Application of Cloud Security Terminal in Information Management of Power Industry

Jiang Jiang[1(✉)], Hanyang Xie[2], Yuqing Li[3], and Jinman Luo[4]

[1] Digital Department of Guangdong Power Grid Corporation, Guangzhou 510800, China
ljhh201@163.com
[2] Information Center of Guangdong Power Grid Corporation, Guangzhou 510000, China
[3] Logistics Service Center of Dongguan Power Supply Bureau of Guangdong Power Grid Corporation, Dongguan 523900, China
[4] Information Center of Dongguan Power Supply Bureau of Guangdong Power Grid Corporation, Dongguan 523900, China

Abstract. With the powerful computing power of cloud computing, cloud security terminals are widely used in many industries. The information construction of the power industry will generate a large amount of data. In order to improve the efficiency of information management in the power industry and reduce the success rate of information cracking, this paper applies the cloud security terminal to the power information management. After deploying the power industry information management cloud security terminal architecture, build a terminal access control model. Cloud node load is predicted through Bayesian model to ensure smooth power information management. The improved Wu-Manber algorithm is used to protect the power information layer and ensure the safety of power circuit information. In the example verification, after the cloud security terminal is applied, the success rate of information being cracked is less than 10%, the response speed of this method is significantly improved, and the level of power information management is improved.

Keywords: Cloud security terminal · Power industry · Information management · Application research · Access control · Bayesian

1 Introduction

The electric power industry is a technology- intensive and asset-intensive basic industry of the national economy. The informationization of the industry started early, but its complexity and difficulty are greater than those of modern service industry and manufacturing industry. The development and maturity of network, computer and communication technologies have basically eliminated the technical bottleneck in the process of enterprise informatization, especially the informatization application technologies. While surrounding the development of Web technologies, the informatization technologies, the optimization, upgrading and integration of equipment have reached a considerable

W. Fu and L. Yun (Eds.): ADHIP 2022, LNICST 468, pp. 771–783, 2023.
https://doi.org/10.1007/978-3-031-28787-9_57

level, the mainstream products and technologies have basically taken shape, and the technical risks for enterprises to implement informatization have been effectively reduced. The construction of information engineering projects in the power industry covers a wide range, including the digital construction of substations, the construction of power transmission and distribution networks, the construction of communication networks, and the construction of more information systems supporting the daily maintenance and management work [1]. At present, the electric power industry has basically realized the informationization management, and has promoted the electric power industry informationization construction ability. The construction of informatization project is a very complicated system project, which has the characteristics of high technical content, fuzzy task boundary, imprecise objectives, strong pertinence, frequent change of business requirements and tight schedule [2]. Because of the lag of the understanding of management personnel and the construction of management mechanism, the management level of informationization construction project is far from the same proficiency as traditional management project. Therefore, to improve the ability of organization informatization project management and make use of informatization project construction to ensure the realization of informatization strategic goal have become the most important and frontier subject.

Cloud security terminal comes into being under the era background of cloud computing and big data, and has advantages in many aspects. People can use Cloud security terminal system to integrate information resources, and also can realize the real improvement of information management level, truly keep up with the trend of development of the times, and not be eliminated by the market. Especially, the contradiction between terminal system and information security will be aggravated when the scale of enterprise is enlarged. Therefore, the managers of enterprise should realize the seriousness of the problem and take some effective measures to avoid the information leakage, which will be beneficial to the electric power industry of our country moving towards the direction of intelligence.

Some scholars have proposed a method of hierarchical management of power information, taking into account factors such as distributed power sources, distribution lines, and equipment controllable levels, to solve the problem of efficient and intelligent management of diverse load equipment under its jurisdiction in the park. The park managers realize the overall collaborative management of the diverse loads to achieve the purpose of improving energy efficiency. However, this method needs to be further improved in the balance of information load. Some scholars have proposed an information management method based on edge computing. This method introduces edge computing as a data processing model, disperses the computing load pressure of the data processing center to the edge side of the device, thereby improving the data response speed, and can still process local data in an offline state. However, there is room for further improvement in data loss prevention. In order to enhance the capability of data disaster tolerance and prevention, strengthen data sharing and business integration, enhance the business support capacity, and ensure the operation security of the power industry, the information management method based on cloud security terminals in the power industry will be studied to explore the practical application of cloud security. This paper deploys the electric power industry information management cloud security terminal architecture,

and constructs the terminal access control model. The Bayesian model predicts the cloud node load passing to ensure the smooth power information management. The improved Wu-Manber algorithm is used to protect the power information layer and manage the university of power information.

