Hindawi
Security and Communication Networks
Volume 2023, Article ID 9873594, 1 page
https://doi.org/10.1155/2023/9873594

Retraction

Retracted: Integrated Energy Security Defense Monitoring Software Based on Cloud Computing

Security and Communication Networks

Received 25 July 2023; Accepted 25 July 2023; Published 26 July 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Shang, "Integrated Energy Security Defense Monitoring Software Based on Cloud Computing," *Security and Communication Networks*, vol. 2022, Article ID 2736904, 7 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 2736904, 7 pages
https://doi.org/10.1155/2022/2736904

Research Article

Integrated Energy Security Defense Monitoring Software Based on Cloud Computing

Yongqiang Shang

Department of Information Engineering Information Engineering, Xinyang Agriculture and Forestry University, Xinyang 464000, Hennan, China

Correspondence should be addressed to Yongqiang Shang; 2013072137@stu.zjhu.edu.cn

Received 30 May 2022; Revised 20 June 2022; Accepted 18 July 2022; Published 8 August 2022

Academic Editor: C. Venkatesan

In order to solve the problem of outlier detection of integrated energy security defense monitoring software, an automatic detection algorithm of virtual machine power anomaly in a cloud computing environment is proposed. The method is implemented through three main steps: data preprocessing, pattern recognition, and prediction of virtual machine power anomaly detection model. It is found through experiments that with the increase of node number, the convergent iterations of the model are less and RMSE is lower, but the increase of node number of the hidden layer will lead to a longer model running time. When the number of nodes reaches 100, the test results of the validation set are significantly improved, and the loss function of the validation set is minimal when the number of nodes is less than 30 iterations. Finally, the hidden layer of the model consists of 100 LSTM units, followed by a dense output layer with 1 neuron, and 0.2 loss, retrospection, and foresight equal to 1. Adam optimizer was used to train LSTM and stop it in advance after 50 iteration steps. Its parameters remained default, with a learning rate of 0.001 and attenuation of 0.9. It can be seen that this model can well predict the virtual machine power consumption data and effectively solve the problem of outlier detection of integrated energy security defense monitoring software.

1. Introduction

With the development and popularization of Internet technology and the continuous expansion of people's demand for computing resources, fast, efficient, and accurate processing of the massive data generated every day on the Internet has become the main direction of the next development of information network technology. At the same time, the demand-use relationship of all kinds of text resources and multimedia resources stored in the network has become more and more unbalanced, and a large number of network resources have not been effectively utilized. In addition, users have more diversified ways to access the Internet. Smartphones, tablets, PCS, and Internet of Things devices can be connected to the Internet and obtain the data they need from the Internet. Therefore, at present, computer science and computer industry urgently need to solve problems such as how to make the storage of data more efficient, how to make the visit of resources more convenient, and how to make computer resources more cheap. Because the development history of cloud computing technology is relatively short, it contains a large number of emerging technologies and advanced ideas and lacks the test of time and actual combat; cloud computing is a pay-for-use model, which provides available, convenient, and on-demand network access and enters a configurable computing resource sharing pool (resources include network, server storage, application software, and services). These resources can be provided quickly with little administrative effort or interaction with service providers. At the same time, due to the cloud computing virtualization technology and a large number of software definition technology, the system itself becomes very complex; subsequently, although there are no reports of malicious attacks against cloud computing platforms, this does not mean that cloud computing platforms are safe and reliable. Relevant attack technologies have been introduced but have not yet been applied in actual attacks. Therefore, the security problem of cloud computing platforms is still the weak board of the whole cloud computing technology. There are great security risks, which slow down the popularity of cloud computing. Among all the security problems faced by cloud computing, the threat from the network part is particularly prominent virtualization security issues. The scalability brought by virtualization is beneficial to strengthen the ability to provide multitenant cloud services at the infrastructure, platform, and software levels. However, virtualization technology also brings the following security problems: if the host is compromised, it is possible for the client server to be compromised; if the virtual network is compromised, the client is also compromised. Although there have been a lot of research and related results on cloud computing network security, at the same time, the network infrastructure of cloud computing platform has fully considered the related security risks and added many corresponding defense mechanisms in the development process. However, these methods and protection mechanisms can only protect a small part of the network infrastructure in the cloud platform, which is not universal and reusable and can provide limited security guarantee functions. In order to solve the shortcomings of the current research method mentioned above, this paper studied the key technologies of network security on the cloud computing platform in depth, proposed a new network defense method, and designed and implemented a cloud computing network security defense system based on this method, effectively resolving the current cloud computing network security threats.

