing at a breakneck pace, and the practical needs of numerous application fields are becoming increasingly urgent. The actual products in different fields are also accelerating the landing process. Simultaneously, the financial sector has begun to enter a new era of intelligence. With the rapid development of the information age and the Internet age, industrial businesses are growing more and more. As a result, more aspects of life, particularly the Internet, telecommunications, finance, Internet of Things, social medicine, aerospace, and some military equipment and networks, require relying on large and complex software and hardware systems. An enormous number of expert operations and maintenance professionals are required to deploy and maintain these large-scale complicated software and hardware systems and to assure their safe and dependable functioning. These operation and maintenance workers are frequently required to be on call 24 hours a day, seven days a week to respond to various crises and provide a positive user experience. At present, the rapid development of the economy makes the market more prosperous and enterprise competition more and more fierce. The authenticity of financial data has attracted further attention. Academia has also taken a variety of measures and methods to analyze the abnormal situation of enterprise financial data and has achieved corresponding results.

As a basic function of all financial work, anomaly detection of financial data is undoubtedly the first place for financial personnel to contact. Setting the alarm threshold in a traditional and original way is a time-consuming, labor-intensive, and unreasonable task. It necessitates not only a thorough understanding of the financial field but also a thorough awareness of the present business environment. It must also be assessed if the company is experiencing good stable growth and development. As a result, financial data anomaly detection is an essential basic technology for the intelligent management and maintenance of Internet services. The data we focus on in the financial scenario is called KPI (key performance indicator), which is a kind of time series data. As an underlying core technology of Internet service intelligent finance, KPI anomaly detection is the foundation of the whole intelligent finance and the supporting technology of most of the upper technologies of intelligent finance. Therefore, the result of KPI anomaly detection is extremely important for intelligent finance. When the KPI shows abnormalities (such as sudden increase, sudden drop, and jitter), there must be some problems in its related applications or services, which may be an early warning signal or an existing fault.

The financial business indicator curve (KPI curve) in large-scale financial systems and Internet services can well reflect the operational status of systems and services. It also serves as an important basis for analyzing the system. Therefore, monitoring the KPI curve and finding the abnormalities in the KPI curve is not only an important task for financial staff but also one of the most difficult problems to solve. Before the emergence of intelligent finance research, the main method to detect the abnormality of the KPI curve was to set a fixed threshold. For example, for different KPI curves, set a fixed threshold or range in accordance with the experience of professional financial personnel. When the curve value exceeds the set threshold or exceeds the fixed range, the system will send an alarm to remind the financial staff that there is an abnormality in a monitoring item of the current system. The financial personnel will conduct a manual analysis. The disadvantages of this method are obvious. Not all abnormalities can be measured by this fixed threshold. For example, most financial data have a certain periodicity that is related to the type of business in the enterprise. In such a scenario, a KPI curve has a peak at the midnight trough, where it is impossible to determine this situation using the threshold technique; otherwise, there will be many errors and omissions, which is not the desired result. Instead of using the historical anomaly detection technique, we intend to increase the effectiveness of anomaly detection by setting a particular depth for the anomaly detection method.

2. Related Work

To identify unexpected errors, a reinforcement learning strategy is given in which the data series' noise-to-signal ratio is reduced to ensure robustness [1]. For systematic use with PIT system anomaly, PCA, ICA, and ensemble learning algorithms are proposed [2]. [3] Intrusion detection intelligence describes a method for automatically classifying normal and abnormal brain MR images using deep transfer learning. Accuracy, detection, precision, F1 score, and receiver operating characteristics are the major performance goals for any intrusion detection system (IDS). Using reinforcement learning techniques on a hybrid IDS framework [4], it offers a large data-driven IDS strategy in wireless sensor networks [5]. This provides two simple but efficient strategies for detecting abnormal odor (outliers): (1) a self-expression model (SEM) with a norm regularizer is provided, which is trained on target odor data for coding and then a small number of abnormal odor data is utilized as previous knowledge for threshold learning; and (2) an extreme learning machine (ELM) based self-expression is presented, which inherits the advantages of ELM in solving a single hidden layer feed-forward neural network. This is inspired by the self-expression mechanism [6]. It suggests a unique strategy for anomaly identification in high-performance computing systems based on a machine (deep) learning technology, namely, a type of neural network called an autoencoder. Using certain known states of the dynamical system that describes the evolution of the financial market [7], it simulates new states by interpolating genuine states and introducing some random variables. DeepBreath, a deep reinforcement learning framework, is used to create a portfolio management system [8, 9]. It intends to build DeepRan, a deep learning-based detector for early detection and categorization of ransomware to prevent network-wide data encryption [10]. This creates a basic model for credit card fraud detection that relies on a linear regression classifier and business rules based on past payment transaction data.