2 Application Research of Cloud Security Terminal in Information Management of Power Industry

2.1 Deployment of Cloud Security Terminal Architecture for Information Management in Power Industry

By integrating resources and assigning to different users according to their needs, cloud terminals maximize the utilization of scheduling management resources, and can uniformly carry out the standardized configuration of software, realize the application system online, version update, unified repair of bugs, active and passive offline server maintenance and other processes, as well as flexible expansion and easy management. Using cloud security terminals can realize unified management and scheduling of office resources, actively control illegal outreach channels, uniformly carry out computer registration and installation of anti-virus software, and eliminate file leaks, software vulnerabilities and hacker attacks. In complex network environments, software deployment platforms usually run in independent trust domains. In this open environment, trust assessment and evidence collection between entities are carried out between untrusted entities. Especially the trusted evidence collection and software credibility assessment in software runtime [3].

The cloud security terminal adopts the virtualization architecture as the bottom design, provides a highly scalable, reliable and stable resource platform for the basic server layer of the cloud terminal system, has built-in business continuity and disaster recovery functions, can protect desktop data and its availability, and provides a powerful backstage guarantee for desktop virtualization. The logical structure of the cloud security terminal is shown in Fig. 1. From bottom to top, the logical structure is: hardware resource layer, third-party cloud monitoring management control layer, virtualization and cloud platform layer, regional central node and terminal access layer. The hardware resource layer integrates and pools existing resources, divides them according to the needs of users, and stores all processing data in fixed data storage devices to improve data security; the third party cloud monitoring management control layer comprises five parts, namely, user access to information parsing interface, parser, filtering and aggregation engine, configuration management module and monitoring rule base [4]. Virtualization and cloud platform layer realizes the redirection of peripherals by adopting Xen virtualization technology and SPICE Desktop Transfer Protocol; Domain center node layer is the core layer of monitoring execution, responsible for subscribing and publishing data. It mainly includes command interface, control components SubAgent _ Manager, TopicAgent _ Manager and PubAgent _ Manager, monitoring agent components SubAgent, TopicAgent and PubAgent. Terminal access layer uses the smaller client to access, and only configures the interface including embedded processor, local flash memory and various peripherals. In the process of transmission, it provides a more secure environment by only transmitting high-strength encryption transform values of terminal signals

and images. Different types of monitoring agents can be deployed, including application monitoring agents that monitor application information, virtual machine monitoring agents that monitor the running information of VMs, and physical infrastructure agents that monitor the running information of the infrastructure.

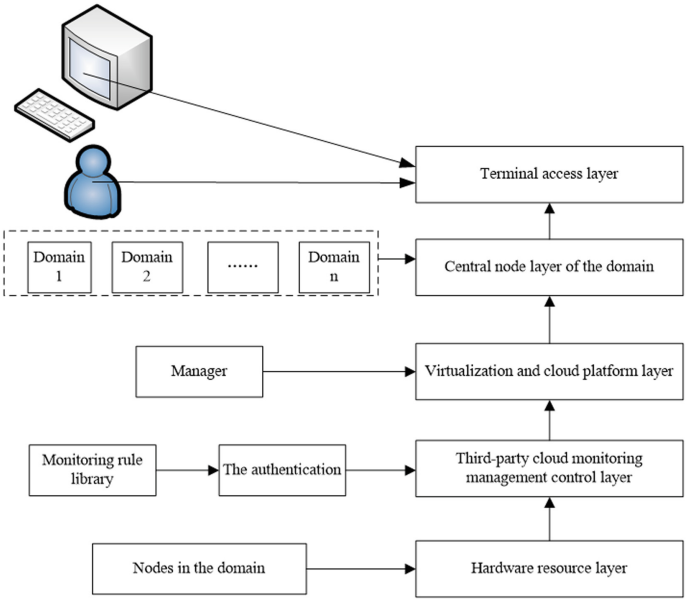

Fig. 1. Cloud security terminal deployment architecture

Under the cloud security terminal deployment architecture, the process of obtaining data related to the information management of the power industry is as follows:

Step 1: The user submits service request information and performs identity authentication;

Step 2: The user access information parsing interface receives the access request from the user, and parses the access request information into a triple, (user ID, cloud service type), monitoring category, monitoring content);

Step 3: The parser receives monitoring information from the cloud user and is responsible for parsing the monitoring information triple (user ID, cloud service type, monitoring category, monitoring content) into domain, topic, content);

Step 4: The configuration management module receives parsing information from the parser, accesses the monitoring rule base, and configures the monitoring file according to the monitoring content;

Step 5: The domain adptor command interface receives the parsed monitoring configuration file from the monitoring configuration management module and, based on the match result of the domain information, determines whether the domain needs to be monitored by the user. If the match succeeds, execute. Otherwise, the domain does not perform monitoring requests.

Step 6: TopicAgent _ Manager enables related TopicAgent; SubAgent _ Manager enables SubAgent; PubAgent _ Manager enables PubAgent based on the topic information of the monitoring configuration file.

Step 7: SubAgent sends a subscription request to the TopicAgent based on the monitoring profile topic information;

Step 8: Agent writes monitoring data to PubAgent in the domain according to data type and organization form;

Step 9: PubAgent publishes data to the TopicAgent by topic number;

Step 10: SubAgent extracts subscription data from the TopicAgent based on topic;

Step 11: SubAgent delivers monitoring data to the filtering and aggregation engines.

Step 12: Filtering and aggregation engines filter and reduce data streams to minimize the additional overhead associated with monitoring data streams;

Step 13: Generates a specific monitor view to the user and displays a warning message based on the refresh of the monitor.

For systems with higher security requirements, it is difficult to meet the requirements only by using autonomous access control mechanism. DPS-CMS can increase or decrease the number of agents flexibly according to the scale of monitoring facilities, thus effectively reduce the storage and computing pressure of monitoring nodes, and is more suitable for cloud computing system composed of large-scale virtual organizations than centralized agent deployment. DPS-CMS adopts P/S communication model, takes data as center, network delay is small, real-time is strong; four-layer agent mode, each layer has corresponding data preprocessing method, which reduces the amount of data transmission and improves the ability of data transmission. From this point of view, DPS-CMS can meet the adaptive requirements of cloud monitoring. DPS-CMS can be implemented by adding or enabling a corresponding PubAgent if there is a new monitoring entity that needs to be monitored, in this sense DPS-CMS meets the elastic requirements of cloud monitoring. The DPS-CMS publish-subscribe app is modular, and PubAgent and SubAgent can join or leave dynamically to meet flexible application requirements [5].

When the amount of tasks processed by the user cloud node increases significantly, the load of the node will also increase accordingly. The user needs to pre-allocate more resources in time to meet the needs of task processing and prevent the excessive load from affecting the normal use of the service.. On the contrary, in order to save expenses, users can reduce some resources without affecting the normal provision of services, so as to prevent the waste of idle resources caused by excessively low load. If we can predict the change of node load in advance and grasp the trend of load change, it will have important guiding significance for the timely allocation and recovery of node resources. This approach can improve the optimization of node service performance and utilization.

2.2 Cloud Security Terminal Access Control Model

The distributed nature of cloud computing means that storage or computing in the cloud may involve resources in different autonomous domains, requiring multiple entities in different domains to coordinate with each other to complete the entire operation. Resource sharing is becoming more and more important, and the security issue of cross-domain resource access that accompanies cross-domain access cannot be ignored. From

the point of view of practical security issues, users upload their important data to the cloud, and it is necessary to consider the ability of cloud computing to ensure data security and integrity in the process of cloud services, and it is also necessary to establish trust in cloud service providers. In the cloud computing environment, each cloud application belongs to different security management domains, each security domain manages local resources and users, and different domains correspond to different security management policies and rules. When users access resources across domains, each domain has its own access control strategy. When sharing and protecting resources, a common and mutually agreed access control strategy must be formulated for the shared resources [6].

First, the X domain Y and the domain start preparations at the same time, and the domain X defines the risk function $\Gamma\left(x_i, x_j, r\right) \in [0, 1]$ of this domain. And calculate the initial risk value Γ_i of the nodes in the domain, the larger the risk value, the higher the risk. Where m is the total number of nodes in domain X. At the same time, the initial value of the risk cursor R^X is set subjectively by the domain management node. In addition to the two initial work of the above-mentioned domain, the preparation work of domain Y also includes defining the shared function related to it. The risk cursor set by the domain Y is R_i^X. In this example, i takes Y, which represents the risk threshold value in the domain Y for the visit from the Y domain.

