ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

Security And Privacy Issues From A Strategic And Long-Term Perspective Of Energy Big Data In Cloud Environment

Aniket U. Vikhe[1]*
[1]*Dept. of ECE, Om Parkash Jogender Singh University, Churu (Raj.) and Assistant Professor, Dept. of E & TC, Dr.VithalraoVikhe Patil College of Engineering, Ahmednagar (Maharashtra)
E-Mai:-vikheaniket@gmail.com

Dr. Suman Rani[2]
[2]Associate Professor, Dept.of ECE, Om Parkash Jogender Singh University, Churu (Raj.)
E-Mai:-smn.bishnoi@gmail.com

***Corresponding Author: -** Aniket U. Vikhe
*Dept. of ECE, Om Parkash Jogender Singh University, Churu (Raj.) and Assistant Professor, Dept. of E & TC, Dr.VithalraoVikhe Patil College of Engineering, Ahmednagar (Maharashtra)
E-Mai:-vikheaniket@gmail.com

Abstract:

Considering the importance of energy in our lives and its impact on other critical infrastructure, this document begins with the full lifecycle of big data and breaks down risk factors on the security and privacy of big data into 5 stages: data collection, data transmission, storage, data use and data destruction. Integrated into the consideration of the cloud environment, this document analyzes the risk factors of each stage in detail and establishes a system of data energy security and confidentiality risk assessment metrics. According to different degrees of risk impact, the AHP method is used to give weights to the indices, a genetic algorithm is used to optimize the initial weights and thresholds of the BP neural network, then optimized weights and thresholds are assigned to the BP Neural Network and the evaluation samples in the database are used to train it. The trained model is then used to evaluate a case to verify the applicability of the model.

Keywords: Risk Assessment, Cloud Environment, Energy, Big Data, Cloud Model etc.

1. INTRODUCTION

In the era of big data, the application of big data technology in the energy sector is a trend that promotes industrial development and innovation. The extensive application of big data technology in the energy sector and the extensive integration of energy production and consumption and the related technological revolution with the concept of big data will accelerate the development of the energy industry [1].

With the implementation of global energy big data strategy, the rapid development of "Internet Plus" smart energy, and the comprehensive construction of intelligent energy layouts, the energy industry is more widely distributed, more data collection points, more data types. Complex business relationships, and a wide range of data usage and users [2]. So while it brings convenience, it also poses a risk to big data management in the energy sector.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

Due to the critical infrastructure of each country, energy is inevitably a priority target during cyber warfare. Increasingly frequent energy security and privacy incidents, such as the "Ukraine power outage" and the "Stuxnet virus" attack on Iran's nuclear facilities, have made big data available and connectable carriers [3]. Using the big data value information obtained by the attack, the power distribution of the target site is analyzed, and the key data such as monitoring, early warning information and operation instructions from the key node are falsified, resulting in a power system failure or major security accident.
Therefore, management research based on big data in the energy field is highly evaluated by scientists all over the world. Given the vast amount of data and management details in the energy industry, scientists are now in a variety of technical and non-technical ways, including establishing large data layers for storing and processing renewable energy data. We manage data and design architecture through means [4] and establish an energy big data processing system that supports distributed memory computing [5].

Big data security and privacy research found that most scientists use a single risk assessment model, including: Analytic Hierarchy (AHP), Factor Analysis, Gray Theory [6], Fuzzy Evaluation Method [7], and Cloud Model [8].

Such methods are based on statistical theory and cannot completely escape the influence of subjectivity and theoretical assumptions. In recent years, machine learning has become an important research tool in the field of security and privacy [9]. When using machine learning methods for risk assessment and prediction, the accuracy is often superior to that of traditional statistical methods [10]. Popular machine learning methods include neural networks, SVMs, and clustering algorithms; The BP neural network is the most widely used neural network in risk prediction and assessment [11], but it is easy to fall into a local minimum in practical applications [12]. Therefore, researchers often use other algorithms to improve the accuracy of predictions and assessments. For example, Zhang (2021) established a regression model through the BP network and used the PSO algorithm to optimize the connection weights to evaluate the slow convergence of the BP network, in order to improve the accuracy. of outbreak prediction [13]. Wang (2019) et al. used the LM algorithm to improve the performance and accuracy of the traditional BP neural network, and at the same time provide an effective theoretical basis and modeling method for predicting the risks of electrical communication networks [14]. This greatly improves prediction and assessment accuracy, but a review of the relevant literature shows that analyzing the significance of the impact of the indicators is often overlooked. Therefore, in this paper, based on the consideration of machine learning, according to different degrees of risk impact, the AHP method is used to determine the weight of the index, overcoming the lack of subjective consideration in previous studies [15]. Neural network optimization genetic algorithm BP (here in after referred to as GABP) with better prediction and evaluation efficiency is used to evaluate [16], which is a successful attempt to realize the combination of energy fields and deep learning. Moreover, for the security and privacy risk assessment of energy big data, the current literature pays more attention to theoretical analysis and lacks a relatively perfect evaluation reference system. Starting from the full lifecycle of big data and considering the cloud environment, this article establishes an energy big data privacy and security risk index system, which enriches theory foundations and frameworks in the field to some extent.