2. Literature Review

In China, cloud computing has a wide range of applications, relatively mature functions, and relatively stable performance, including Alibaba's Ali Cloud platform and Qiniu Cloud storage platform. Among them, Aliyun under Alibaba Group is one of the leading figures in China's cloud computing technology, with high independent intellectual property rights and a wide range of cloud users in China. However, compared with Amazon, Google, and other cloud computing platforms with strong technical capital and early start, Ali Cloud still has its own safety shortcomings. On October 30, 2012, Ali Cloud computer room was disconnected due to power failure, and a large number of users could not access the services deployed on Ali Cloud. On May 27, 2015, due to a variety of reasons, the network services of Ali Cloud Hong Kong computer room were forced to stop, a large number of companies overseas services were forced to stop as well, resulting in huge economic losses [1].

To this end, many institutions and manufacturers in China also began to put forward a variety of new cloud defense methods, although relatively late compared with other countries, but the momentum of development is strong and the results are remarkable. Make sure that the system files of the cloud server are the latest version, and update the system patches in time. The server may have loopholes or errors in processing equipment. If it is not discovered and processed in time or repaired as soon as possible, there is a possibility of being attacked by hackers, close the common operation methods of operation and maintenance and delete unused services on the cloud server, and close unused ports. Set up a security group or firewall on the cloud server, and run the port mapper or port scanner on the firewall. Use the snapshot backup function on the cloud server to ensure that website data is not lost. Cloud computing in its development road will experience three obstacles, respectively, for the safety of personnel and standards, which is the most important security issues. Deng et al. in their paper analysis of cloud computing and information security not only introduced the relevant concepts, principles, system architecture, and main forms of cloud computing but also analyzed the challenges and opportunities brought by the development of cloud computing to the discipline of information security [2].

Pattern recognition based on virtual machine power consumption data and the analysis of the typical abnormal situation presents a cloud computing environment of the virtual machine power automatic detection algorithm, through the data preprocessing and pattern recognition and prediction of the virtual machine power. Three main steps of the anomaly detection model effectively solve the comprehensive energy security defense monitoring software outlier detection problem.

3. Research Method

3.1. Data Preprocessing. Temporal anomaly detection data is the initial step of power consumption of the original stream data preprocessing using dataset from the former to build the virtual machine power model, the model through the acquisition of virtual machine internal events to build a regression model to assess the performance of time-stamped virtual machine power consumption data, after transmission through the network transmission to the temporal database [3]. However, whether it is the performance event collector power estimation model failure or the transmission process due to the interruption of network fluctuation, there may be noisy data. Due to the space radiation interference introduced by the transmission line, this kind of interference phenomenon is mostly caused by the strong and high-frequency space radiation source near the transmission system, the front end of the system, or the central control room. One solution to this situation is to understand the surrounding environment when the system is established and try to avoid or stay away from the radiation source; another solution is to strengthen the shielding of the front-end and central equipment when the radiation source cannot be avoided. The pipeline of the transmission line is made of steel pipe and is well grounded. Due to the existence of noise data and the numerical characteristics of power sequence data, the data must be preprocessed to adapt to the anomaly detection algorithm used. If the original power data is directly input into the prediction model without preprocessing, the reliability, accuracy, and stability of the results will be affected. Therefore, we will discuss how to preprocess data in an appropriate way. The following sections describe the specific steps involved in data preprocessing [4].

3.1.1. Data Cleaning. As mentioned above, in this study, there are two types of noise data, including null or zero data and mutation data.

(1) Null or Zero Data Identification Method. Empty or zero data identification is the first step in the virtual machine power consumption data anomaly. In this type of data recognition method, the empty or zero data is very easy to recognize, but whether it is the marker for the abnormal data needs to be analyzed, according to the actual situation of the virtual machine. Under the close state of the virtual machine, virtual machine power consumption data is empty, in addition, the virtual machine power consumption data are not empty [5].

(2) Mutation Data Identification Method. Since virtual machine power consumption anomalies are bound to last for a period of time, rather than only exist in a single point, all point anomalies are regarded as abrupt data.

