sensors

MDPI

Article

Security Risk Intelligent Assessment of Power Distribution Internet of Things via Entropy-Weight Method and Cloud Model

Siyuan Cai [1], Wei Wei [1], Deng Chen [1,*], Jianping Ju [2], Yanduo Zhang [1], Wei Liu [1] and Zhaohui Zheng [3]

[1] Hubei Province Key Laboratory of Intelligent Robot, Wuhan Institute of Technology, Wuhan 430079, China; csy@stu.wit.edu.cn (S.C.); 15011801@wit.edu.cn (W.W.); zhangyanduo@hotmail.com (Y.Z.); liuwei@wit.edu.cn (W.L.)
[2] School of Artificial Intelligence, Hubei Business College, Wuhan 430079, China; jjp@hbc.edu.cn
[3] School of Mathematics and Physics, Wuhan Institute of Technology, Wuhan 430079, China; zhengzhaohui@whu.edu.cn
* Correspondence: dchen@wit.edu.cn

Abstract: The current power distribution Internet of Things (PDIoT) lacks security protection terminals and techniques. Network security has a large exposure surface that can be attacked from multiple paths. In addition, there are many network security vulnerabilities and weak security protection capabilities of power distribution Internet of Things terminals. Therefore, it is crucial to conduct a scientific assessment of the security of PDIoT. However, traditional security assessment methods are relatively subjective and ambiguous. To address the problems, we propose to use the entropy-weight method and cloud model theory to assess the security risk of the PDIoT. We first analyze the factors of security risks in PDIoT systems and establish a three-layer PDIoT security evaluation index system, including a perception layer, network layer, and application layer. The index system has three first-level indicators and sixteen second-level indicators. Then, the entropy-weight method is used to optimize the weight of each index. Additionally, the cloud model theory is employed to calculate the affiliation degree and eigenvalue of each evaluation index. Based on a comprehensive analysis of all evaluation indexes, we can achieve the security level of PDIoT. Taking the PDIoT of Meizhou Power Supply Bureau of Guangdong Power Grid as an example for empirical testing, the experimental results show that the evaluation results are consistent with the actual situation, which proves that the proposed method is effective and feasible.

Keywords: power distribution Internet of Things; security risk assessment; evaluation index system; entropy-weight method; cloud model

Citation: Cai, S.; Wei, W.; Chen, D.; Ju, J.; Zhang, Y.; Liu, W.; Zheng, Z. Security Risk Intelligent Assessment of Power Distribution Internet of Things via Entropy-Weight Method and Cloud Model. *Sensors* **2022**, *22*, 4663. https://doi.org/10.3390/s22134663

Academic Editors: Hai Liu, Anne Roudaut, Zhanpeng Shao and Tingting Liu

Received: 9 May 2022
Accepted: 15 June 2022
Published: 21 June 2022

1. Introduction

The techniques of the Internet of Things (IoT) have been widely used in electric power distribution networks and form the PDIoT. Different from the traditional power distribution network (PDN), PDIoT has may distinctive characteristics: (1) it has a complex network architecture, (2) master stations are located in the cloud, (3) electric terminal devices are connected by the IoT, and (4) it has a flexible architecture, which can be freely expanded. The above characteristics make the PDIoT more vulnerable than traditional PDN. In recent years, the network security situation has become increasingly severe, and the security events of IoT and industrial control systems [1,2] have increased year by year [3,4]. Through analysis, we found that most of the security problems in PDIoT originated from the following sources: sensors, the network, and terminal devices. Some functional components in the sensors may be attacked to obtain abnormal data and affect system stability. In addition, with functional components as a pluggable expansion module, there may be security risks, permission abuse, and other issues. Network security has a large exposure surface, and a large number of terminals and network interfaces will be deployed to the user side and all levels of system nodes. Malicious attackers can gain

physical access to a very large number of points, and these points are difficult to monitor in a comprehensive and timely manner. The terminal devices can attack more paths, such as tablets and other mobile terminals running on various types of third-party developed measurement and control equipment management software, and there may be data leakage, malicious attacks, abuse of privileges, and other abnormal behavior. Therefore, scientific evaluation of the safe and reliable performance of the PDIoT system and a timely grasp of the operation and maintenance status of the distribution network are of great significance to guarantee the security of the PDIoT.

At present, the security assessment of the PDIoT is facing problems of subjectivity and repetition. The traditional reliability assessment method is rule- or model-driven. The main research methods include the fuzzy comprehensive evaluation method, principal component analysis, analytic hierarchy process, etc. For example, Guo et al. [5] proposed a security risk evaluation method for urban power grids based on the fuzzy comprehensive evaluation method, and calculated the security risk level of a city, providing a basis for power grid enterprises to put forward risk control measures in terms of management measures, technical measures, and working standards. However, there is a strong subjectivity in determining the index weights with a complicated calculation process. He et al. [6] applied the principal component analysis method to reduce the dimensions and compress the original variables of power equipment status to obtain the principal component system, and then established a comprehensive evaluation model based on the principal component system to perform a comprehensive and objective evaluation of power equipment status, which has certain practicability. However, the meaning of the integrated evaluation function in this method is unclear when the sign of the factor loadings is positive or negative. Lu et al. [7] designed a state evaluation method of an electric energy metering device by using the analytic hierarchy process and obtained the conclusion of fuzzy evaluation of the operating state of electric energy metering devices. However, it is difficult to conduct consistency tests on the judgment matrix, and the selection of test criteria also lacks a sufficient basis [8].