2. THE INDEX SYSTEM OF SECURITY AND PRIVACY RISK ASSESSMENT OF

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

ENERGY BIG DATA IN CLOUD ENVIRONMENT

2.1 Principles for the Construction of the Index System

During the risk assessment, the probability of the occurrence of the risk, the extent of the loss and other factors should be comprehensively considered in order to obtain the probability and extent of the occurrence of systematic risk, determine level of risk and then decide whether to implement the corresponding control measures and to what extent [17].

Therefore, the building of a risk assessment index system needs to follow the principles of completeness, science, representation and feasibility, selection of representative risk factors in a scientific manner, risk quantification is based on practical principles and strives to demonstrate a level of risk management, comprehensively and accurately.

2.2 Identification of Risk Factors

Managing data security is the most significant risk faced by big data applications. Although big data is stored centrally, which is convenient for data analysis and processing, the loss and damage of big data due to poor security management will lead to catastrophic disaster. Due to the development of new technology and new activities, privacy violations are not limited to physical and forced invasions, but originate in more sophisticated ways through a variety of other data and the security and data privacy risks posed by this will be more than serious [18].

Compared with the Internet and previous computer technology, the application advantage of big data in the cloud environment is more obvious. Big data platform has strong sharing ability, can manage the security of usage information and improve resource efficiency. The construction of cloud platforms and system applications has strict standards. Cloud computing technology provides more comprehensive technical support and makes privacy management more reasonable, in line with the level of technology development in the new era [19]. But from another angle, it is under the influence of the sharing features of the cloud platform, that part of the information is easily exposed, creating an opportunity for some illegal intrusions. Therefore, we must pay special attention to its risks.

Based on Xu [20], Tawalbeh [21] combined with the analysis of related cases and consultation with experts, this article follows the principle of setting the above evaluative index, combined with the development characteristics. Development of big data security energy and consider the impact of the cloud environment. From the perspective of the entire big data lifecycle, this document summarizes the current privacy risks of cloud computing and big data and breaks down the risk assessment factors into five phases: data collection, data transmission, data storage, data use and data destruction, for a total of 22 clues, as shown in Table 1.

2.3 Index Quantification

In terms of data collection, to quantify the security and privacy risk indicators of big energy data, this study introduces the concept of level of risk. Depending on the probability of occurrence and level of loss of each risk indicator, the product of the probability and the degree of loss is used as a reference standard to quantify the level of risk and the specific value of the risk, can reasonably be changed around the product. The quantification of probability and degree of loss can be divided into 5 levels: very high risk (5 points), high

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

risk (4 points), medium risk (3 points), low risk (2 points) and very low risk (1 point).

$$R = P * L \quad (1)$$

In formula (1), P is the probability of occurrence and L is the degree of loss.

The normalized input value is multiplied by the corresponding weight of each index as input to the neural network for training, combined with the output value; the level of risk assessment achievable, as shown in Table 2.

Table 1. Security and privacy risk assessment index system based on the whole life cycle of energy big data.

Risk Factors				
Data Collection A	**Data Transmission B**	**Data Storage C**	**Data Used D**	**Data Destruction E**
1.Software and hardware fault risk A1 2.Damage or consumption risk of energy infrastructure A2 3.External malicious attack A3 4.Irresistible force risk A4	1. Malicious intercepting risk B1 2. Malicious tampering risk B2 3. Data distortion risk B3 4. Access control risk B4 5. Cloud platform risk B5	1. Sleeping data risk C1 2. Quality of data input risk C2 3. Data leakage risk C3 4. Management data destruction risk C4 5. Virus intrusion risk C5	1. Multi source data fusion risk D1 2. Privacy awareness of business personnel D2 3. Data parsing risk D3 4. Data regulatory risk D4 5. Manage authorizatio n risk D5	1. Data residual risk E1 2. Data backup risk E2 3. Termination of cloud service agreement risk E3

Table 2. Risk assessment level.