Then, the user u of the domain Y initiates an access request r. At this time, the management node of domain Y compares the risk value Γ_i of this visit with the risk cursor R^X of domain Y. And compare the counter value c with the set maximum access times F_i. The decision of the management node of domain Y for this visit is defined as follows [7].

$$D(r)^X = \begin{cases} A, \Gamma_i(r) < R_i^X \wedge (c < F_i) \\ D, else \end{cases} \tag{1}$$

If the result is A, go to the next step; otherwise, the access request of u is rejected, and the process is terminated. After that, domain Y will calculate user u's mapping role set $f_Y(X)$ in domain Y according to u's request r and sharing function $S(Y)(X)$. And calculate the risk value of this access, compare the risk value and the size of the risk cursor, and decide whether to allow this access request. If access is allowed, continue to step 5. If access is denied, the cross-domain access process is terminated. The detailed process is shown in Fig. 2.

If access is allowed. Domain Y verifies the identity of user u. If the verification passes, assign the mapping role set $Y(X)$ to u. And allow it to access resources in domain Y with this role.

Based on the role-based access control model, the concept of "trust" is introduced, which is the so-called trust-based access control technology. That is, on the basis of granting permissions to roles, the user's trust degree must be verified. Only when the user's identity verification and trust degree both meet the requirements set by the system, can the user access rights be assigned. The cloud computing environment has potential vulnerabilities in the application layer and the basic service layer. The vulnerability identification refers to the correlation analysis, which may be attacked and exploited. The weak point of the system is an important link in the security situation assessment of static indicators. Organizational and logical errors in software, inconsistency in coordination

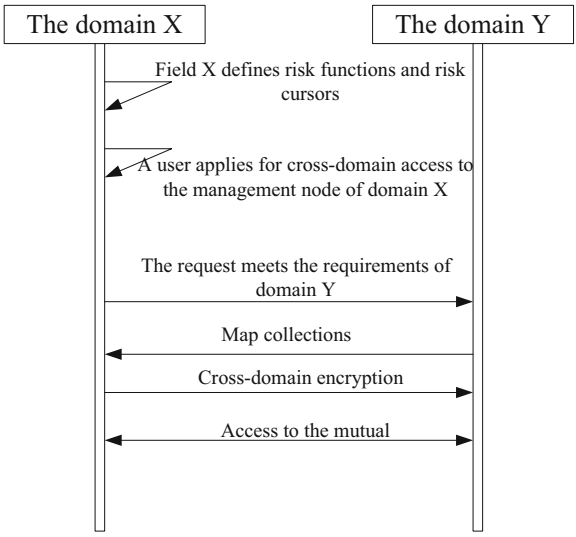

Fig. 2. Cloud security terminal cross-domain access

between different devices and other factors inevitably lead to security policy defects, identify weaknesses that may be exploited by threats, identify technical vulnerabilities and identify objects, such as physical environmental factors, internal and external network structure Access policy, apply the security protocol type in the middleware, and then perform qualitative or quantitative assignment.

Initialization of trust relationship between nodes The establishment of trust relationship between nodes needs to go through two stages: service discovery stage and trust evaluation stage, monitoring the impact of all interactions between nodes on the cloud security management system, evaluation, update and decision-making of trust values. The justification is largely dependent on the observer. The main task to observe is how the trust context changes when the nodes interact, and another task is to store, manage and trigger the dynamic update of the trust value. When the observation system observes that the behavior of a node exceeds the "allowed" range, that is, it determines that the behavior of this node is an aggressive behavior. At this time, it is necessary to trigger the re-evaluation of the relevant trust degree. During cross-domain access, there are generally two access policies for cloud security terminals: Boolean function or LSSS matrix. Boolean functions can be represented by an access structure tree, the attributes are leaf nodes, and "and" and "or" represent other nodes except leaf nodes. In general, the form of the access policy is represented by a matrix, so we need to convert the form represented by the Boolean function to the LSSS matrix representation. The algorithm is roughly as follows: Assume that the root node is the vector l, and the child node is the vector of the parent node. If node i is "AND", then its left and right child nodes are $(v_i|l)$ and $(0, -1)$, respectively. if node i is "OR". Then its left child node and right child node are consistent with their own vectors.

