Analysis of Internal Threat Detection Methods of Power Grid under the Characteristic Cloud Computing Model

Jing Li¹*, Jie Huang¹,Fen Liu²

¹State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430077
²Information & Communication Branch of Hubei EPC, Hubei Wuhan, China, 430077

*Corresponding author e-mail: lijing8@sghec.org

Abstract. Advances in science and technology are driving the development of society, and with the development of society, our power grid coverage has become more extensive, which has solved the power supply problem in most parts of the country. As an important infrastructure of the country, the safety and nursing work of the power grid industrial control system is very important. However, the increase of coverage makes the maintenance and management of the power grid itself more difficult, and the internal threat of the power grid cannot be ignored. To get a clearer understanding of the methods and patterns we use in terms of threats within the grid, this article will analyze the objects we are studying using cloud computing simulation methods, and then analyze the results of the data. The experimental results show that the detection method of internal threat of power grid is still in the preliminary stage of development in our country.

Keywords: cloud computing, models, internal threats to the grid, detection methods

1. Introduction.
Due to the popularity of the power grid and the development in recent years, the material and price of the power grid itself has been controlled in a better range, but this only solves the surface threat of the power grid. As the occurrence of internal threats in power grid is more uncontrollable and discoverable, our research on internal threat detection is still in its infancy.

The power grid internal threat detection needs to extract the rights and objectives of the operator. According to the above characteristics, the threat degree of operation behavior is predicted and compared with the threat degree standard to complete the internal threat test of power grid [1]. This paper will analyze the research of power grid internal threat detection method through characteristic cloud computing model method [2]. With the advancement of "industrialization and industrialization integration" process, the industrial control network has changed from the original control mode, and the network control has extended to the management network [3]. The industrial control system is
closely connected with the Internet, and the industrial control network in the world is becoming more and more intelligent and networked [4]. At the same time, it also brings more and more security threats to the industrial control system, so does the industrial control system [5]. Many of the "2010" attacks on the industrial control system of Iran's state-owned nuclear control system involved in the "2010" nuclear power plant control system. Power, therefore, the state attaches great importance to the security of industrial control system, the traditional network security has many differences [6]. This is equivalent to a relatively new field of traffic anomaly detection technology in network information security has been widely used in full protection [7]. It makes the power grid more secure and more efficient. [8] It can improve power grid transmission capacity and material saving [9].

Power network internal threat detection is the core issue of power security research. It is inevitable to use traditional algorithm to detect the internal threat of power grid, so as to avoid the influence of subjective factors on the feature extraction of the main body, which leads to the high rate of missing detection. Therefore, the characteristic cloud computing model based on cloud computing can be used to solve the problem more effectively.

2. Model building and algorithm input
First of all, based on the cloud computing load historical data matching the corresponding timing data, should be after the data cleaning and data normalization processing, the enhanced data set as the input data of the composite model; Match the timing data again, and normalize the data, as the input data of LSTM network, determine the LSTM network structure and weight, threshold parameters, train and forecast, get BPNN residual prediction value, and finally, add the total BPNN prediction results and LSTM residual prediction results, get the final cloud computing resource load prediction value.

2.1. Data entry and its processing
With \( x_i \) \((i \in (1, n + k))\) represents the cloud computing resource load history data of the ith time node \( x_1, x_2, \ldots, x_n \) build the historical data from the first time node to the nth time node, and use \( x_2, x_3, \ldots, x_n + 1 \) constructs the historical data from the second time node to the n + 1 time node, and so on, constructs the cloud computing resource load historical data matrix:

\[
X_{\text{Original}} = \begin{pmatrix}
  x_1 & \cdots & x_k \\
  \vdots & \ddots & \vdots \\
  x_n & \cdots & x_{n+k-1}
\end{pmatrix}
\]  

Based on the timing characteristics of the requirements for intra-grid threat detection methods under the cloud computing model, date attributes (in: d, \( i \in (1, n-k) \)) and time attributes (in h, \( i \in (1, n-k) \)) are introduced to match the historical data matrix of the cloud computing resource load, build dataset X and data set Y to be predicted. 

\[
D_1 T_1 
\]

\[
X = ( x_1, \ldots, x_k, D_1, T_1, x_{k+1} ) \\
Y = ( \vdots, \vdots, \vdots, \vdots ) \\
X_{n}, \ldots, x_{n+k-1}, D_n, T_n, x_{n+k}
\]

After data cleaning and normalization, the enhanced data set \((X, Y)\) is obtained as input data for the combined model.