Risk level	Meaning
First class ($0 \le R \le 0.2$)	The risk level is very low, so it is not necessary to pay special attention to it. The plan and general prevention can be made.
Second class ($0.2 < R \le 0.4$)	The risk level is low, the plan and general prevention should be made and need to be checked regularly.
Third class ($0.4 < R \le 0.6$)	The risk level is medium; the major risk factors should be paid attention to in combination with the specific situation and the corresponding counter measures should be formulated.
Fourth class ($0.6 < R \le 0.8$)	The risk level is high; it is necessary to pay attention to all the risk factors that may threaten the security of energy data, formulate the process sequence after the occurrence of the risk according to the importance degree and track the inspection and evaluation.
Fifth Class ($0.8 < R \le 1.0$)	The risk level is very high; if necessary, it can be stopped and maintained and the comprehensive inspection and special evaluation should be carried

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

	out immediately and can be continued after improvement.

3. ASSESSMENT MODEL OF ENERGY BIG DATA SECURITY AND PRIVACY RISK IN CLOUD ENVIRONMENT

3.1. AHP Method

In the existing BP neural network part of the process, all risk factor types are defaulted to the same level of impact, without strict segregation, which is not favorable for designing neural network modeling.

Considering the particularity of energy and privacy big data security risks, quantitative analysis may not reasonably determine the actual impact of the indicators. Therefore, the AHP method is used to give weights to the clues in this article and the various elements of the complex problem are divided into linked and ordered levels to make them. According to the structure of subjective judgment about a given objective fact, the opinions of experts and the results of the objective judgment of analysts are directly and effectively combined and the importance of a pairwise comparison of quantitatively described single-level items.

Therefore, after setting up the privacy index system and assessing the energy big data security risks, according to the degree of influence of each risk factor, the Delphi method is used to invite the expert quantifies the importance between them and the AHP Method is used to give corresponding weights for the 22 indicators.

a) Construct the judgment matrix. The judgment matrix $A=(a_{ij})$ n*n is established by pair wise comparison. In order to make the judgment quantitative, the quantitative scale is given for the evaluation of different situations. The scale specification is mention in Table 3.

b) Simply calculate the Eigen value and Eigen vector by the square root method and calculate the product of elements in each row of judgment matrix.

C.I. ≤ 0.10 represents that the judgment matrix is consistent. With the increase of value n, the judgment error will increase, so the influence of n should be considered when judging the consistency and the random consistency ratio C.I/R.I should be used, where R.I. is the average random consistency index. Table 3 represents the average random consistency index test values obtained by the judgment matrix.

3.2 BP Neural Network

BP neural network is a type of multilayer neural network, proposed by Rumelhart in 1986. It is one of the most widely used neural network models today. It can learn and store a large number of input-output model mapping relationships. Its learning rule is to use the steepest descent method to continuously adjust the weights and thresholds of the network by back propagation, in order to minimize the mean square error of the network. It usually consists of an input layer, a hidden layer and an output layer [23] and its network model is shown in Figure 1.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

In BP neural network, the mean square error E is used as the index to judge the training performance of the model. The principle of minimizing the mean square error by adjusting the network weights is shown in formula (9), where e is the network error vector, y_i is the model output, and t_i is the target output.

Table 3. Scale specification.

Scale	Meaning (ai vs aj)
2,4,6 and 8	The intermediate value of the above two adjacent judgments
9	Former extremely is more important than the latter
7	Former is strongly more important than the latter
5	Former is obviously more important than the latter
3	Former is slightly more important than the latter
1	Former is as important as the latter

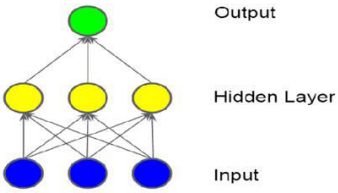

Figure 1. Structural model of neural network.

Compared with binary encoding, real encoding can greatly reduce the encoding length and avoid subsequent decoding, with high accuracy. A series of parameters that need to be optimized, such as connection weights, hidden layer node thresholds and output layer node thresholds, are encoded by the actual control matrix with a range of values [1,1]. After coding, selection, crossover and mutation were performed. These three activities are based on the fitness value calculated by the fitness function as the benchmark. The smaller the value, the greater the fitness value and the better the individual.