In the attribute encryption algorithm, it is necessary to judge whether the user attribute set that sends the request to the cloud security terminal matches the access policy tree of

the file. The general judgment method is: set the root node of the access policy tree T as G. T' is a subtree of T, and its root node is g. 5If a set ξ satisfies the access policy tree T' that is $T'(g) = 1$. And the node is a leaf node, then if and only if $\xi(g) \in G$. If this node is a non-leaf node, the value of $T'(g)$ of all child nodes of g needs to be calculated. $T'(g) = 1$ can only be established when the number of nodes whose $T'(g)$ value is 1 is more than k.

When using the attribute encryption access control system to protect the security of the data stored in the cloud security terminal, the key ciphertext encrypted by the CP-ABE algorithm is stored in the cloud together with the data ciphertext, which can reduce the key management of the system To a large extent, it can improve the efficiency of key distribution and the flexibility of users to access data. When attacks from outside the cloud continue to intensify, in addition to causing damage to public cloud tenant applications, for example, customers cannot log in to access. In addition, the attacker's ability will gradually increase the malicious behavior with the gradual accumulation of attack resources. The attack ability threat value *TH* is a measure of the threat to cloud security caused by the attack ability possessed by malicious attacks at a certain time. Affected by the degree of control over the target tenant, the sensitive data obtained by the attack. The level of attack capability assessment is attack capability threat value → component threat value → security data threat value → threat interval.

$$TH = \sum_{i=0}^{n} th_{next}[i]w[i] \tag{2}$$

Malicious attacks transform read permissions into remote login permissions by acquiring permissions layer by layer. Therefore, by setting the access control of the cloud security terminal, the operation security of the cloud security terminal can be guaranteed.

2.3 Cloud Security Endpoint Access Load Prediction

When the cloud security terminal protects the information management of the power industry, the difference in the volume of information and data exchange will cause the overload of the security node. Therefore, this paper will predict the load of cloud security terminal nodes to ensure the smoothness of power information management.

Due to the high correlation between cloud node loads, it is usually manifested as adjacent short time gaps. A series of load situations with time intervals of different lengths are then predicted. Each time interval starts from t_0, and the average load of each time period is recorded as $L_1, L_2, \ldots, L_n$. Assuming that the current moment is t_0, two load averages have now been predicted. L_i and L_{i-1} correspond to two different time intervals $[t_0, t_i]$ and $\left[t_0, t_{i-1}\right]$, respectively. The load value $\overline{L}_i$ corresponding to the $\left[t_{i-1}, t_i\right]$ time can be calculated according to the following formula.

$$\overline{L}_i = L_i + \frac{t_{i-1} - t_0}{t_i - t_{i-1}}(L_i - L_{i-1}) \tag{3}$$

Applying Bayesian theory to load prediction of cloud security endpoints should be implemented in the following six steps:

1) Determine the load state vector of the cloud security node, that is, the vector $Z = \{z_1, z_2, \ldots, z_m\}^T$ of the class. Where m is the number of states associated with the security endpoint.
2) An attribute vector that determines the cloud node's load, $AT = \{at_1, at_2, \cdots, at_n\}^T$, where n is the number of attributes.
3) Calculate the prior probability $P_B(Z_i)$ of each state using the sample data set (historical data).
4) Calculate the joint probability $P(at_i|Z_i)$ for each state separately.
5) The posterior probability is calculated based on the historical data and the following formula.

$$P(Z_i|at_i) = \frac{P(at_i|Z_i)P(Z_i)}{\sum_m P(at_i|Z_k)P(Z_k)} \tag{4}$$

6) The predicted value of the state is selected according to the following formula

$$\overline{L}_i = E(Z_i|at_i) = \sum_{i=1}^{m} Z_i P(Z_i|at_i) \tag{5}$$

If the predicted node load of the cloud security terminal meets the node migration condition, the running task will be migrated to other nodes. The node migration condition includes two restrictions, namely the upper limit trigger condition and the lower limit trigger condition. The main function of the upper limit trigger condition is to reduce the load of nodes running under high load. If the cloud security terminal node used by the user is often under high load, in order to ensure the quality of service, the user can select a suitable cloud node on the running node that meets the upper limit trigger condition and migrate it to other running nodes. This ensures that the computing power running on this node meets the needs of users.