For noise data, it is commonly done to delete it directly or replace it with an interpolation algorithm after deletion. Noise data can be identified by the above two methods. The usual way to do this is to complete or replace the data, binning refers to putting the data to be processed into the bins according to certain rules and using a certain method for each bin; smoothing is performed on the data in each bin after binning; according to the mean value: average the data in the same box, and replace all the data in the box with the mean; by median: take the median of all the data in the box, and replace all the data in the latent box with the median. There are many ways to complete or replace data. Linear interpolation can be used to complement or replace the power consumption time series data due to its context-dependent characteristics, so as to reduce the adverse effects of poor data quality on abnormal detection results [6].

3.1.2. Character Building. After power consumption data is cleaned, it will be reorganized and new features will be generated. The selection of characteristic values of time series data largely determines the quality of subsequent analysis of time series data. Therefore, in order to better distinguish normal samples from abnormal samples, it is particularly important to construct an appropriate combination of characteristic values. These two processes include feature generation and data rearrangement, and the final result should be a set of distinguishing feature value combinations without information redundancy. The process of feature generation and data rearrangement will be described in the following two parts, respectively [7].

Feature generation: this step involves introducing more features into the anomaly detection process and reducing the time difference between continuous sliding windows by using overlapping sliding windows. Therefore, to accommodate this shorter gap between sliding windows, the framework introduces contextual features of months, weeks, hours, and minutes. The features generated by the method in Table 1 are also selected: maximum value of power data value in each window (max) minimum value (min), average (avg), variance of power data value in each window, difference between the first and last elements of the sliding window different, absolute sum of changes (absolute_sum_of_changes) of the sliding window sum of changes, and mean_change [8].

Table 1: Feature extraction method of time series data.

Feature extraction method	Formula
Max	$\max_{1\leq i\leq n}\{x_1,\ldots,x_n\}$
Min	$\min_{1\leq i\leq n}\{x_1,\ldots,x_n\}$
Avg	$\mu=\sum_{i=1}^{n}x_i/n$
Variance	$\sigma^2=\sum_{i=i}^{n}(x_i-\mu)^2/n$, where$\mu=\sum_{i=1}^{n}x_i/n$
Skewness	$\sum_{i=1}^{n}[(x_i-\mu)/\sigma]^3$
Kurtosis	$\sum_{i=1}^{n}[(x_i-\mu/\sigma)]^4$
Difference	$x_2-x_1,x_3-x_2,\ldots,x_n-x_{n-1}$
Integration	$\sum_{i=1}^{n}x_i$
Absolute_sum_of_changes	$E=\sum_{i=1}^{n-1}\lvert x_{i+1}-x_i\rvert$
Mean_change	$(1/n)\sum_{i=1}^{n-1}\lvert x_{i+1}-x_i\rvert$ $=(1/n)(x_n-x_1)$

Data rearrangement: it is rearrangement of power data by representing each input instance with sliding window data rather than a single power value. This involves defining a method to convert an array of values into a matrix of datasets and to convert unlabeled sequential data into labeled datasets for LSTM network learning. The algorithm is implemented as follows: given the current time (t), to predict the next value (t−1) in the sequence, the current time (t) and the first n times ($t-1,t-2,\ldots,t-n$) can be used.

3.1.3. Normalization. In the cloud computing environment, VM power consumption varies greatly under different loads or time periods. Therefore, a larger value may have a greater impact than a smaller value [9]. In order to give the features the same weight, the dataset is normalized by scaling the features back to [0,1] using the following formula:

$$x_{\text{normalization}}=\frac{x-x_{\min}}{x_{\max}-x_{\min}}. \tag{1}$$

There is $x_{\text{normalization}}$ data from the normalization process $x_{\text{normalization}}\in[0.1]$. x represents raw data; $x_{\max}$ indicates the maximum value of the original data. $x_{\min}$ represents the minimum value of the original data. Formula (2) is used to reverse normalize the $x_{\text{normalization}}$ of the predicted value in the [0, 1] interval to obtain the final predicted power consumption value x_{t}. The formula is as follows:

$$x_t=x_{\text{normalization}}\times\left(x_{\max}-x_{\min}\right)+x_{\min}. \tag{2}$$