In the selection operation, the most common roulette method is used. The probability that each individual is selected is proportional to its fitness value. N represents the size of the population, Fi represents the value of the fitness function of individual i and pi represents the probability that the i^{th} individual will be selected. The calculation is as follows:

(1) Use AHP method to process data.
(2) Determine the topological structure of BP neural network.
(3) After the weights are given by AHP, determine the input and output sample set and test sample set of training.
(4) The network parameters to be optimized are real-coded to form their own chromosomes.
(5) Determine the parameters of selection, crossover and mutation.
(6) Set the population size popu.
(7) After inputting samples, each chromosome produces corresponding output after network transmission.
(8) The fitness value of each chromosome is calculated by fitness function and the selection operation is carried out according to the fitness value.
(9) A new generation of population is generated by crossover and mutation.
(10) Repeat steps 6–8 until the fitness value of the optimal individual and the fitness value of

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

the population do not rise within the specified number. Use arithmetic hybridization as formula (13), one individuals are obtained using a linear match between the two, where d is a random number with a uniform distribution in [0,1].

3.3. Construction of AHP-GABP Model

Compared with the traditional BP neural network, the GABP model uses a genetic algorithm to optimize the weights and thresholds of the network, and this process can optimize the prediction performance of the BP neural network to some extent. At the same time, using the AHP method to determine the weight of the indicator can better disadvantage of network complexity, thus reducing effectiveness of training [25]. For the multi-input single-output network model established in this paper, in order to increase the approximation and convergence effects and reduce the oscillation during simulation, the number of hidden layer nodes is determined by referencing the refer to equation (15) and combine with the simulation results of real numbers.

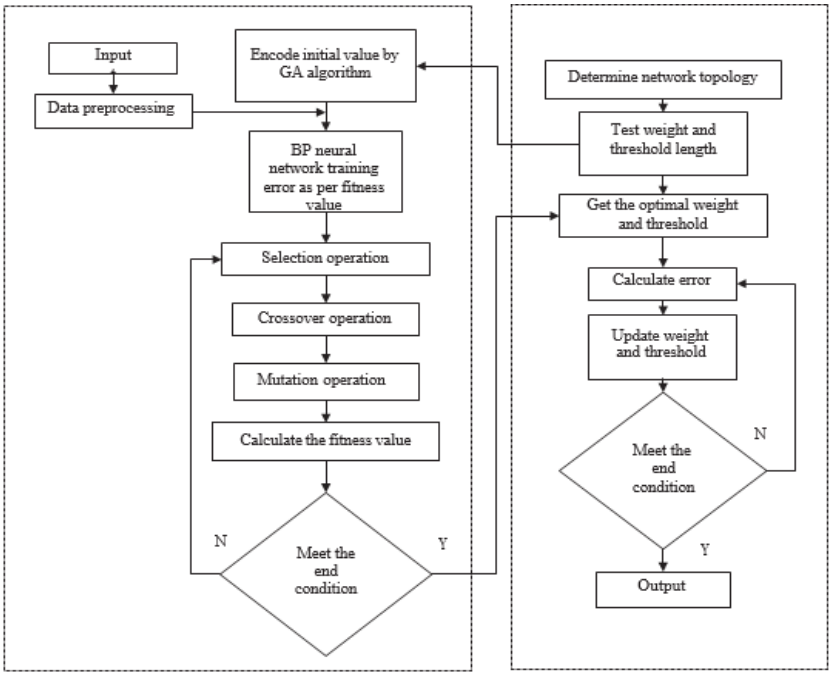

Figure 2. AHP-GABP flowchart.

4. PARAMETER SETTING

This study uses a feed-forward network to generate a function, train lm to train the function, logic to transfer the function, sigmoid to activate the function, and MSE to represent the error E. Training time is 100, scale learning is 0.01 and training target error is 0.01. For the genetic algorithm part, the number of populations is set to 100, the maximum evolutionary algebra is set to 100, the variable precision is 1e 6, the crossover probability is 0.8, and the mutation probability is 0.2.

4.1.Training Results

After reading the literature and cases on the security and privacy risks of energy big data, a total of 44 samples were collected, including 36 training samples and 8 testing samples. Some of the training data is shown in Table 4. Model training was achieved by programming MATLAB and developing the Goat Genetic Algorithm Toolkit. The training data is entered

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

into the program and the convergence curve of the BP neural network optimized by the genetic algorithm is shown in Figure 5. From the figure, it can be seen that the algorithm of the BP neural network is optimized after optimization. An optimal path optimization solution when iterating the population about 60 generations, this shows the superiority of the genetic algorithm in neural network weight and BP threshold optimization. We can also see that the optimal function tends to be stable when iteratively close to 70 generations.