In response to the above problems, we establish a security evaluation index system for PDIoT based on sensors, networks, and terminal devices, and abstract it into three levels: sensing layer, network layer, and application layer. We record these three levels as primary evaluation indexes, and establish secondary evaluation indexes under each primary index, totaling 16. The entropy power method is introduced to establish the evaluation matrix of PDIoT indexes and carry out the structural entropy calculation, and the cognitive blindness is processed to obtain the weight coefficient ratio of evaluation indexes, which can combine subjective and objective assignment [9]. The cloud model theory is used to study the safety evaluation of the PDIoT system, which can solve the problems of complexity and uncertainty and reveal the inner relationship between randomness and fuzziness [10], which is more consistent with objective facts and higher accuracy of evaluation results than traditional evaluation methods, and makes the evaluation results more intuitive and accurate.

We applied the above method to conduct a security risk assessment on the PDIoT system of the Meizhou Power Supply Bureau of Guangdong Power Grid, and the experiment shows that the security risk level of the PDIoT in this area is "better", in which the security risk of the network layer is slightly higher, and the security of the sensing layer and the application layer is better. The overall evaluation results are consistent with the facts.

Our main contributions can be summarized as:

- Proposing a novel approach to PDIoT security assessment, combining subjective and objective assignment of evaluation indicators, while enabling the interconversion between qualitative and quantitative evaluation indicators, as well as making the evaluation results more intuitive and accurate.
- Constructing a new security evaluation index system for PDIoT and scoring criteria.
- Putting forward improvement suggestions for modules of potential security risks for the PDIoT.

The rest of this paper is organized as follows. In Section 2, we construct the evaluation index system scientifically and systematically, and set the scoring criteria and principles according to the characteristics of PDIoT. In Section 3, we introduce the entropy-weight method and calculate the weight of each index based on the entropy-weight method. In Section 4, we introduce the cloud model theory, build a comprehensive cloud model of the PDIoT, and use the PDIoT system of Meizhou Power Supply Bureau of Guangdong Power Grid as an example to carry out an empirical test to determine the security level of the PDIoT system in the region and provide the corresponding analysis of the evaluation results. The main conclusions of this paper are presented in Section 5.

2. Construction of Evaluation Index System

2.1. Construction of Security Evaluation Index

The establishment of the evaluation index system of PDIoT should conform to the principles of systemic and scientific evaluation and be operable, and the evaluation indexes should be independent of each other [11,12]. According to the fact that the PDIoT has a similar architecture to other IoT applications and is basically the same in terms of technology and functional level, and the security flaws of PDIoT mainly come from three aspects: sensors, network, and terminal devices, we abstracted it into three levels: perception layer, network layer, and application layer [13]. We recorded these three levels as the first-level evaluation index, referring to the relevant standards of the PDIoT, and established a second-level evaluation index under each first-level index, with a total of 16 indicators, as shown in Figure 1.

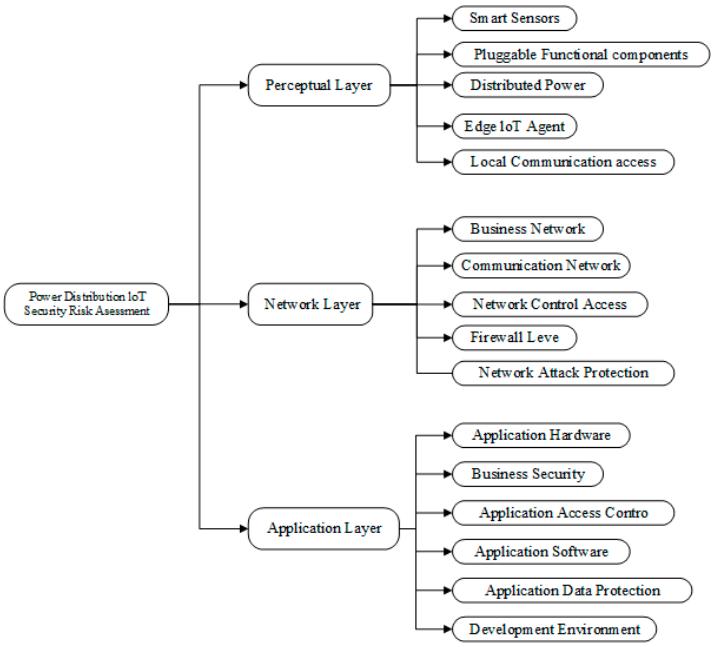

Figure 1. Evaluation index of three-layer architecture of PDIoT system.