Liu Min and others proposed an abnormal data detection method based on neighborhood preserving embedding and principal component analysis for the high-voltage abnormal states and verified the correctness of the model through an example. Wen Yu et al. examined the efficiency and security of China's financial market from four perspectives—economic efficiency, system risk, data security, and income forecasting—and proposed solutions to address each. Zhu Haiqi et al. proposed a data anomaly detection method based on artificial intelligence, which provides a feasible research idea for the development of operation and maintenance data anomaly detection technology, given the current situation where traditional operation and maintenance data anomaly detection requires a lot of manpower and financial resources and has low accuracy. From the perspectives of anomaly categories (attributes, topology, and mixing) and anomaly detection methods, Han Dongming et al. categorized and summarized the visual analysis work for anomaly identification of time series data (direct projection method, clustering method, and machine learning method). Deng Linlin et al. proposed a financial abnormal data monitoring and analysis algorithm. Wen Yu and colleagues analyzed the efficiency and security of China's financial market from four perspectives: economic efficiency, system risk, data security, and income forecasting. They proposed solutions to address each based on the combination of data mining and neural network. Zhang Sushi and others proposed an anomaly access detection algorithm, PCA-R, based on principal component analysis (PCA) and random tree (RT) for database access behavior. The simulation results show that data reduction using the PCA algorithm is more than 35%, and the accuracy and recall of the PCA-RT algorithm are improved by 1.78% and 9.76%, respectively. In the TPC-E database, the suggested user behavior contour vector construction method and the PCA-RT algorithm are useful for detecting anomalies in user access behaviour. Based on the findings, the advancement of deep learning technology offers a novel approach to financial data anomalous analysis. This research uses deep learning theory for abnormal financial data analysis in enterprises and proposes a model for intelligent financial data abnormality analysis.

3. Anomaly Detection of Financial Data Based on Reinforcement Learning

3.1. Judgment of Abnormal Financial Data. There are usually three aspects of abnormal financial data in enterprises, namely, abnormal articulation relationship, abnormal annual change, and horizontal industry abnormality. The data in the relevant financial statements of the enterprise that is

inconsistent with the accounting standards are referred to as an "abnormal articulation relationship" [9]. The term "abnormal annual change" refers to financial information in the annual report that is inconsistent with the enterprise's operating process, resulting in anomalies. The term "industry horizontal anomaly" refers to when an enterprise's financial data considerably outperforms those of its competitors [11–13].

3.2. Selection and Construction of Time Series Index. The model will perform better if you choose financial indicators that are likely to be anomalous. As a result, five factors are considered: the indicators chosen must be connected to the fraud problem itself [14]; sensitively represent fraud behavior; thoroughly reflect all types of fraud; be operable; and pay attention to the frequency of relevant indicators in past comparable research. In the current study, 24 nonsequential indicators from two categories have been chosen, financial indicators and nonfinancial indicators, based on the five principles mentioned above [15–17]. Financial indicators refer to the indicators that reflect the operating status of an enterprise through financial data, mainly including operating indicators, debt repayment indicators, profit indicators, growth indicators, and cash flow indicators. Nonfinancial indicators are those that are calculated using nonfinancial data. These indicators have an impact on the operation of the enterprise, such as the proportion of external directors, management's shareholding proportion, the largest shareholder's shareholding proportion, and nontradable/tradable shares. Finally, the index system is formed. In this paper, non-time series index data will be constructed into time series index data in the form of difference, ratio, and relative value. Let x_i ($i = 1, 2, \ldots, 24$) and x_i' ($i = 1, 2, \ldots, 24$) represent 24 indicators of the abnormal data of the current year and the previous year, respectively, and construct various forms of timing indicators as follows:

(i) Time series index of difference form

(ii) $X_{D-\text{value}} = x_i - x_i'$

(iii) Ratio form time series index

(iv) $X_{S-\text{value}} = x_i / x_i'$

(v) Timing index of relative value form 1

(vi) $X_{R_1-\text{value}} = (x_i - x_i')/x_i'$

(vii) Timing index of relative value form 2

(viii) $X_{R_2-\text{value}} = (x_i - x_i')/|(x_i - x_i')/2|$

This paper selects the simple and naive Bayesian classification method. Let $U = X, Y$, where U is the variable set, X is the nonclass variable set, and Y is the class variable set, based on the temporal index data created previously. According to the Bayesian formula, the probability solution formula of sample x_i belonging to category Y_i is

$$\Pr\left(\frac{Y}{X}\right) = \frac{\Pr(Y = y_i)\Pr(X = x_i/Y = y_i)}{\Pr(X = x_i)}. \tag{1}$$

where $\Pr(Y = y_i)$ and $\Pr(X = x_i/Y = y_i)$ are a priori probability and a posteriori probability of category y_i, respectively.

Because the variables are independent of each other, equation (1) can be converted into

$$\Pr\left(\frac{Y}{X}\right) = \frac{\Pr(Y = y_i)\prod \Pr(x_i/y_i)}{\Pr(x_1, \ldots, x_n)}. \tag{2}$$

The financial data studied in this paper are mainly discrete constants. For a given sample, according to the Bayesian maximum, a posteriori criterion, the class label with the largest posteriori probability for a given sample is

$$\text{argmax}_{y_i \in Y} \Pr(y_i) \prod_{i=1}^{n} \Pr\left(\frac{x_i}{y_i}\right). \tag{3}$$

In the specific processing operation process in this paper, the priori probability is obtained by the corresponding frequency of the training samples, and part $\prod_{i=1}^{n} \Pr(x_i/y_i)$ in equation (3) is also estimated by the training samples.

3.3. Intelligent Data Anomaly Detection Method. Data on operations and maintenance anomaly detection is a sequence-to-sequence task that may be considered end-to-end. The sequence-to-sequence task is primarily concerned with sequence-to-sequence mapping issues. Simply described, it is the process of creating another output sequence from a single input sequence. In deep learning, an encoder-decoder structure is a popular model framework. For example, the unsupervised algorithm's autoencoding is built and trained using the encoding decoding structure. In recent years, this model framework has often been used in image capture, which is trending in research. The earliest research using this method was in the field of machine translation. At present, the state-of-the-art neural network machine translation (NMT) model in this field still adopts the framework of the LSTM-LSTM encoder-decoder. Therefore, to be exact, encoder-decoder is not a specific model but a kind of framework. The encoder and decoder parts can make any text, voice, image, and so on. In the model selection of encoder and decoder, networks such as CNN, RNN, LSTM, and so on can be adopted. Take the neural network machine translation (NMT) model as an example. The idea of the encoder-decoder model is very simple. First, use a neural network (encoder) to encode the input sentence f into a fixed length vector and then use another neural network (decoder) to decode (based on the vector) and output the corrected sentence. As shown in Figure 1, the calculation diagram of the RNN encoder-decoder model is given.