2.2. Neural network prediction
Split input data \((X, Y)\) for the training data set \(X_{\text{train}}, Y_{\text{train}}\) and test data set \((X_{\text{test}}, Y_{\text{test}})\), build the first layer of the input layer: the cloud computing resource load prediction implicit layer of the base BPNN-LSTM composite model, the second layer of implicit layer, the four-tier network structure of the output layer, using random function generation to initialize the weights and threshold parameters. Select the sigmoid function as the activation function of the BPNN neural network, and the function expression is:

\[
\text{sigmoid}(x) = \frac{1}{1 + e^{-x}}
\]
\[ f(x) = \frac{1}{1 + e^{-x}} \] (3)

Make a positive prediction of the training dataset and set the ratio of the forecast results to the actual load data (the loss function is the square root function of the square square of the square square error of the square \( Y_{\text{predict}} \times \text{Ytest}\text{square} \):

\[ \text{MSE} = \frac{1}{m} \sum_{i=1}^{m} (Y_{\text{train}} - Y_{\text{predict}})^2 \] (4)

According to the gradient drop rule to adjust the weight, the reverse error signal of the output layer is transmitted by the second layer of implicit layer and the first layer of implicit layer, and finally to the output layer. Through the reverse propagation of error, the connection weight between the nodes is corrected to achieve network optimization. After the network training is completed, the residual \( E_{X_{\text{test}}} \) between BPNN prediction result \( Y_{BP} \) and actual load data \( Y_{\text{test}} \) is calculated and transmitted to the LSTM network.

3. Experimental method

3.1. Features modeling options for cloud computing

The big data feature selection algorithm mainly based on data aggregation according to statistical principle, divides the data information into different subsets and extracts its number according to the characteristics of the data. The method adopts offline feature selection, that is, assuming that the sample set and its corresponding data characteristics have been obtained in advance, the method can effectively reduce the time complexity and cluster accuracy of the entropy algorithm to handle the processing of large amounts of big data effectively.

3.2. Data source

We used algorithms to model, in the domestic 20 power grid institutions to conduct a survey, data statistics integration to analyze this experiment. To provide data for this experiment, we selected twenty institutions to expand the subjects to increase the universality and usefulness of the data. As a result of more than 3,000 lines, 121 power grid points for statistics, the subject of this experiment is very representative, wide coverage, the results are very real and feasible, part of the power grid due to external reasons and method errors caused by the experimental error through the reliability test was finally eliminated [10].

4. Experimental results and data analysis

4.1. Simulation results

By comparing traditional methods and text algorithms to analyze the internal threat detection methods of the power grid under the characteristic cloud computing model, the following data are analyzed:

| Internal threat detection data | Traditional algorithms | The text algorithm |
|-------------------------------|------------------------|-------------------|
| Detection time                | 25s                    | 30s               |
| Number of detections          | 20 times               | 20 times          |
| The number of internal threats| 48                     | 70                |
| The number of internal threats detected | 45           | 67                |
| Missed detection rate         | 6.25%                  | 4.28%             |
In Table 1, the leakage detection rate of the algorithm used to detect the internal threat of the power grid is lower than that of the traditional algorithm, which shows that the algorithm is influenced by subjective factors in feature extraction, and the detection of the internal threat of the power grid has great advantages. After recording the experimental data, you can get Figure 1.

4.2. Analog computational detection and stability analysis

Table 2. Results of the effect of different information objects on the reliability of the system

| The object of the information attack | $T_{SAIDI}$ | $E_{EENS}$ |
|------------------------------------|-------------|------------|
| The main power distribution station | 0.23       | 0.85       |
| 1 IED                             | 2.34        | 8.69       |
| 2 IEDs                            | 1.11        | 4.14       |

It can be seen from Table 2 that the information change object is reliable to the system the results show that the impact sequence of 1IED, 2IED and distribution main station with more action points and describe the information layer selection success rate of the way to implement information attack fluctuations, will cause greater economic losses to the system.

In order to study the normal operation and failure of the system in the event of a particular IED attack based on the normal operation and failure of the simulation model operation, the information attack scenario for 1 IED and 2 LEDs is then classified as shown in Table A3 of Appendix A, and the results are shown in Figure 2.
Figure 2. simulates the operation deviation of the model

Finally, the experimental results are derived from the above simulation operations and tests.

4.3. Computing tools for cloud computing

The amount of data in a cloud computing environment is huge and you may encounter security features that extract network intrusions. This is a journey based on certain rules and means of effective data processing optimization methods to extract a high degree of recognition of the characteristic set, effectively reduce the data dimensionality, improve the accuracy of network intrusion detection. Depending on whether the measure of feature extraction can be divided into three parts, single variable feature extraction and multivariable feature extraction. Single-variable special feature extraction method, linear judgment analysis (LDA), main component. Analysis method (PCA), packaging model, embedded model and so on are a widely used single variable feature extraction method. With regard to the multi-feature extraction method, according to the definition of information gain measurement index, Pearson coefficient achieves the maximum reduction of information gain and achieves the best feature extraction, and the effectiveness of this scheme is obvious by using malcoltt, which combines various measurement standards to achieve the optimal extraction of feature sets. Although it overcomes the unique defects of multivariable feature extraction single-variable feature extraction index, it is necessary to achieve optimal feature extraction in stages, which in short increases the difficulty of calculation.