2.2. Scoring Criteria and Principles

Based on the characteristics of PDIoT and combined with the security evaluation theory, we divided the security evaluation level of the PDIoT system and the rating of each evaluation index into five levels: "excellent", "superior", "moderate", "poor", and "awful". Indicators were unified using a 10-point scale, that is, all evaluation indicators were assessed in the range of [0, 10], with higher scores indicating higher security. According to the relevant industry standards, operating procedures, and expert recommendations, we divided the evaluated values into five intervals, namely: [0, 3), [3, 5), [5, 7), [7, 9), and [9, 10], and the corresponding five levels are "awful", "poor", "moderate", "superior", and "excellent".

3. Determination of Evaluation Index Weights

3.1. Entropy-Weight Method

In the whole evaluation system, different weights need to be assigned to each indicator due to the varying importance of each [14]. We used the entropy-weighting method to determine the weights of each evaluation index, which can balance the subjectivity and objectivity of the weight calculation and combine qualitative analysis with quantitative analysis.

(1) Expert opinion collection. In this study, we conducted a questionnaire survey with five experts, including technical leaders and senior engineers of a power supply section, etc. The five experts independently provided their opinions on the importance of each evaluation index set based on their professional knowledge and practical experience in an anonymous manner. The importance ranking is shown in Table 1. The higher the ranking, the higher the importance.

Table 1. Expert ranking table of importance of first-level indicators.

Experts	A_1	A_2	A_3
Expert 1	1	3	2
Expert 2	1	2	3
Expert 3	2	3	1
Expert 4	1	3	2
Expert 5	2	1	3

(2) Blindness analysis of typical ranking [15]. We used entropy theory to calculate the entropy values of the three first-level indicators: perception layer, network layer, and application layer, to reduce the inconsistency and uncertainty in the ranking of different indicator systems by various experts. The specific method was as follows: the set of indicators corresponding to each consulting expert is denoted as $U = \{u_1, u_2, \ldots, u_n\}$, and the ranking array corresponding to U is denoted as $(a_{i1}, a_{i2}, \ldots, a_{in})$, so as to obtain the ranking matrix of each indicator, $A = (a_{ij})_{k\times n}$.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{k1} & a_{k2} & a_{k3} & a_{kn} \end{bmatrix}$$

Calculating the affiliation degree of each expert index: Through qualitative transformation of the above expert opinion according to the information entropy function $\chi(l) = -\lambda p_n(l) \ln(p_n(l))$, the affiliation degree of each expert index is calculated:

$$p_n(l) = \frac{m-l}{m-1}, \ \lambda = \frac{1}{\ln(m-1)} \tag{1}$$

where l is the number of the important ranking given by experts according to the first-level indicators, k is the number of experts involved in the consulting survey, here take $k = 3$, and n is the number of evaluation indicators: as there are three first-level indicators, take $n = 3$. a_{ij} is the evaluation of the ith expert on the jth indicator, u_j, which can also be expressed as the number of the ranking of a certain expert on an indicator. The value range of a_{ij} is {1, 2,..., j}, where j represents the maximum ordinal number, here take $j = 3$. m is the number of transformed parameters, take $m = j + 2$, that is $m = 5$. Make:

$$\frac{\chi(l)}{\frac{(m-l)}{(m-1)}} - 1 = u(l) \tag{2}$$

where $u(l)$ is a function defined as [0, 1]. Bringing each A in matrix $l = a_{ij}$ into the above equation, for the quantitative transformation of a_{ij}, the corresponding affiliation function a_{ij} of $u(a_{ij})$ is rewritten as:

$$u(a_{ij}) = \frac{\ln(m - a_{ij})}{\ln(m - 1)} \tag{3}$$

The affiliation matrix $B = (b_{ij})_{k \times n}$ is obtained by setting $b_{ij} = u(a_{ij})$. Approximating that the experts involved in the research have the same "right to speak", i.e., the ranking of each evaluation index, u_j, is equally important, the average affiliation of the ranking number of five experts in the evaluation index, u_j, is called the average recognition degree, which is denoted as b_j, so that:

$$b_j = (b_{1j} + b_{2j} + \ldots + b_{nj})/k \tag{4}$$

Let the uncertainty generated by the expert's perception of the PDIoT assessment factor u_j be the awareness blindness, denoted as Q_j, such that:

$$Q_j = \sqrt{\frac{1}{k}\sum_{i=1}^{k}(b_{ij} - b_j)^2} \tag{5}$$

Then, the overall awareness degree (x_j) of the k experts is:

$$x_j = b_j(1 - Q_j), x_j > 0 \tag{6}$$

(3) Normalization is carried out to obtain the indicator, u_j, weights, which are normalized to $x_j = b_j(1 - Q_j)$. Let:

$$v_j = x_j / \sum_{i=1}^{n} x_i \tag{7}$$

3.2. Results of Weight Calculation

According to the calculation process of the above steps, the weights, v_j, of the primary indicators can be obtained, and the above method was also used to calculate the weights of the secondary indicators under each primary indicator. The calculation results are shown in Table 2.