The standard and common practice of this model framework in the present deep learning field is to encode the input sequence into an intermediate context, which is a particular length of coding, and then restore it to an output target sequence through this intermediate context. When solving the problem of sequence-to-sequence, the encoder-decoder LSTM structure has been proven to be very effective in various research fields mentioned above. This architecture consists of two models: one is used to read the input

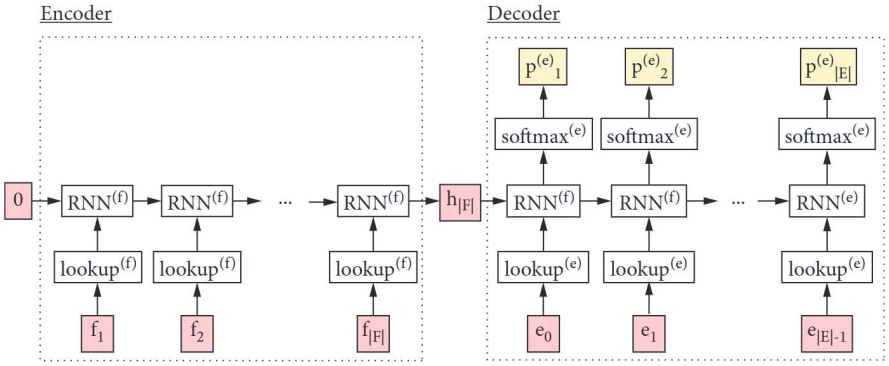

Figure 1: RNN encoder-decoder calculation graph.

sequence and encode it into a fixed length vector, and the other is used to decode the fixed length vector and output the result sequence. The collaborative use of the model provides the architecture with an encoder-decoder LSTM specially designed for sequence-to-sequence problems. We regard financial data detection as a sequence-to-sequence problem. In financial data anomaly detection, the sequence can be understood as a time series. When we give a time series, we want to get another time series corresponding to it. Such a task is called the sequence-to-sequence task. The encoder-decoder architecture is commonly used in the sequence-to-sequence problems. Theoretically, the encoder converts the input into a potential representation, which the decoder decodes and restores it to its original state. The encoder-decoder structure is a lossy compression approach. It also contains a noise reduction function and allows it to filter abnormal points or sequences.

Therefore, in this method, we trained an LSTM encoder-decoder model to reconstruct the normal KPI time series we have mastered. The input is a fixed length time series to the LSTM encoder, and the output of the model is a fixed length vector representing the internal representation of the input sequence. After our experiment, the input length is 256, and the number of memory units is 16 which is also the length of the output vector. The LSTM decoder translates the learned input sequence of internal representation into the correct output sequence. Like the ordinary LSTM, it uses a sensing layer as the output of the network, outputting the output sequence of each time step with the same weight. There is a problem here. We must connect the encoder and decoder, but their input and output are inconsistent. The encoder will produce the output of a two-dimensional matrix, and the decoder is also an LSTM network. It needs a 3D input (sample, time step, and feature) to generate decoding sequences of different lengths defined by the problem, as shown in Figure 2.

4. Experimental Analysis of the Financial Data Anomaly Detection Method

When a large financial system is running, a good deal of relevant data will be generated. The data can reflect the problems existing in the current system to some extent, or we can find out some problems existing in the system

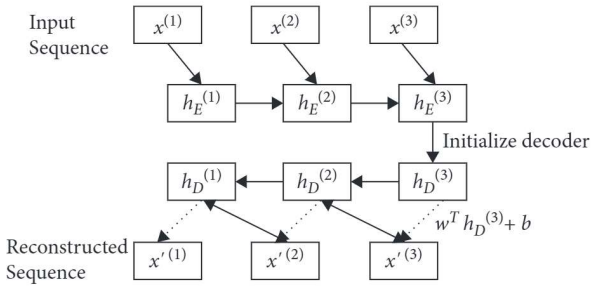

Figure 2: LSTM encoder-decoder.

through the analysis of these data. Most of the existing large-scale financial systems in the market use special financial monitoring tools to collect these data, such as open source monitoring projects such as ZABBIX, Nagios, and Ganglia.

This mature financial software can undertake distributed system and network monitoring. This may track not only the status of a single point financial operation but also the overall health status of the whole financial business system, as well as the performance changes and indications of each interface. This data will be converted into a fixed and unified format through financial software and then be imported into the operation and maintenance database we care about. In these financial monitoring projects, some simple financial data anomaly detection functions are integrated, but these simple functions are not enough to meet the concerns in the field of operation and maintenance, so they will not be repeated here.