The BP neural network and the optimized genetic BP neural network are compared and their error values calculated. The final experimental results are shown in Table 5. Through analysis and comparison, in 8 groups of samples, predicting AHPGABP has significant advantages over predicting BP, with larger error than small, cycle time. Shorter evaluation period and more improved evaluation performance. As shown in Table 5 and Figure 5, the genetic algorithm-optimized BP neural network improves the shortcomings of the BP neural network, thereby greatly improving the predictive power of the neural network. At the same time, the application evaluation results of the genetic algorithm optimization BP neural network in the security and privacy risks of energy big data are basically consistent with the actual evaluation results of experts, shows that the training network has high accuracy.

4.2. Model Applications

4.2.1. Background

Power Grid System Z uses energy big data information to provide data services related to economic development. It can provide more reliable data support for poverty alleviation effectiveness assessment, credit assessment, census, pollution monitoring and work continuation assessment. According to the energy big data privacy and security risk assessment index system designed above, the comprehensive privacy and big data security risk assessment steps of the power grid this is as follows:

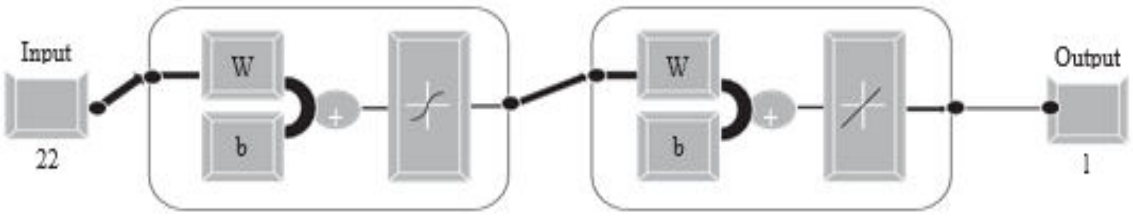

Figure 3. MATLAB structure.

Table 4. Training samples.

	1	2	3	4	5	6	7	8
A1	0.7029	0.5020	0.6034	0.6526	0.5522	0.6024	0.6024	0.5532
A2	0.3784	0.8514	0.9933	1.0406	0.6622	0.6622	0.6149	0.2838
A3	0.5401	0.2700	0.7199	0.8100	0.4049	0.2690	0.4500	0.1800
A4	0.3612	0.3010	0.4515	0.5418	0.2408	0.3010	0.3311	0.2408
B1	0.0516	0.0344	0.1290	0.1290	0.0688	0.0774	0.0688	0.0430

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

B2	0.0748	0.0408	0.1088	0.1360	0.0680	0.0816	0.0476	0.0476
B3	1.4922	0.9948	1.9067	0.9948	1.4922	1.2435	1.0777	0.9948
B4	1.9100	2.1965	2.0055	1.1460	2.0055	1.2415	1.3370	0.9550
B5	0.4992	0.6240	0.5408	0.3328	0.5824	0.2496	0.4160	0.2496
C1	0.1854	0.4326	0.4326	0.1545	0.5871	0.3090	0.2781	0.2163
C2	0.0648	0.1620	0.1944	0.0810	0.2430	0.1134	0.1134	0.0486
C3	1.6300	1.6300	2.2820	1.6300	1.9560	1.7930	1.6300	1.4670
C4	1.8032	1.0304	2.0608	0.7728	1.2880	2.7048	1.8032	1.2880
C5	0.5130	0.5130	1.0260	0.4617	0.5130	0.9747	0.4104	0.4104
D1	0.2808	0.5967	0.6318	0.2808	0.3159	0.5265	0.2106	0.3159
D2	0.5136	0.3531	0.6741	0.3210	0.3210	0.6420	0.2247	0.2247
D3	0.1932	0.1380	0.2208	0.0966	0.0828	0.2346	0.0966	0.0828
D4	0.3108	0.4144	0.3626	0.2331	0.1813	0.4662	0.2072	0.2072
D5	0.2100	0.2520	0.1680	0.1260	0.1680	0.3360	0.1260	0.1680
E1	0.7434	0.2891	0.7847	0.4956	0.4130	0.5369	0.8260	0.4130
E2	0.1261	0.1164	0.1358	0.0970	0.0582	0.1358	0.1552	0.0582
E3	0.0156	0.0117	0.0312	0.0156	0.0195	0.0234	0.0546	0.0234
Output	0.7813	0.7558	0.9149	0.6012	0.7801	0.7889	0.5989	0.4569
Risk Level	4	4	5	4	4	4	3	3