3.2. Virtual Machine Power Anomaly Detection Model Based on Pattern Recognition and Prediction. In order to improve the accuracy of abnormal data identification, a new algorithm is proposed to detect abnormal power by combining data in the same power mode with a set of anomaly detection methods [10]. DBSCAN clustering analysis algorithm is used to dynamically identify different types of VM power consumption modes. LSTM, an unsupervised machine learning

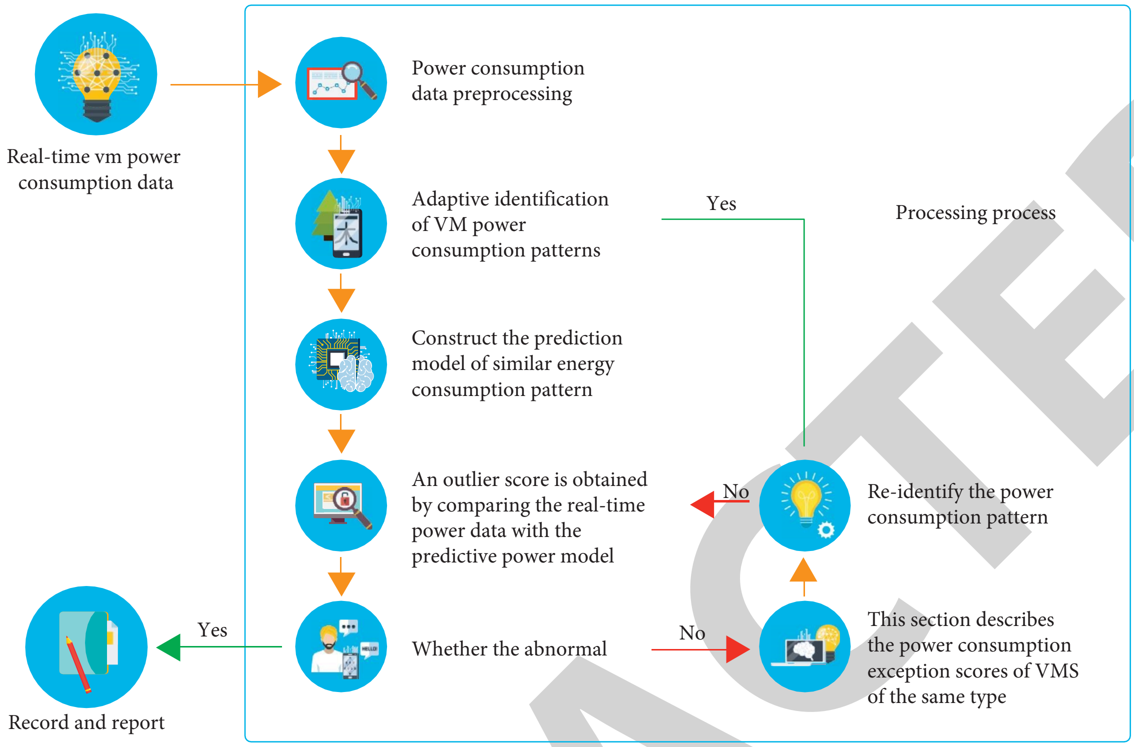
Real-time vm power consumption data
Power consumption data preprocessing
Adaptive identification of VM power consumption patterns
Construct the prediction model of similar energy consumption pattern
An outlier score is obtained by comparing the real-time power data with the predictive power model
Whether the abnormal
Yes
Record and report
No
This section describes the power consumption exception scores of VMS of the same type
Re-identify the power consumption pattern
No
Yes
Processing process

Figure 1: VM power exception detection model.

method without any prior knowledge, is used to learn the implied energy rule in the normal power consumption data to predict the normal power consumption value. The power anomaly detection is realized by outlier analysis with the actual value. The same power consumption mode of the virtual machine is defined as with similar characteristics (configuration operation service Tenant type traffic) a collection of all virtual machines, thus may respond to and consume energy in a similar way to external conditions. Congeners can be predefined based on previous virtual machine power consumption, or they can be identified by analyzing historical power consumption data [11]. The process of this method is shown in Figure 1.