The data collected by the financial monitoring projects include some performance indicators and system status indicators of key concern. They are usually time series collected at fixed time intervals. The data will form some potential connections and have some specific laws. Generally, KPI curves are often cyclical, with cycles ranging from days to weeks depending on applications, user patterns, and other factors. As a result, each KPI often requires thousands of points to adequately represent its behaviour over time. The idealized time series is compared to the real KPI data in Figure 3.

As illustrated in Figure 4, we have chosen to provide some representative financial data. The maximum time constraint is a week. Most of the financial data have a defined

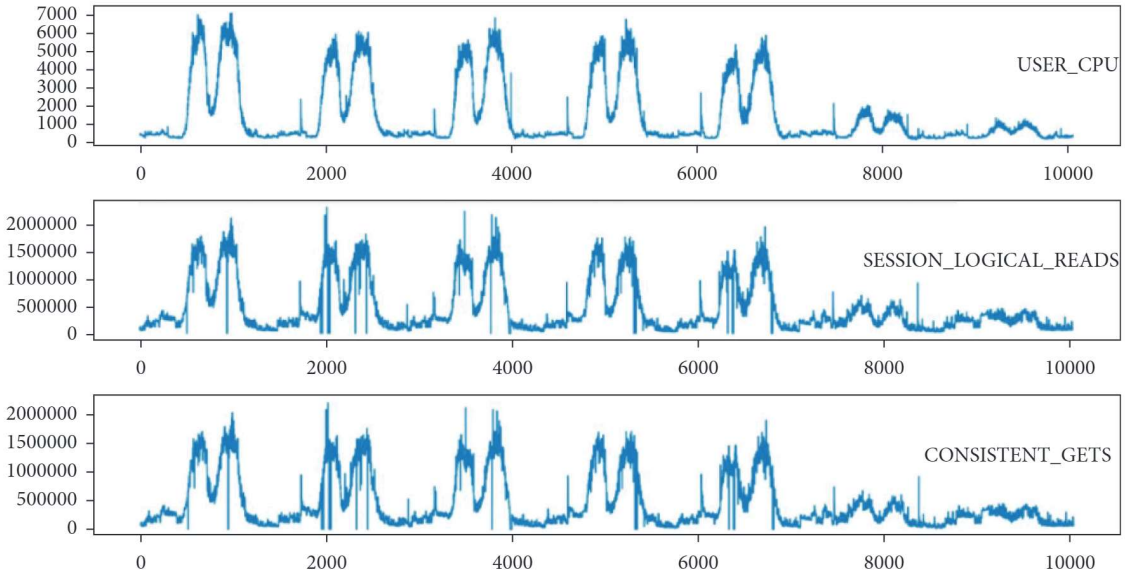

Figure 3: Examples of operational data.