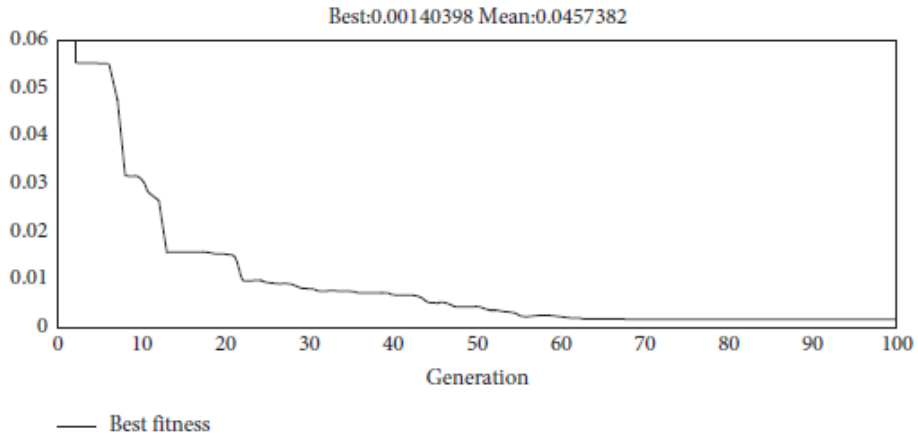

Figure 4. Fitness value.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

Table 5. Comparison of training sample error between BP neural network and AHP-GABP neural network.

TABLE 5: Comparison of training sample error between BP neural network and AHP-GABP neural network.

Sample number	Real value	Predictive value		Error	
		BP	AHP-GABP	BP	AHP-GABP
1	0.7813	1.4328	0.7717	0.6515	−0.0096
2	0.7558	0.4292	0.7443	−0.3266	−0.0115
3	0.9149	1.9229	0.8984	1.0080	−0.0165
4	0.6012	−1.0077	0.5324	−1.6089	−0.0688
5	0.7801	0.3213	0.7503	−0.4588	−0.0298
6	0.7889	0.7989	0.8125	0.0100	0.0236
7	0.5989	1.3607	0.5810	0.7618	−0.0179
8	0.4569	−0.0912	0.4442	−0.5481	−0.0127

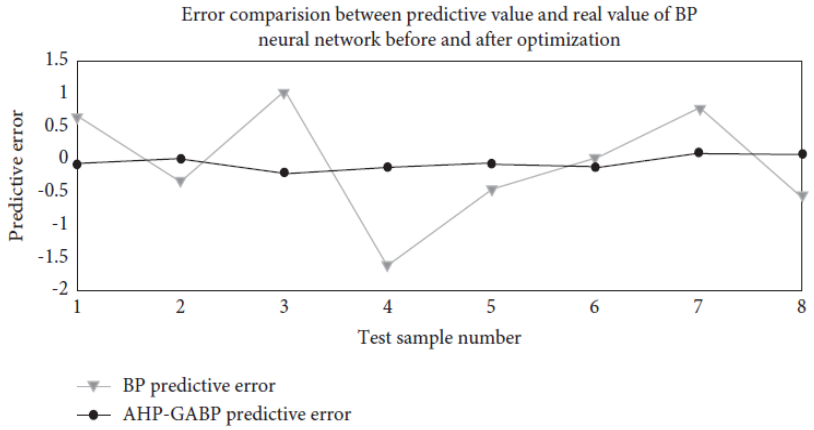

Figure 5: Error comparison between predictive value and real value.

Table 6. Weights of Risk Assessment

First-level index	Second-level index	Weight
Data collection A	Software and hardware fault risk A1	0.0601
	Damage or consumption risk of energy infrastructure A2	0.0270
	External malicious attack A3	0.1058
	Irresistible force risk A4	0.0108
Data transmission B	Malicious intercepting risk B1	0.1774
	Malicious tampering risk B2	0.1133
	Data distortion risk B3	0.0720
	Access control risk B4	0.0210
	Cloud platform risk B5	0.0317
Data storage C	Sleeping data risk C1	0.0124
	Quality of data input risk C2	0.0163
	Data leakage risk C3	0.1237
	Management data destruction risk C4	0.0324
	Virus intrusion risk C5	0.0680
Data use D	Multi source data fusion risk D1	0.0432
	Privacy awareness of business personnel D2	0.0046
	Data parsing risk D3	0.0113
	Data regulatory risk D4	0.0165
	Manage authorization risk D5	0.0071
Data destruction E	Data residual risk E1	0.0135
	Data backup risk E2	0.0245
	Termination of cloud service agreement risk E3	0.0074

4.2.2. Assessment Results

In this study, three groups of related data collected by the power grid are selected. After training, the AHPGABP neural network model is set up. First, check that the pricing model makes sense. Second, a risk assessment is required. The assessment results shown in Table 6 show that the risk level of the grid system is Level 1, similar to the normal risk level of the power grid system. Low level of risk, no special handling required and regular testing is carried out. It also shows that the AHPGABP algorithm is reasonable and correct in assessment and prediction, with high prediction accuracy, objective and fair evaluation

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

results, wide application range, and valuable application, high practical use.