As can be seen from Figure 1, this model is a typical abnormal detection process of time series data. The input is the characteristic attribute of real-time equipment power consumption data, and the output is the warning result. The processing process is divided into the following three major processes:

(1) Power consumption data preprocessing: the identification method including null or zero data and abrupt data is based on the analysis of typical power abnormal scenarios, the judgment rules of power noise data are extracted by combining with manual experience, and the power noise data are identified by qualitative method, and these noise data are deleted or replaced by data cleaning [12].

(2) Identify abnormal power data: the recognition method is mainly based on clustering and prediction hybrid anomaly detection method of time series data, including power pattern recognition⟶power prediction outlier detection in the same mode⟶ outlier detection. The technical means are clustering analysis based on machine learning time series, data prediction, and outlier analysis, respectively. In the first step, the algorithm through the virtual machine is only considered the energy consumption and consumption in the past to identify periodically with the same power consumption model of the virtual machine. The second step, for each type of abnormal power consumption data, without any prior knowledge of unsupervised method LSTM study implied in normal power consumption data can rule, predict the normal power consumption value. In the third step, the abnormal score of virtual machines is adjusted by analyzing the actual power data and predicted power value of similar virtual machines, and outlier point analysis is performed to dynamically identify the suspected abnormal power data outside the threshold range, and record the abnormal state when it is detected and send an alarm [13].

(3) Dynamic model update: to adapt to the constant change of the VM power consumption mode, a cumulative anomaly score is maintained for each power consumption mode. If the value exceeds a threshold, it indicates that the power consumption mode cannot adapt to the current data. Reidentify the power consumption mode and regenerate the power consumption prediction model in this mode [14].

4. Interpretation of Result

4.1. Analysis of Normal Power Consumption Prediction Effect. Based on the load generator, the power consumption data of virtual machines that work properly in the cloud computing environment are obtained by periodically adjusting the concurrent number. The power consumption data of virtual machines are shown in Figure 2 [15]. The power consumption dataset takes one day as a cycle, setting low power consumption in the evening and high power consumption in the day, which is similar to the real user traffic distribution, according to 3.2. The data preprocessing described in section processes the power data, removes the noise data, converts the data into decimals between (0,1) using normalization, and then transforms the dataset into the format required by the algorithm through feature generation and data rearrangement [16]. The dataset contains readings corresponding to a week and is divided into training data and test data.

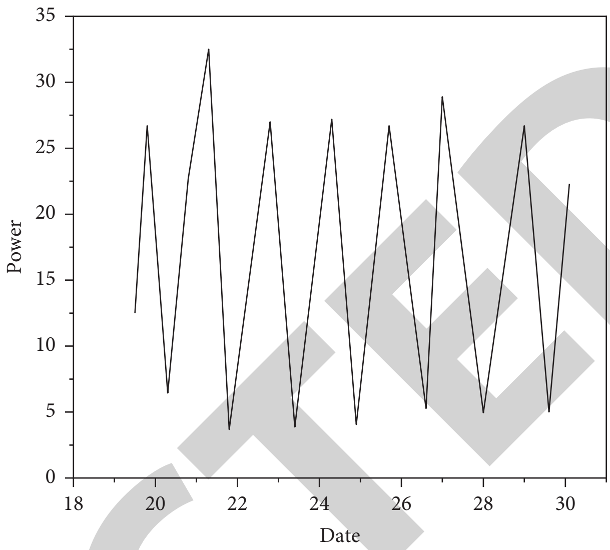

Figure 2: Generated VM power consumption dataset.

Next, based on the LSTM model, the training data is used to learn the power behavior of normal virtual machines, which is used to predict the next power trend. Several software packages provide the implementation of LSTM, and Keras provides advanced API for neural network, which can realize fast experiments. Keras is easy to use, but implementing custom changes is not easy [17]. Another option is to use TensorFlow directly. It provides a more flexible, lower-level API than Keras.

As for the selection of the optimal LSTM network structure, there are different optimal choices for different time series data. It is necessary to judge through experiments because the input of the model is the power consumption of the virtual machine, the number of input nodes is 1, and the output of the model is the predicted future power consumption of virtual the machine. Therefore, the number of output nodes is also 1. LSTM units in the hidden layer are fully connected through circular connection, as shown in Figure 3. Since curve fitting is a regression problem, MSE is used in the loss function [18].