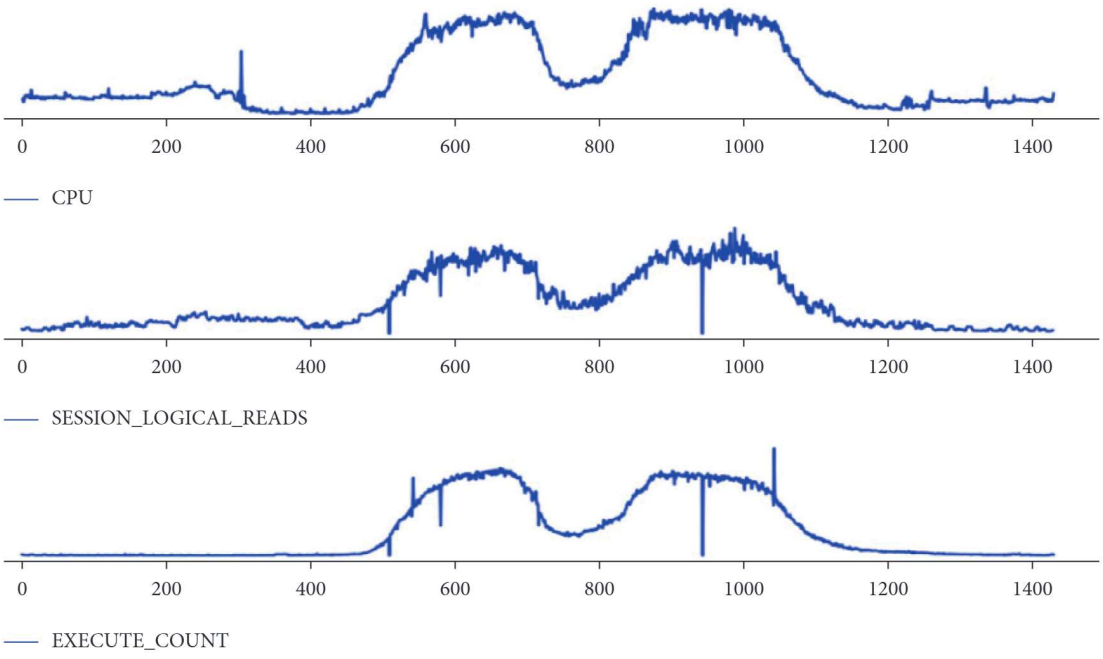

Figure 4: Comparison of data.

frequency that is connected to the business. On working days, the peak times might be in the morning and afternoon or at lunch break. These data are referred to as periodic KPI. There are also certain data on the interaction of the system's internal interfaces that are always kept at a constant and stable level, i.e., stable KPI. In addition to the two, there is an unstable KPI whose performance is chaotic and devoid of any guidelines. Dealing with anomaly detection is a hard job and is considered impossible in many situations.

The two types of data for the experimental part have been chosen for the present work. The daily operation and maintenance data are taken from local insurance firms, while the daily operations and maintenance data are chosen from Baidu, which is being released by Tsinghua University in collaboration with Baidu. In comparison, the daily operation and maintenance data of insurance companies contain more normal samples, and the abnormal samples are relatively scattered. According to the communication with customers, the abnormal samples are all made by manual adjustment. The operation and maintenance data from Baidu also contain many normal samples, but the abnormal samples are relatively concentrated. Most of them are abnormal periods (there are exceptions in a time series) rather than abnormal points.

Table 1: Comparing the data of company 1 and company 2.

Dataset	Company 1	Company 2
Total points	317522	268952
Missing points	1117/0.35%	1451/0.54%
Anomaly points	16113/5.07%	42/0.01%

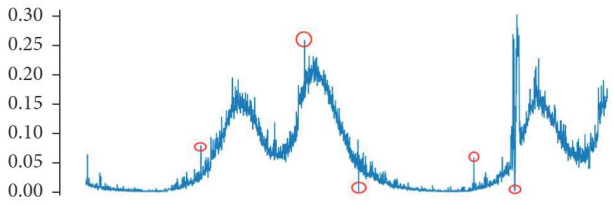

Figure 5: Company 1 data example, noise is large, and some abnormal points can be directly observed.

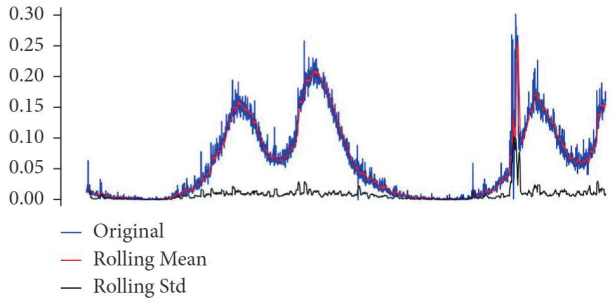

Figure 6: Rolling mean and rolling STD of company 1 data.