2.4 Power Information Level Protection of Cloud Security Terminal

When using the cloud security terminal for power information transmission, in order to ensure the information security of the power industry, it is necessary to carry out transmission authentication according to the dynamic protocol. The dynamic protocol structure in this study is used to describe the dynamic behavior of a certain moment or a certain state, focusing on the description of the control logic, examining the state and connection between objects in the protocol at any moment. In UML, sequence diagrams and activity diagrams are used to represent the dynamic structure model of the protocol: the sequence diagram depicts the interaction model of the protocol and describes the interaction of some elements of the protocol in time. The sequence diagram is oriented to the process of protocol execution; the activity diagram describes the The state model of the protocol, the dynamic behavior of a class, can also describe concurrent activities, and the activity diagram is oriented to specific objects. In this section, the dynamic structure model of the protocol is described, mainly from the initialization of the protocol and the execution phase of the protocol.

The initialization of the protocol is initiated by the back-end server, the back-end server completes all initialization work, and the information receiving end passively accepts the identification and writes it into the memory unit. At the beginning of the protocol execution, the message sender initiates a session and transmits the message to the server. The server receives the information, performs corresponding calculations, and feeds back a message to the information receiver. The receiving end receives the message, and performs preliminary verification on the identity of the receiving end through calculation and comparison. The back-end server receives the message and calculates it, searches the database to determine whether there is a calculated value, and continues to calculate and transmits the message to the access controller if it exists. The access controller receives the message for calculation, and transmits the message to the authentication server. The authentication server receives the message for verification. If it passes, the authentication is realized. If it fails, the authentication fails.

This study uses the improved Wu-Manber algorithm to protect different information levels in the power industry. The Wu-Manber algorithm uses three tables, SHIFT, HASH, and PREFIX, to store the information that the algorithm needs to run. The lookup of the two tables, SHIFT and HASH, is realized by hashing the suffix of the pattern string, and there are certain repetitions. For example, in the preprocessing stage, each pattern string suffix will calculate the hash twice, once to initialize the SHIFT table and once to initialize the HASH table. In the matching process, the algorithm calculates the hash value h according to the last B characters of the current window according to the HASH function. First use h to find the SHIFT table to determine whether the window slides backwards. If SHIFT[h] $= 0$, then use h to look up the HASH table. In this way, the same hash value h is searched twice. If SHIFT $= 0$, then look up the HASH table by hash calculation to get all possible keywords that match the suffix of the current matching window. Then look up the PREFIX table to determine whether the prefixes of these keywords match. This process involves the lookup operation of two tables, and the efficiency is relatively low. Merge the SHIFT and PREFIX tables into the HASH table, and modify the data structure of the HASH linked list. Add a data field to store the shift value in the main table node. The prefix data field used to store the prefix hash value of the pattern string is added to the child linked list node. It can be seen that only the main entry with the shift value of 0 has a sub-linked list, and the sub-linked list pointer fields of the main entry with the shift value of not 0 are all NULL. The maximum shift value in the algorithm is $m - 1$, which is generally not very large in practical situations. When the cloud security terminal creates the HASH table, the memory space of the sub-linked list is dynamically applied. The process of the improved algorithm to protect the power information level is as follows:

1) According to the last B characters of the current window, the hash value h is calculated according to the HASH function.
2) Check the main table of the HASH table to determine the size of the data field value d. If $d < m$, the data field value represents the shift value, slide the window data positions to the right, and return to step (1). If it is $d \geq m$, the value of the data field represents the address of the head node of the sub-chain list, and the step (3) is entered.
3) Calculate the current window prefix hash value text prefix.

4) Find all the pattern strings with the suffix hash value *h* according to the HASH table, and compare text_prefLx with the prefix hash value prefix of these pattern string nodes one by one in the order of the pattern strings in the HASH table sub-linked list. If the two are not equal, go to the next pattern string. If the two are equal, complete comparison is performed until it is judged whether the match is successful.
5) Slide the current window back one character, turn step (1).

According to the above process, the research on the information management method of the power industry based on the cloud security terminal is completed. In order to clarify the application of cloud security terminal in the actual information management of the power industry, the next section will carry out example verification.