Table 2. Weight of PDIoT three-level security evaluation index calculated according to the entropy-weight method.

Tier 1 Indicators	Secondary Indicators
Perceptual Layer A_1 (0.378)	Smart sensors A_{11} (0.262) Pluggable functional components A_{12} (0.250) Distributed power A_{13} (0.133) Edge IoT agent A_{14} (0.173) Local communication access A_{15} (0.182)
Network Layer A_2 (0.214)	Communication network A_{21} (0.223) Business network A_{22} (0.244) Firewall level A_{23} (0.161) Network control access A_{24} (0.262) Network attack protection A_{25} (0.129)
Application Layer A_3 (0.399)	Application software A_{31} (0.124) Application hardware A_{32} (0.109) Development environment A_{33} (0.140) Business security A_{34} (0.198) Application access control A_{35} (0.218) Application data protection A_{36} (0.211)

4. Cloud Theory and the Construction of the Cloud Evaluation Model

4.1. Definition of Cloud Model

The cloud model is a cognitive computing model that realizes the conversion between qualitative and quantitative representation on the basis of the combination of probability theory and fuzzy mathematics theory. It can reflect the internal relationship between fuzziness and randomness and establish the mapping between qualitative and quantitative data. In recent years, this method has been widely used in various fields, such as data mining [16], algorithm improvement [17], system measurement [18], and decision support [19].

The cloud model represents its overall characteristics through three parameters: expectation, Ex, entropy, En, and super-entropy, He. Ex represents the expectation of the distribution of cloud drops in the domain space, which is the most typical sample of this concept of quantification, a point representing the qualitative concept [20]. En reveals the association between vagueness and randomness, and is used to measure the vagueness and probability of the qualitative concept. He is the uncertainty measure of entropy, i.e., the entropy reflects the cohesiveness of the uncertainty of all points representing the linguistic value in the number field space, i.e., the cohesiveness of the cloud drops [21].

4.2. Cloud Model Algorithm

The cloud generator is a specific method to realize the cloud model, including forward and reverse cloud generators. Among them, the forward cloud generator generates a cloud map through the characteristic numbers Ex, En, He of the cloud, which can reflect the process from a qualitative concept to a quantitative expression [22]. In this paper, the three digital characteristics of each evaluation index of PDIoT were calculated, and then the standard cloud map and comprehensive evaluation cloud map were generated through the cloud forward generator to evaluate the risk level of PDIoT. The generation algorithm of the cloud graph in the cloud model is the forward cloud generator. The forward cloud generator is an algorithm that can convert qualitative concepts into quantitative values. It was used to generate cloud droplets in this paper. The algorithm of the forward cloud generator is as shown below, Algorithm 1.

Algorithm 1 Forward cloud generator

Input: $\{Ex, En, He\}$;
Output: $\{Drop(x_i, u_i), i = 1, 2, \ldots, n\}$

1. Generate normal random numbers $En_i' \sim N(En, He^2)$;
2. Generate normal random numbers $x_i' \sim N(En, En_i')$;
3. Find the cloud drops $u(x_i) = \exp\left(-\frac{(x_i - Ex)^2}{2(En_i')^2}\right)$;
4. $u(x_i)$ is the degree of determination and x_i is 1 cloud drop in the number field;
5. Repeat steps 1–4 until N cloud drops are generated. Let the left boundary of each rating interval of the evaluation index be I_{min} and the right boundary be I_{max} Cloud parameters (Ex, En, He) are determined by I_{min} and I_{max}:

$$\begin{cases} Ex = (I_{max} + I_{min})/2 \\ En = (I_{max} - I_{min})/6 \\ He = k \end{cases} \tag{8}$$

where Ex is the sample cloud expectation, En is the cloud entropy value, He is the cloud super-entropy, En_i' is the cloud entropy value of the index after the next iteration, and k reflects the randomness and linguistic fuzziness of each evaluation index and is a constant and should not be too large; here, k is 0.02.

4.3. Determination of Cloud Model Eigenvalues

Based on the principle of the forward cloud generator, the cloud eigenvalues Ex, En, and He corresponding to different security levels were calculated according to Equation (8), and the results are shown in Table 3. The cloud model diagrams corresponding to different

security levels can be calculated according to the calculation results in Table 3 and were drawn with Matlab software (see Figure 2).

Table 3. Cloud feature values for different security levels, including three characteristic values: *Ex*, *En*, and *He*.