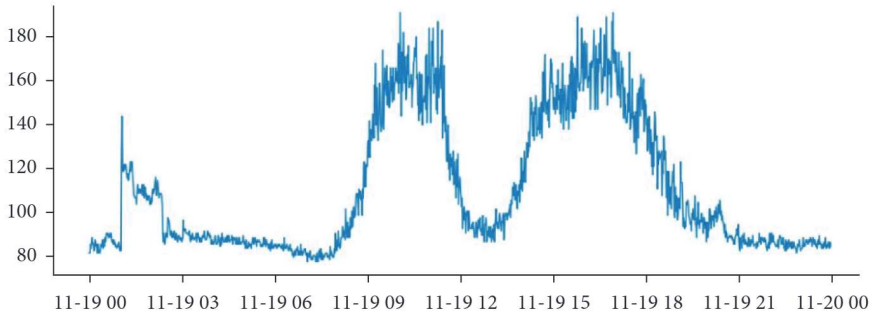

Figure 7: As an example of the data of company 2, it is not easy to observe the abnormal point directly, but there is also a lot of noise.

The following is a comparison of the data of the two data sets (Table 1).

All our algorithms calculate an outlier for each point, and we can select the threshold for judgment. Once the outlier of a point is greater than the threshold, an alarm will be triggered. In this way, anomaly detection is like a classification problem. We have tested our method on two data sets in the actual scene. To measure the performance of the model, we calculated recall and F-score under different thresholds. We also calculated the mean absolute error (MAE) and mean square error (MSE) as evaluation indexes. In addition to the delay between the first alarm point and the actual detection point in each scene, we also calculated the difference between the first alarm point and the actual detection point. After we completed the missing points, the two groups of data are continuous time series with a time interval of one minute. In the financial data from company 1, their values are relatively small and there is only one-dimensional data. Their abnormalities often appear in the form of abnormal sequences, and therefore, they have continuous abnormal points. In the financial data from company 2, there are 22 dimensions of data with few outliers and even negligible ones. We divide the data set into a training set and a test set in accordance with the ratio of 4 : 1 (excluding the abnormal points in the training set, only using the normal data for training).

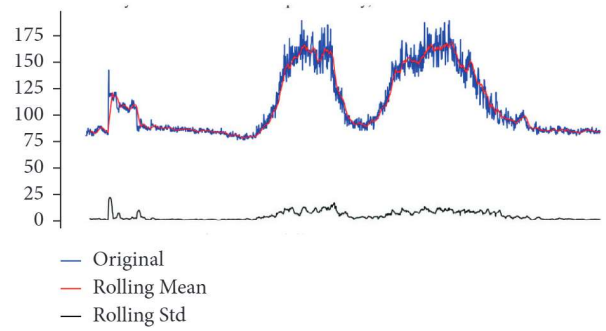

Figure 8: Company 2 data rolling mean and rolling STD.

The data in the two data sets are shown in Figures 5–8. In the financial data of company 1, we can intuitively see that the noise of the data is large and there are some abnormal points. We can artificially and directly observe the possible abnormal points. After simple data smoothing operation and calculating the mean and variance, we can directly see that there is a large variance in some suspected abnormal points. After the difference, the mean and variance are calculated again, and the effect is more obvious. Similarly, we can also observe a lot of noise in the financial data of company 2, but the suspected outliers are not as intuitive as the financial data of company 1.

5. Conclusions

This paper proposes a new direction for financial data anomaly detection. The multifeature fusion financial data anomaly detection algorithm based on CNN achieves 0.70 on the F-score, which is the same as the effect of the current intelligent financial anomaly detection framework. In addition to the solution, this paper also adopts the KPI curve clustering method to solve the problem and achieve more reliable results. In addition, the financial data anomaly detection method in this paper is integrated with the financial data trend prediction algorithm and multidimensional correlation analysis algorithm. From the anomaly detection methods and application status of financial data, we can learn that the anomaly detection of financial data does not transplant the general anomaly detection methods to this field. Many enterprises and researchers are now researching the appropriate anomaly detection algorithms based on application situations and financial data properties. To improve and strengthen the effect of anomaly detection, much research has steadily brought the latest theories and achievements of machine learning and deep learning into the field of financial data anomaly detection. Although the classification method is a common method to solve anomaly detection, it is unrealistic to expect to always have data sets with sufficient and diversified labeled anomalies. In addition, anomaly detection of financial data usually focuses on hundreds of parameters in a large system. There will be many models in the deep learning method. The ability to reduce the models and the number of models by using the universal model is also the key for us to introduce the latest deep learning technology into the anomaly detection of financial data.