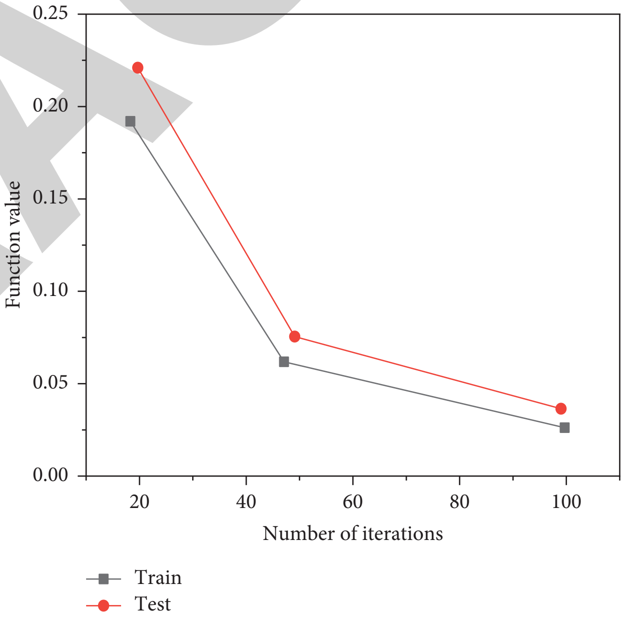

Figure 3: Loss function decline of LSTM networks with different nodes.

In addition, the number of nodes in the LSTM hidden layer needs to be determined through experiments. Although there are infinite combinations of hidden layer and node, considering the limited training samples, it is impossible to export too many parameters, so it is impossible to use a very large network. Stepwise adjustment method is adopted to increase the number of nodes from 1 backward until the maximum number of nodes is determined. Experiments are conducted to compare several groups of LSTM networks with different number of nodes, as shown in Figure 4 and Table 2. It can be seen that with the increase of node number, the number of convergent iterations of the model decreases, while RMSE is lower, but increasing the number of hidden layer nodes will lead to a longer model running time [19]. When the number of nodes reaches 100, the test results of the verification set are significantly improved, and the loss function of the verification set is minimal in less than 30 iterations, and the evaluation index RMSE of the final network prediction results can meet the needs. Finally, the hidden layer of the model is composed of 100 LSTM units, followed by a dense output layer with 1 neuron and 0.2 loss. Retrospection and foresight are equal to 1. Adam optimizer is used to train LSTM and stop in advance after 50 iterative steps with a learning rate of 0.001 and attenuation of 0.9. The prediction of the test set is shown in Figure 3, which shows that the model can well predict the virtual machine power consumption data.

By comparing LSTM with the other four time series data prediction models, as shown in Table 2, it can be seen that the prediction effect of the Holt–Winters model is second only to the LSTM model, while the fitting effect of ARMA

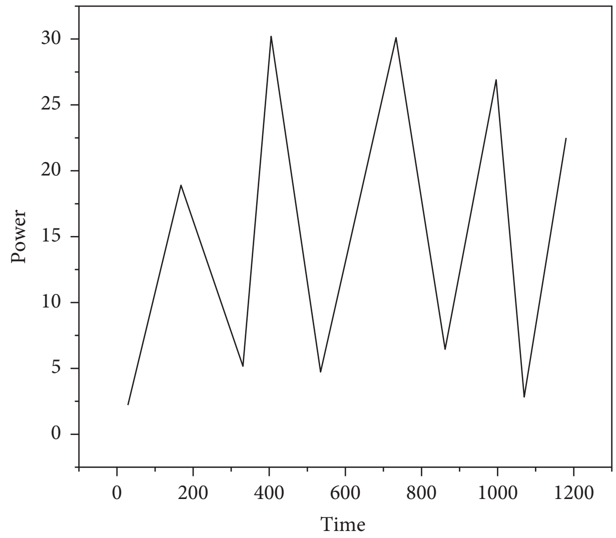

Figure 4: Prediction of VM power consumption based on LSTM.

Table 2: Comparison of virtual machine power time series data prediction models.

Time series data prediction model	Evaluation index RMSE
LSTM	1.807
ARMA	4.875
ARIMA	3.758
Holt–Winters	2.054

and ARIMA, the two traditional time series models, is poor, and LSTM is obvious. The traceability of historical values does have a good ability to fit [20].