5. CONCLUSION AND DEVELOPMENT SUGGESTIONS

In summary, in the process of controlling energy big data privacy and security risks, the risk of every step cannot be ignored. Assuming that it comprehensively considers the cloud environment and risk factors, this document breaks down the security and privacy risks of big data the potential energy of each stage as completely as possible. Can follow the big data lifecycle and use the AHP method to assign weights to the index, providing a benchmark for future energy big data research. At the same time, this paper optimizes the BP neural network model based on the assessment and tries to apply the AHPGABP method to assess the privacy and security risks of big data energy, which greatly reduces the risk. When randomly selecting the first weights and thresholds in the BP algorithm makes the model training easy to fall to the local minimum, improves the accuracy of neural network model evaluation and prediction, and realizes the application of the AI-related knowledge in the energy sector.

The AHPGABP model was applied to evaluate the security and privacy of energy big data, and the evaluation results were good. Based on case studies and expert interviews, the following development recommendations are summarized for general energy big data privacy and security risks.

Pay Attention to the Security of the Whole Life Cycle of Energy Big Data

Energy big data stems from production and management and operations data, and protecting that data must focus on the entire data collection, transmission, storage, use, and destruction lifecycle. From policy and system requirements to management and engineering controls, we must comprehensively assess the risk of critical data and develop targeted protection strategies at all levels.

Strengthen Technical Protection of Energy Industry Based on Big Data Security

The energy industry should deploy comprehensive threat early warning technology based on security big data, breaking with traditional practices and being more active in detecting potential security threats. The advent of big data analytics technology in threat detection can more comprehensively detect attacks against data assets, software assets, physical assets, personnel assets, and so on, service assets and other intangible assets that support operations [26]. At the same time, it is possible to expand the scope of analysis content. The threat analysis window can cover several years of data, so the threat detection is stronger and can respond to the attack effectively [27].

Consider Security and Privacy Issues from a Strategic and Long-Term Perspective

Big data presents opportunities and challenges for the energy industry. The more widely it is applied, the more value it brings. The concept of security management focusing on data security will change traditional working ideas [28]. We need to recognize new changes, new features and new trends in big data security, and thoroughly analyze the remaining issues of big data security in the current situation. In order to ensure that the big data energy information safety development strategy is suitable for the national conditions and is continuously improved, it is necessary to have a plan to provide the main focus of big data application, technology research and development. With the rapid development of cloud computing and continuously improving the digital level, the energy big data privacy and security risk assessment index system can be further improved. At the same time, with the

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

abundance of data indicators and training models, the model proposed in this article can also be better optimized and extended to other fields for evaluation and prediction, more precisely in the future.