Security Levels	*Ex*	*En*	*He*
excellent	9.5	0.167	0.02
superior	8.0	0.332	0.02
moderate	6.0	0.332	0.02
poor	4.0	0.332	0.02
awful	1.5	0.332	0.02

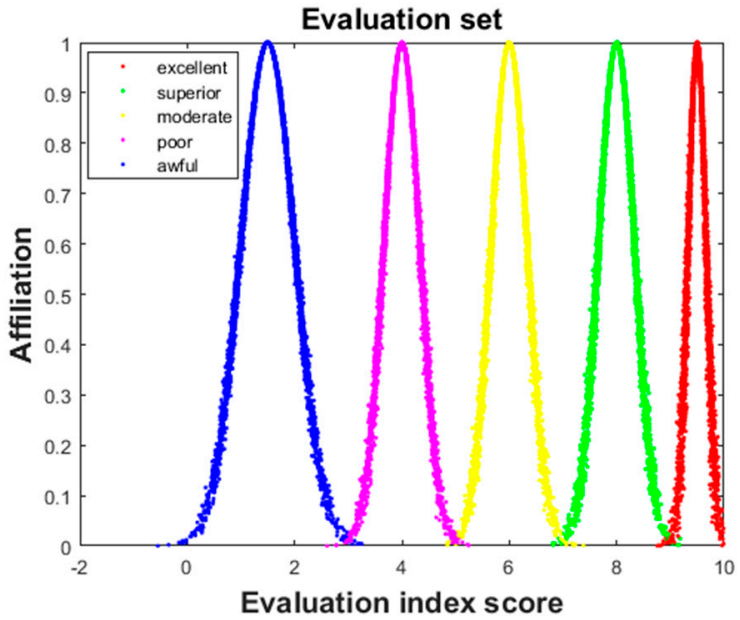

Figure 2. Cloud model with different security levels. Different color point sets represent different security levels: the red represents "excellent", the green represents "superior", the yellow represents "moderate", the purple represents "poor", and the blue represents "awful".

4.4. Security Evaluation Process

We analyzed the case of the PDIoT system of Meizhou Power Supply Bureau of Guangdong Power Grid. The safety evaluation of this PDIoT system was carried out according to the safety evaluation index system constructed in Figure 1, and experienced engineers of the company were invited to participate in the survey, including two deputy chief engineers and two engineers of the technical section of this power supply section, as well as one deputy chief engineer of each of the other two power supply sections and two engineers of each of the technical sections of the other two power supply sections, for a total of ten participants.

According to the actual situation, the evaluation indexes were scored with reference to the corresponding scoring rules. We considered that although the deputy chief engineer has the advantage in terms of knowledge level and work experience and has more authority, the engineers of the grassroots section have a deeper understanding of the site situation and can compensate for the relative lack of knowledge level and working experience to a certain extent. Therefore, the 10 scores were directly averaged to obtain the final average score. The average scores of each evaluation index are shown in Table 4.

Table 4. Average score of each indicator.

Index	Average Score	Index	Average Score
A_{11}	8.3	A_{24}	7.8
A_{12}	8.2	A_{25}	5.5
A_{13}	7.5	A_{31}	8.7
A_{14}	6.5	A_{32}	9.0
A_{15}	7.7	A_{33}	8.2
A_{21}	7.2	A_{34}	7.4
A_{22}	6.4	A_{35}	8.8
A_{23}	7.2	A_{36}	7.2

4.4.1. Determination of Integrated Cloud Parameters for PDIoT

Suppose that there are n identical types of language concepts, B_1, B_2,..., B_n, and $B_1 \in (Ex_1, En_1, He_1)$, $B_2 \in (Ex_2, En_2, He_2)$,..., $B_n \in (Ex_n, En_n, He_n)$, whose weights are v_1, v_2,... v_n in order; then, these n language concepts can form a composite cloud of the same type, and the eigenvalue, $B \in (Ex, En, He)$, of this composite cloud [23] can be calculated as:

$$\begin{cases} Ex = \sum_{i=1}^{n} Ex_i En_n v_i / \sum_{i=1}^{n} En_n v_i \\ En = \sum_{i=1}^{n} En_n v_i \\ He = \sum_{i=1}^{n} He_i En_n v_i / \sum_{i=1}^{n} En_n v_i \end{cases} \quad (9)$$

The resulting weights calculated by the entropy-weight method are shown in Table 4, and according to Equation (8), the eigenvalues of the integrated cloud of the evaluation system were calculated as $Ex = 8.257$, $En = 0.342$, and $He = 0.02$. The integrated cloud model was plotted using Matlab (see Figure 3) and compared with the cloud model images of each security level.