4.2. The Effect of Injection Exception Detection. Based on the exception injector, the CPU load is suddenly increased for a period of time by triggering the modification of the RBE concurrency to double to occupy additional CPU resources, artificially causing a sudden change in virtual machine power consumption [21]. During the period from December 1 to December 3, the abnormal power injector introduced a power anomaly. The peak power consumption of the VM reached about 34W, 7W higher than the previous maximum power consumption. During this period, the minimum power consumption was also higher than the previous maximum power consumption. The prediction of the VM power consumption dataset with abnormal power consumption and the corresponding prediction error is displayed. The log-PD value of the prediction error and the threshold time on the X-axis and the corresponding measurement value on the Y-axis are displayed [22, 23]. If the log-PD threshold is set to −3 and a section of virtual machine power consumption is marked in red, real exceptions are identified. However, at other times, there are also places where the log-PD threshold is less than −3, and these are false-positive problems [24, 25].

5. Conclusion

Based on pattern recognition of virtual machine power consumption data and analysis of typical abnormal scenarios, an automatic detection algorithm for virtual machine power anomaly in cloud computing environment is proposed, which is implemented through three main steps of data preprocessing and pattern recognition and prediction of virtual machine power anomaly detection model: the power consumption patterns of different types of virtual machines are dynamically identified by clustering analysis algorithm. For each type of power consumption data, the unsupervised machine learning method LSTM without any prior knowledge is used to learn the power consumption law implied in the normal power consumption data to predict the normal power consumption value. The power anomaly detection is realized by outlier analysis of the difference between the predicted and actual values. In order to verify the effectiveness of the algorithm, TPC-W is used to simulate the general load and complete the exception injection. Based on the experimental platform, it is proved that the algorithm proposed in this design has higher anomaly detection rate and lower false positive rate than the classical anomaly detection algorithm.

With the further development of cloud computing, in-depth excavation of large power consumption data will become more important and urgent. Due to the lack of time and energy, there are still many shortcomings in this research. In view of the problems found in the process of writing and the difficulties and challenges faced by this field, we plan to do in-depth research from the following aspects:

(1) Power modeling for services or containers within virtual machines: as enterprises grow, the application architectures they use become more complex, from single applications to multiple applications combined to form services, to microservice architectures, to containerization, which is now popular. In order to support more fine-grained power-aware policies, higher level management techniques are required based on the virtual machine power model in cloud computing environment. In order to eliminate the energy waste caused by tasks, applications, processes, and threads, a service-oriented power model is further constructed to enable real-time monitoring of service power changes in cloud computing environment.

(2) Power abnormal cause diagnosis: this study can find power abnormal conditions, but how to build the relationship between typical power abnormal scenario database and energy consumption parameters and intelligent diagnosis of power abnormal causes will be the next research direction of this paper.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] X. Feng, F. Yan, X. Y. Liu, and Q. Jiang, "Development of iot cloud platform based intelligent raising system for rice seedlings," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1695–1707, 2021.

[2] T. Deng, X. Li, J. Xiong, and Y. Wu, "Poisidd: privacy-preserving outsourced image sharing scheme with illegal distributor detection in cloud computing," *Multimedia Tools and Applications*, vol. 81, no. 3, pp. 3693–3714, 2022.

[3] P. Upadhyay, M. K. Pandey, and N. Kohli, "Periodic pattern mining from spatio-temporal database using novel global pollination artificial fish swarm optimizer-based clustering and modified fp tree," *Soft Computing*, vol. 25, no. 6, pp. 4327–4344, 2021.

[4] M. Edwards, F. Chevillotte, F. X. Becot, L. Jaouen, and N. Totaro, "Development of a prediction model for indoor rolling noise," *Journal of Sound and Vibration*, vol. 507, no. 2, Article ID 116199, 2021.

[5] R. Kumar and A. Sharma, "Risk-energy aware service level agreement assessment for computing quickest path in computer networks," *International Journal of Reliability and Safety*, vol. 13, no. 1/2, p. 96, 2019.

[6] A. R. Kandula, S. Narayan, and R. Sathya, "Performing univariate analysis on cancer gene mutation data using sgd optimized logistic regression," *International Journal of Engineering Trends and Technology*, vol. 69, no. 2, pp. 59–67, 2021.

[7] Y. Xu, L. He, Y. Liang, J. Si, and Y. Bao, "Enterprise power consumption data and gdp forecasting based on ensemble algorithms," *E3S Web of Conferences*, vol. 233, Article ID 01030, 2021.