4.4. Based on the original cloud computing security and resource optimization

Because of open network connectivity and full face-to-face sharing of all resources of cloud computing applications, integrated information services, centralized targets for cyberspace attacks, diverse means, rapid change, strong capabilities it has greater destructive and broader scope of impact, so as to build a reasonable and complete cloud security throughout the system, we can break through and solve a variety of key security technologies it has an impact on the cloud environment complex security risks to meet the needs of cloud services cloud ecosystem by suppliers, operators, security providers and users composed of unified security services needs. Cloud computing environment consists of hardware facilities, virtual resources and virtual computing resources, software platform and application software are the main types of services It includes software as a service and platform as a service (PAAS), infrastructure as a service infrastructure as a service (IAAs) has three service
models. Without the same service model, different features of cloud service providers and cloud tenants/customers accessing resources result in different security requirements. Cloud security computing environment security services need to be supported and developed by a range of basic security services based on a unified full-service policy, regulations, and standards, according to the latest requirements of the National Information Security Technology Network Security Protection Level Design Technology.

There are different task flow requirements in cloud computing, and the types, quantities, and time required for services vary, but the same or similar task flows require resources to seek basic similarity. Whether we can find out the resource requirements of the task flow execution process, we can realize the rational use of resources in cloud computing. In addition, in cloud computing, service resources are virtualized as pools of resources, and multiple tasks are performed during which resource fluctuations resonance occur. Based on these aspects, this paper analyzes and studies the task flow. The main work of this article is as follows:

1. Modeling and analyzing the task flow in cloud computing uses three modeling methods to describe the resource occupancy characteristics of the task flow and perform process characteristic analysis.
2. Analysis of multiple task flows that use or release the same resource at the same time, continuous fluctuation resonance will lead to a shortage of resources from time to time, however, excess is not conducive to the use of resources.
3. The solution to the problem of volatility of multistate flow resources in cloud computing is to use the application of arbitration mechanisms to avoid this phenomenon, for example, by entering a cooperative task process to use resources collaboratively.

5. Conclusions
In short, through the above-mentioned experimental results, it is found that the existing internal threat detection method of the power grid is still inefficient, the detection surface is small, not enough attention and so on. In China's distribution network, due to the limitation of distribution lines and transmission lines, its lightning protection capacity is still limited. In the investigation of urban power distribution lines, it was found that the power distribution lines were not set up irregularly, such as some insulators or even bowls and other mouths facing up, cross-arm is not standard. The insulators of the distribution line are not tested before installation, are not maintained regularly during operation, some insulators accumulate mud during installation and many years of operation, resulting in many weak links in the distribution network insulation. Distribution network often malfunction and explosion, seriously affecting the safe and stable operation of the distribution network. In addition, there are many sections and buildings in the distribution line, which has become a great threat to the safe operation and personal safety of the distribution network. Therefore, we have carried out statistical simulation analysis of the research objects by the method mentioned in this paper, and get the above conclusions.

References
[1] Al-Dhuraibi Y, Paraíso F, Djarallah N, et al. Elasticity in Cloud Computing: State of Art and Research Challenges. IEEE Transactions on Services Computing, 2018, PP (99): 1-1.
[2] Abdel-Basset M, Mohamed M, Chang V. NMCDA: A framework for evaluating cloud computing services. FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE, 2018, 86 (SEP.):12-29.
[3] Du J, Zhao L, Feng J, et al. Computation Offloading and Resource Allocation in Mixed Fog/Cloud Computing Systems with Min-Max Fairness Guarantee. IEEE Transactions on Communications, 2018, 66 (4): 1594-1608.
[4] Wei W, Fan X, Song H, et al. Imperfect Information Dynamic Stackelberg Game Based Resource Allocation Using Hidden Markov for Cloud Computing. IEEE Transactions on Services Computing, 2018, 11 (99): 78-89.
[5] Hueckel T, Ciantia M, Mielniczuk B, et al. Modeling Physico-Chemical Mechanical Properties to Assess Resilience of Geomaterials. Journal of Non-Crystalline Solids, 2018, 27 (2): 273-283.

[6] Lee L, Petter S, Fayard D, et al. On the use of partial least squares path modeling in accounting research. International Journal of Accounting Information Systems, 2018, 12 (4): 305-328.

[7] Na W, Liu W, Zhu L, et al. Advanced Extrapolation for Neural-Based Microwave Modeling and Design. IEEE Transactions on Microwave Theory and 2018, PP (10): 1-22.

[8] Chattopadhyay A, Ukil A, Jap D, et al. Towards Threat of Executive Attacks on Substation Security: Case Study on Detection Fault and Isolation. IEEE Transactions on Industrial Informatics, 2018, 14 (6): 2442-2451.

[9] Lu J, Guo J, Jian Z, et al. Optimal Allocation of Fire Forting Equipment for a Power Grid Under Widespread Fire Disasters. IEEE Access, 2018, 6:6382-6389.

[10] Sun C C, Hahn A, Liu C C. Cyber-Physical System Security of a Power Grid: State-of-the-Art. International Journal of Electric Power and Energy Systems, 2018, 99 (JUL.):45-56.