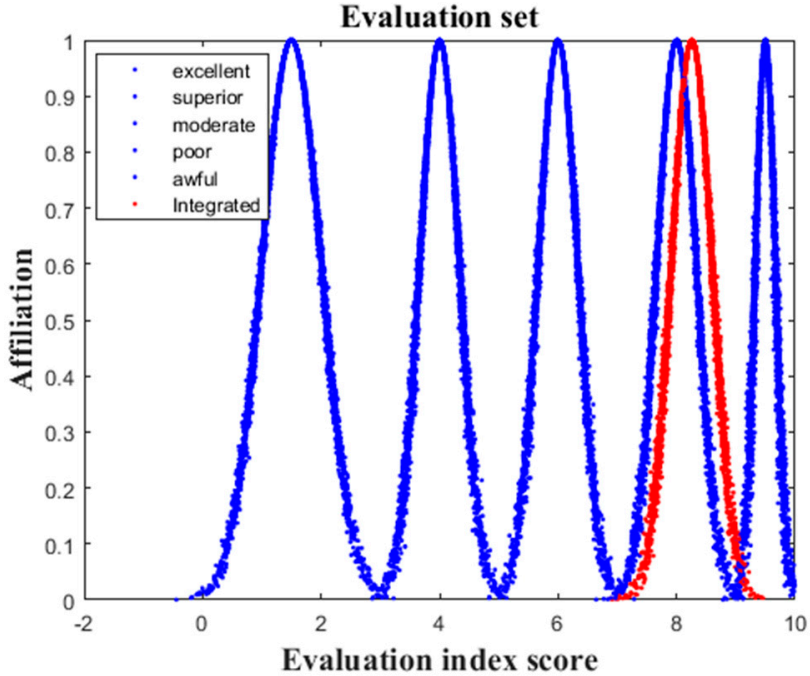

Figure 3. Integrated cloud model. The figure compares the generated integrated cloud model diagram with the standard cloud model diagram to judge the security level of the integrated cloud model. The red represents the integrated cloud model, and the blue represents the standard cloud model.

4.4.2. Determination of the Affiliation Degree of Each Level

According to the algorithm of the forward cloud generator, the affiliation degree of each evaluation index score belonging to a certain safety evaluation level was calculated by Equation (8). The process of determining the affiliation degree is illustrated by taking the case of the secondary indicator smart sensor A_{11} under the primary sensor factor A_1. From Equation (8), the affiliation degree of the index corresponding to the five security levels is $u_1 = 0$, $u_2 = 0.793$, $u_3 = 0$, $u_4 = 0$, and $u_5 = 0$. According to the principle of maximum affiliation, employee culture A_1 has the highest degree of affiliation for u_2, so the security level is "superior". Similarly, other indicators can be determined with the corresponding affiliation of their safety evaluation level.

According to the subordination degree of each evaluation index, the comprehensive subordination degree, *K*, can be calculated from Equation (10), and according to the maximum comprehensive subordination degree, the safety evaluation level of the power distribution Internet of Things system can be judged:

$$K = \sum_{i=0}^{n} u_i \omega_i \tag{10}$$

where ω_i denotes the weight of each evaluation index, and u_i is the affiliation degree of each evaluation index.

According to the characteristic parameters $Ex = 8.257$, $En = 0.342$, and $He = 0.02$ of the integrated cloud, the affiliation degrees, $u_1 = 0.083$, $u_2 = 0.405$, $u_3 = 0$, $u_4 = 0$, and $u_5 = 0$, of the integrated cloud could be obtained, and the integrated affiliation degrees were calculated as 0.083 and 0.405, respectively, according to Equation (8). It can be concluded that the evaluation level of PDIoT in this area was between "excellent" and "superior", with a preference for "superior". From Figure 3, we can see that the cloud droplets were dense, the evaluation results were stable, and the evaluation results were consistent with the actual situation of the region, indicating that the evaluation method proposed in this paper is effective and feasible.

4.4.3. Comparative Analysis

The method of this paper is compared with entropy fuzzy set theory, mainly comparing the differences of the evaluation methods, as shown below.

The entropy-weight fuzzy set theory evaluation method determined in [24] was used to evaluate the security of the PDIoT system. The calculated comprehensive risk value was 0.1413, which was substituted into the entropy-weight fuzzy set theory evaluation table, and the evaluation result was "superior", as shown in Table 5. The results obtained by this method are consistent with those in this work.

Table 5. Security risk level based on entropy-weight fuzzy set theory.

Security Levels	Risk Value
excellent	0~0.2
superior	0.2~0.4
moderate	0.4~0.6
poor	0.6~0.8
awful	0.8~1

Through the comparison of the two evaluation methods, it can be found that the evaluation results obtained by using the cloud model were more intuitive and persuasive. Since the result of the cloud model is $C = (Ex, En, He)$, it contains three values of the cloud model. Not only will the evaluation results (expected values) be displayed visually, but also the entropy (width) and super-entropy (thickness) of the cloud model, which makes it clear and persuasive.