[8] M. Bradha, N. Balakrishnan, S. Suvi et al., "Experimental, computational analysis of butein and lanceoletin for natural dye-sensitized solar cells and stabilizing efficiency by iot. environment," *Development and Sustainability*, vol. 24, no. 7, 2021.

[9] L. Li, Y. Diao, and X. Liu, "Ce-Mn mixed oxides supported on glass-fiber for low-temperature selective catalytic reduction of NO with NH3," *Journal of Rare Earths*, vol. 32, no. 5, pp. 409–415, 2014.

[10] U. Gopalan, "Sensitive data identification and protection in a structured and unstructured data in cloud based storage," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 2, pp. 1157–1166, 2021.

[11] R. Yan, J. Liu, J. Wu, C. Xu, and Y. Hu, "The weak frequency anomaly detection method of atomic clocks based on kalman filter and extrapolation-accumulation," *Measurement and Control*, vol. 54, no. 5-6, pp. 565–575, 2021.

[12] J. J. Cai, J. Yang, S. Zheng et al., "Preliminary analysis on the noise characteristics of MWISP data," *Research in Astronomy and Astrophysics*, vol. 21, no. 12, p. 304, 2021.

[13] R. Huang, "Framework for a smart adult education environment," *World Transactions on Engineering and Technology Education*, vol. 13, no. 4, pp. 637–641, 2015.

[14] J. Mankart, A. Michaelides, and S. Pagratis, "Bank capital buffers in a dynamic model," *Financial Management*, vol. 49, no. 2, pp. 473–502, 2020.

[15] M. Zhang, Y. Zhao, and X. Song, "Dynamics of bilateral control system with state feedback for price adjustment strategy," *International Journal of Biomathematics*, vol. 14, no. 5, Article ID 2150031, 2021.

[16] J. Singer, "The abraham accords: normalization agreements signed by Israel with the U.A.E., Bahrain, Sudan, and Morocco," *International Legal Materials*, vol. 60, no. 3, pp. 448–463, 2021.

[17] P. Ajay, B. Nagaraj, R. A. Kumar, R. Huang, and P. Ananthi, "Unsupervised hyperspectral microscopic image segmentation using deep embedded clustering algorithm," *Scanning*, vol. 2022, Article ID 1200860, 9 pages, 2022.

[18] Y. Peng, "Super-resolution reconstruction using multiconnection deep residual network combined an improved loss function for single-frame image," *Multimedia Tools and Applications*, vol. 79, no. 13-14, pp. 9351–9362, 2020.

[19] O. Palii and M. Schlottbom, "On a convergent DSA preconditioned source iteration for a DGFEM method for radiative transfer," *Computers & Mathematics with Applications*, vol. 79, no. 12, pp. 3366–3377, 2020.

[20] S. Emmanuel, P. Jansz, D. McGiffin et al., "Anatomical human fitting of the bivacor total artificial heart," *The Journal of Heart and Lung Transplantation*, vol. 40, no. 4, p. S401, 2021.

[21] H. Eishi, K. Yamaguchi, Y. Hiramatsu, and K. Akita, "Intramural distribution of the blood vessels in the stomach demonstrated by contrast medium injection: a cadaver study," *Surgical and Radiologic Anatomy: SRA*, vol. 43, pp. 1–8, 2020.

[22] H. S. Choi, "Different degradation mechanism by conduction region in astegesin threshold switching device," *Electronics Letters*, vol. 56, no. 22, pp. 1202–1204, 2020.

[23] I. T. Gabdrakhmanov, M. V. Gorshkov, and I. A. Tarasova, "Proteomics of cellular response to stress: taking control of false positive results," *Biochemistry (Moscow)*, vol. 86, no. 3, pp. 338–349, 2021.

[24] Y. Zhang, B. Guo, H. Zhang, and J. Sun, "Abnormal heart rate detection based on double slope qrs beat location," *Journal of Physics: Conference Series*, vol. 1966, no. 1, Article ID 12032, 1966.

[25] G. Veselov, A. Tselykh, A. Sharma, and R. Huang, "Special issue on applications of artificial intelligence in evolution of smart cities and societies," *Informatica*, vol. 45, no. 5, 2021.