REFERENCES

- Y. Ouadine, M. Mjahed, H. Ayad, and A. El Kari, "UAV quadrotor fault detection and isolation using artificial neural network and hammerstein-wiener model," Studies in Informatics and Control, vol. 29, no. 3, pp. 317–328, 2020.
- L. Fu and Y. Dong, "Research on internet search data in China's social problems under the background of big data," Journal of Logistics, Informatics and Service Science, vol. 5, pp. 55–67, 2018.
- D. Banciu, M. Ra˘doi, and S. Belloiu, "Information security awareness in Romanian public administration: an exploratory case study," Studies in Informatics and Control, vol. 29, no. 1, pp. 121–129, 2020.
- M. A. Naoui, L. Brahim, and M. Ayad, "Integrating iot devices and deep learning for renewable energy in big data system," UPB Scientific Bulletin, Series C: Electrical Times, vol. 82, pp. 251–266, 2020.
- M. Song, "Development of big data system for energy big data," KIISE Transactions on Computing Practices, vol. 24, no. 1, pp. 24–32, 2018.
- M. Mendonça Silva, T. Poleto, L. Camara e Silva, P. Henriques de Gusmao, and A. P. Cabral Seixas Costa, "A grey theory based approach to big data risk management using fmea," Mathematical Problems in Engineering, vol. 2016, Article ID 9175418, 15 pages, 2016.
- Y. Fu, X.. p. Wu, Q. Ye, and X. Peng, "An approach for information systems security risk assessment on fuzzy set and entropy-weight," Acta Electronica Sinica, vol. 38, pp. 1489–1494, 2010.
- L. Chen and H.-Y. Pan, "Cloud-model based decision-making for network risk assessment," Journal of Computer Applications, vol. 32, no. 2, pp. 472–474, 2013.
- R. Sagar, R. Jhaveri, and C. Borrego, "Applications in security and evasions in machine learning: a survey," Electronics, vol. 9, no. 1, p. 97, 2020.
- J. B. Kim, "Implementation of artificial intelligence system and traditional system: a comparative study," Journal of System and Management Sciences, vol. 9, pp. 135–146, 2019.
- O¨ ztu¨rk and F. Ta¸spinar, "Short term load forecasting for Turkey energy distribution system with artificial neural net- works," Tehnicki vjesnik - Technical Gazette, vol. 26, no. 6, pp. 1545–1553, 2019.
- S. Li, F. Bi, W. Chen, X. Miao, J. Liu, and C. Tang, "An improved information security risk assessments method for cyber-physical-social computing and networking," IEEE Access, vol. 6, pp. 10311–10319, 2018.
- M. Zhang, "Prediction of rockburst hazard based on particle swarm algorithm and neural network," Neural Computing and Applications, vol. 1, 2021.
- Y. Wang, K. Wang, R. Zhang, Q. Xue, X. Chen, and G. Zhang, "Risk assessment of power communication network based on LM-BP neural network," Journal of Physics: Conference Series, vol. 1187, no. 2, Article ID 022063, 2019.
- L. Wang and X. Bi, "Risk assessment of knowledge fusion in an innovation ecosystem based on a ga-bp neural network," Cognitive Systems Research, vol. 66, pp. 201–210,

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, S Iss 3, Dec 2022

2021.

- Zhu, J. Zhang, Y. Liu, D. Ma, M. Li, and B. Xiang, "Comparison of GA-BP and PSO-BP neural network models with initial BP model for rainfall-induced landslides risk assessment in regional scale: a case study in Sichuan, China," Natural Hazards, vol. 100, no. 1, pp. 173–204, 2020.
- Y. Li, M. Xu, X. Wen, and D. Guo, "The role of internet search index for tourist volume prediction based on gdfm model," Tehnicki vjesnik - Technical Gazette, vol. 27, no. 2, pp. 576–582, 2020.
- E. Anthi, A. Javed, O. Rana, and G. Theodorakopoulos, "Secure data sharing and analysis in cloud-based energy management systems," Cloud Infrastructures, Services, and IoT Systems for Smart Cities, pp. 228–242, Springer, 2017.
- H. Bommala and S. Kiran, "Cloud computing technology for digital economy," i-manager's Journal on Cloud Computing, vol. 7, no. 1, p. 1, 2020.
- L. Lei Xu, C. Chunxiao Jiang, J. Jian Wang, J. Jian Yuan, and Y. Yong Ren, "Information security in big data: privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.
- L. a. A. Tawalbeh and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," Journal of King Saud University - Computer and Information Sciences, vol. 33, no. 7, pp. 810–819, 2021.
- Y. He and J. Ji, "Analysis of information security risk defense in the development of big data," Journal of Physics: Conference Series, vol. 1881, no. 3, Article ID 032048, 2021.
- Lorenc, M. Kuz´nar, T. Lerher, and M. Szkoda, "Predicting the probability of cargo theft for individual cases in railway transport," Tehnicki vjesnik - Technical Gazette, vol. 27, no. 3, pp. 773–780, 2020.
- Y. Xing and F. Li, "Research on the influence of hidden layers on the prediction accuracy of GA-BP neural network," Journal of Physics: Conference Series, vol. 1486, Article ID 022010, 2020.
- Y. . s. Qian, J. . w. Zeng, S. . f. Zhang, D. . j. Xu, and X. . t. Wei, "Short-term traffic prediction based on genetic algorithm improved neural network," Tehnicki vjesnik - Technical Ga- zette, vol. 27, no. 4, pp. 1270–1276, 2020.
- Y. Tabsh and V. Davidavic˘ien_e, "Ict in energy security and efficiency assurance," Journal of System and Management Sciences, vol. 9, pp. 1–18, 2019.
- Y. Fu, H. Li, X. Wu, and J. Wang, "Detecting apt attacks: a survey from the perspective of big data analysis," Journal on Communications, vol. 36, pp. 1–14, 2015.
- N. Tijani and O. D. Popoola, "Challenges and opportunities in organizational operations and research methods," Journal of Logistics, Informatics and Service Science, vol. 6, pp. 23–42, 2019.