4.4.4. Analysis of Evaluation Results

We can see from the integrated cloud model in Figure 3 that the evaluation result was between "excellent" and "superior", with a preference for "superior", and the comprehensive affiliation degrees calculated according to Equation (8) were 0.083 and 0.405. The scores of each index show that the scores of perception layer A_1 and application layer A_3 were generally high, which means that most of the index parameters of the PDIoT system were in good condition, the quality of the staff met the requirements, and the operating environment had slight adverse effects but did not cause danger. Therefore, there is overall a low probability of safety accidents. The scores of indicators under network layer A_2 were generally low, indicating that the security management of the PDIoT system network needs to be strengthened, and the results were consistent with the internal security inspection results of the PDIoT system. During the internal security inspection, it was found that the network firewall was weak and was subject to network attacks from time to time, and the communication network and business network were not sufficiently secure, which could also be reflected in this evaluation system.

In response to the above problems, we have developed the following measures. First, network security management should be strengthened, firewall protection should be enhanced, network supervision should be strengthened, and access rights to both the external and internal networks should be strictly managed. Secondly, the security management system should be continuously revised and improved, the implementation and effective implementation of the system should be guaranteed, and the supervision of the grassroots maintenance personnel should be strengthened to ensure the mastery of the maintenance site situation.

Therefore, by using the cloud model theory, the evaluation of the PDIoT system can be accurately and visually carried out, the security status of the PDIoT system can be grasped, and the weak links can be found in the operation and maintenance of the PDIoT system.

5. Conclusions

In this paper, we built a safety evaluation index system containing three first-level indicators and sixteen second-level indicators for the characteristics of PDIoT, combined with the actual site, relevant operation procedures, and management documents. Then, based on the entropy-weight method, we performed an objective evaluation of the evaluation index weight of the PDIoT, and used the entropy theory to objectively correct the evaluation differences of different experts. We introduced the cloud model into the security evaluation of PDIoT to solve the randomness and fuzziness between the security level of PDIoT and different indicators. To verify the feasibility of the method, we analyzed the case of the PDIoT system of Meizhou Power Supply Bureau of Guangdong Power Grid. The evaluation results showed that the characteristic parameters of the integrated cloud of the PDIoT system in this area were $Ex = 8.257$, $En = 0.342$, and $He = 0.02$, and the comprehensive membership degrees were $u_1 = 0.083$ and $u_2 = 0.405$, indicating that the security level in this area was in a "superior" security state, which is consistent with the actual situation of this area, which proved that the evaluation method proposed in this paper is effective and feasible. Then, we compared and analyzed the security evaluation method used in this paper with the entropy-weight fuzzy set method, and found that the evaluation results of the two methods were similar. However, the evaluation results of the cloud model were more intuitive and persuasive. Finally, according to the evaluation results, we put forward some reasonable suggestions for the PDIoT system in this area to reduce the possible security risks. In the future, the deep learning-based technique [25–27] will be examined to improve the performance of PDIoT.

Author Contributions: Conceptualization, W.W. and J.J.; data collection, S.C., J.J. and Z.Z.; data curation, S.C. and Z.Z.; funding acquisition, D.C.; investigation, J.J.; methodology, Y.Z.; project administration, Y.Z.; software, W.L.; supervision, D.C., Y.Z. and W.L.; validation, W.L.; visualization,

S.C.; writing—original draft, S.C.; writing—review and editing, S.C. and D.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No. 62171328) and by Education Sciences Planning of China (No. 2019GA090).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
PDIoT	power distribution Internet of Things
PDN	Power distribution network