Data Availability

The datasets used and analyzed during the current study are available from the author upon reasonable request.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] D. Zhang, Z. Lin, and Z. Gao, "A Novel fault detection with Minimizing the Noise-signal ratio using reinforcement learning," *Sensors*, vol. 18, no. 9, p. 3087, 2018.

[2] B. Morris, "Explainable anomaly and intrusion detection intelligence for Platform information technology using Dimensionality reduction and ensemble learning," in *Proceedings of the 2019 IEEE AUTOTESTCON*, IEEE, National Harbor, MD, USA, August 2019.

[3] M. Talo, U. B. Baloglu, Ö. Yıldırım, and U. Rajendra Acharya, "Application of deep transfer learning for automated brain abnormality classification using MR images," *Cognitive Systems Research*, vol. 54, pp. 176–188, 2019.

[4] S. Otoum, B. Kantarci, and H. T. Mouftah, "Empowering reinforcement learning on big sensed data for intrusion detection," in *Proceedings of the ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, IEEE, Shanghai, China, May 2019.

[5] L. Zhang and P. Deng, "Abnormal odor detection in Electronic Nose via self-expression inspired extreme learning machine," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 10, pp. 1922–1932, 2019.

[6] A. Borghesi, A. Bartolini, M. Lombardi, M. Milano, and L. Benini, "Anomaly detection using Autoencoders in high performance Computing systems," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 9428–9433, 2019.

[7] J. M. Calabuig, H. Falciani, and E. A. Sánchez-Pérez, "Dreaming machine learning: Lipschitz Extensions for reinforcement learning on financial markets," *Neurocomputing*, vol. 398, pp. 172–184, 2020.

[8] F. Soleymani and E. Paquet, "Financial portfolio optimization with online deep reinforcement learning and restricted stacked autoencoder-DeepBreath," *Expert Systems with Applications*, vol. 156, Article ID 113456, 2020.

[9] K. C. Roy and Q. Chen, "DeepRan: attention-based BiLSTM and CRF for ransomware early detection and classification," *Information Systems Frontiers*, vol. 23, no. 2, pp. 299–315, 2021.

[10] K. El-Awady, "Adaptive stress testing for Adversarial learning in A financial Environment," 2021, https://arxiv.org/abs/2107.03577.

[11] S. Kwon, B. H. Go, and J. H. Lee, "A text-based visual context modulation neural model for multimodal machine translation," *Pattern Recognition Letters*, vol. 136, no. 2, pp. 212–218, 2020.

[12] D. Song and D. Huang, "A Chinese-English Statistical Machine Translation method integrating syntactic phrases," *Small microcomputer system*, vol. 38, no. 10, pp. 2197–2201, 2017.

[13] X. Tong and J. Zhu, "Hierarchical phrase machine translation decoding method based the on tree to string model enhancement," *Journal of Computer Science*, vol. 39, no. 4, pp. 808–821, 2016.

[14] C. Xue, "A discourse parser language model based on an improved neural network in machine translation," in *Proceedings of the International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, pp. 605–608, IEEE, Xiamen, China, January 2018.

[15] L. Yuan, "A statistical model of syntactic analysis using semantic information," *Small microcomputer system*, vol. 40, no. 10, pp. 2125–2129, 2019.

[16] Y. Zhang, R. Alturki, H. J. Alyamani, M. A. Ikram, A. Rehman, and M. Haleem, "Multilabel CNN-based hybrid learning Metric for Pedestrian Reidentification," *Mobile Information Systems*, vol. 2021, Article ID 5512382, 2021.

[17] J. Zhao, "Research on Chinese - English machine translation technology based on statistics," *Electronic design engineering*, vol. 24, no. 21, pp. 69–71, 2016.