3 Example Verification

3.1 Validate the Design

This experiment will verify the information management method of the power industry based on the cloud security terminal studied above from the two aspects of the security and efficiency of the management method. In order to make the verification results of the example more authentic and reliable, in this verification, the information management method based on hierarchy and the information management method based on edge computing are used as comparison groups. This verification is completed by comparing the success rate of the power industry information being deciphered and the response time of the method under the application of the method.

3.2 Validation Results

The following Table 1 is for the verification of this example, when different management methods are applied to the information management of the power industry. The comparison of the success rate of power information transmission and the response time of the method to the attack.

Analysis of the data in Table 1 shows that when the management method proposed in this paper is used in the information management of the power industry, the probability of information being successfully deciphered is less than 10%, which is better than other management methods. From the perspective of the response time of the method, after using the method in this paper, it can respond quickly to attacks on power information transmission, reduce the risk of data damage and loss, and effectively manage power information. That is to say, the application of cloud security terminal in the information management of the power industry can fully protect the security of power information data and ensure the normal operation of the power industry.

Table 1. Instance validation data

Group	Management method based on cloud security terminal		Hierarchical Information Management Method		Information management method based on edge computing	
	Cracked success rate/%	Response time/ms	Cracked success rate/%	Response time/ms	Cracked success rate/%	Response time/ms
1	6.3	4.03	22.9	7.96	15.9	5.80
2	7.7	3.76	21.5	7.84	13.2	5.86
3	8.8	3.53	22.4	7.37	16.8	6.55
4	9.2	3.54	19.3	7.90	13.1	6.17
5	6.5	3.76	21.1	7.21	16.5	6.46
6	7.4	3.95	18.0	6.92	16.6	6.43
7	9.3	3.80	19.2	8.15	15.4	6.22
8	9.6	3.87	17.6	7.73	14.2	6.84
9	8.1	3.93	22.7	7.64	13.3	6.63
10	6.5	4.09	20.8	7.06	15.7	6.25

4 Conclusion

With the deepening of electricity market reform, electricity informatization has developed by leaps and bounds. In recent years, the level of informatization in the electric power industry has been getting higher and higher, all of which are inseparable from the support of information technology, and the corresponding requirements for the security of information systems have also increased. The cloud security terminal is an innovative office system based on cloud computing technology, which can realize the push of the desktop system on the remote server to the terminal and the redirection of the terminal and terminal peripherals to the desktop system on the remote server. It will release applications including computing resources, storage resources, and management services to end users through a variety of terminal types. At the same time, the storage and management of data is centralized in the cloud, and the client does not participate in any calculation and application. It is efficient and green, and can effectively solve problems such as office terminal operation and maintenance and security management. With the help of the good characteristics of cloud security terminal, this paper explores the application of cloud security terminal in the information management of power industry. It has been verified by examples that the use of cloud security terminals can effectively deal with the security protection problems in the information management of the power industry. Due to the limited time, this paper still needs to improve in the resource-domain interaction and resource scheduling. The extensive and in-depth study of these problems will undoubtedly have a profound impact on the development of intelligent cloud computing technology.

References

1. Wang, H., Liu, G.: Security audit strategy of e-government cloud in big data age. Audit Econ. Res. **36**(04), 1–9 (2021)
2. Gan, Y., Chen, X.: Trusted client identity authentication simulation for power security control process. Comput. Simul. **38**(08), 181–184+189 (2021)
3. Wang, J.: Implementation of cloud security terminal in power information management. Appl. IC **38**(10), 118–119 (2021)
4. Yang, Q.: Research and construction of data quality management application in electric power enterprises based on HAWQ. Process Autom. Instr. **41**(12), 67–71 (2020)
5. Guan, G., Song, Q., Liu, H., et al.: Research on distribution network management and operation and maintenance system based on edge computing. Adv. Power Syst. Hydroelectr. Eng. **36**(10), 90–96 (2020)
6. Yang, R.: Research on regional big data analysis method based on cloud security and deep learning. Electron. Design Eng. **29**(10), 15–18+23 (2021)
7. Zhao, G., Chao, M., Xie, B., et al.: Application of deep belief network in cloud security situation prediction. J. Chin. Comput. Syst. **41**(06), 1195–1202 (2020)