References

1. Liu, H.; Zheng, C.; Li, D.; Shen, X.; Lin, K.; Wang, J.; Zhang, Z.; Zhang, Z.; Xiong, N.N. EDMF: Efficient Deep Matrix Factorization with Review Feature Learning for Industrial Recommender System. *IEEE Trans. Ind. Inf.* **2022**, *18*, 4361–4371. [CrossRef]
2. Liu, T.; Wang, J.; Yang, B.; Wang, X. NGDNet: Nonuniform Gaussian-label distribution learning for infrared head pose estimation and on-task behavior understanding in the classroom. *Neurocomputing* **2021**, *436*, 210–220. [CrossRef]
3. Liu, H.; Fang, S.; Zhang, Z.; Li, D.; Lin, K.; Wang, J. MFDNet: Collaborative Poses Perception and Matrix Fisher Distribution for Head Pose Estimation. *IEEE Trans. Multimed.* **2022**, *24*, 2449–2460. [CrossRef]
4. Kawamoto, D. IOT security incident analysis report. *China Inf. Secur.* **2017**, *71*.
5. Yusong, G.; Wenjie, Y.; Zongliang, H.; Zhen, Y. Safety risk assessment of urban power grid based on fuzzy comprehensive evaluation method. *Electr. Appl.* **2015**, *34*, 517–521.
6. He, C.; Du, X.; Yan Yi Chen, Y.; Sheng, G.; Jiang, X. Condition evaluation of power equipment based on data mining and principal component analysis. *High Volt. Electr.* **2017**, *53*, 34–41. [CrossRef]
7. Lu, J.; Nie, Y.; Wen, S.; Yang, Y. Evaluation method of electric energy metering device operation status based on hierarchical analysis method. *Electr. Meas. Instrum.* **2017**, *54*, 81–86.
8. Wu, J. *Systems Engineering*; Beijing Institute of Technology Press: Beijing, China, 2008.
9. Yu, G.K.; Yu, J.; Gao Guoliang Yu, C.P.; Xian, L.; Li, Y.Q. Research and application of FAHP model based on entropy power theory in the evaluation of urban distribution network construction. *Sichuan Electr. Power Technol.* **2021**, *44*, 29–34. [CrossRef]
10. Wang, H.; Feng, C. Safety evaluation of high-speed railway contact network system based on structural entropy power method and cloud model. *China Railw.* **2019**, *12*, 41–46. [CrossRef]
11. Zhao, Y.; Zhang, Y.; Zhang, X.; Li, H.; Chen, D.; Xie, D. Research on evaluation index system of the operation efficiency in electricity market. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *766*, 012047. [CrossRef]
12. Li, J.; Shang, Z.; Qiang, R.; Pang, J.; Guo, H.; Wang, J.; Niu, H. Energy Internet Security Risk Evaluation Index System. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *645*, 012045. [CrossRef]
13. Gui, C. Research on the security architecture of Internet of Things. *Wirel. Interconnect. Technol.* **2019**, *16*, 107–108.
14. Sheng, J.; Chen, T.; Jin, W.; Zhou, Y. Selection of Cost Allocation Methods for Power Grid Enterprises Based on Entropy Weight Method. *J. Phys. Conf. Ser.* **2021**, *1881*, 022063. [CrossRef]
15. Wang, Y.; Yaling, J.; Yang, J.; Tang, Y.; Zhou, P.; Chen, C. Research on Power Grid Infrastructure Investment Distribution Model Based on Entropy Weight Method. *E3S Web Conf.* **2021**, *253*, 03049. [CrossRef]
16. Xiang, S.; Hongkeng, Y.; Chen, D. Data mining analysis method of voltage transient events based on gray target theory and cloud model. *Power Grid Technol.* **2019**, *43*, 722–731. [CrossRef]
17. Pang, Y.; Liu, S. MIMO radar sparse array optimization based on improved artificial bee colony algorithm. *Syst. Eng. Electron. Technol.* **2018**, *40*, 1026–1030.
18. Gao, D.; Yu, X.; Du, H. Research on the assessment of civil airport fire commanders' decision making ability based on cloud model. *China Sci. Technol. Saf. Prod.* **2018**, *14*, 57–62.
19. Sun, Y.; Xie, J.; Su, K.; Li, Y. Decision evaluation model for military-civilian integration of military information system projects. *Syst. Eng. Theory Pract.* **2018**, *38*, 2713–2720.
20. Zhao, J.; Tian, J.; Meng, F.; Zhang, M.; Wu, Q. Safety assessment method for storage tank farm based on the combination of structure entropy weight method and cloud model. *J. Loss Prev. Process Ind.* **2022**, *75*, 104709. [CrossRef]
21. Song, W.; Zhu, J. A goal-reference-point decision-making method based on normal cloud model and its application in distribution network planning evaluation. *Inf. Sci.* **2021**, *577*, 883–898. [CrossRef]

22. Wei, F.; Xu, Q.; Xie, N.; Gong, Z. weighting power quality evaluation based on cloud model and anti-entropy. *J. Phys. Conf. Ser.* **2021**, *2005*, 012158. [CrossRef]
23. Yi, L.; Guo, Y.; Liu, N.; Liu, J.; Zhao, J.; Jiang, G. Health Status Sensing of Catenary Based on Combination Weighting and Normal Cloud Model. *Arab. J. Sci. Eng.* **2021**, *47*, 2835–2849. [CrossRef]
24. Yuan, J.; Li, C. Power grid information security risk assessment based on entropy weight fuzzy set theory. *J. Tianjin Norm. Univ. Nat. Sci. Ed.* **2014**, *34*, 93–96.
25. Liu, H.; Zheng, C.; Li, D.; Zhang, Z.; Lin, K.; Shen, X.; Xiong, N.N.; Wang, J. Multi-perspective social recommendation method with graph representation learning. *Neurocomputing* **2022**, *468*, 469–481. [CrossRef]
26. Liu, H.; Nie, H.; Zhang, Z.; Li, Y.-F. Anisotropic angle distribution learning for head pose estimation and attention understanding in human-computer interaction. *Neurocomputing* **2021**, *433*, 310–322. [CrossRef]
27. Liu, H.; Liu, T.; Zhang, Z.; Sangaiah, A.K.; Yang, B.; Li, Y.F. ARHPE: Asymmetric Relation-aware Representation Learning for Head Pose Estimation in Industrial Human-machine Interaction. *IEEE Trans. Ind. Inform.* **2022**, 1. [CrossRef]