Journal of Computers Vol. 31 No. 1, 2020, pp. 192-198
doi:10.3966/199115992020023101016

A Situation Awareness System for the Information Security of Power Grid

Ming Xie*, Zhubin Chen

Science and Information Department, Guangxi Company of Southern Power Grid, Nanning,
Guangxi 530023, China
xie_m@gx.csg.cn

Received 13 January 2019; Revised 12 March 2019; Accepted 12 March 2019

Abstract. With the development of intelligent power grid and the application of artificial intelligence, cloud computing and other technologies in the field of information security, the information security of the power grid will be faced with more security challenges. The research of security perception in environmental system startup detection, data encryption and management will be an important issue that information security must face. This paper proposes a Power Grid Information Security Perceptual System on the basis of Artificial Intelligence technology. Thus, Virus Pre detection is implemented before BIOS and operation system start. Combined with the encryption and decryption calculation method of multiple dynamic security, the credible risk assessment theory of dynamic cycle is established by independent recognition and learning model. It solves the problem of passive defense of information security of power grid, strengthens the control and situational awareness of power data risk, and enhances the reliability and credibility of information security system of power grid.

Keywords: secure cloud computing, security management, virus defense

1 Introduction

With rapid development of energy transformation and “Internet +”, artificial intelligence and big data are playing increasingly important roles in the construction of management mode and value function. The research and application of large power data are being paid more and more attention.

However, the growing scale of multi-source heterogeneous data and the requirement of real-time processing, the complexity of data processing is getting higher and higher, which brings new technical challenge to the management of traditional security transmission [1]. Cloud computing, with the idea of “network is computer”, provides convenient, economical and highly scalable IT services for remote computer users. As an integral part of cloud computing platform [2], PaaS can integrate various business capabilities, gather a large number of different services in the network through application software to work together and provide data storage and business access capabilities externally [3]. PaaS can provide users with application infrastructure services in the cloud environment [4]. The traditional cloud-based data transmission method is to transfer the big data from a cloud storage point to a destination storage point according to the path sequence of cloud storage [5]. The advantage of this method is that it can get rid of the limitation of hardware resources [6]. However, in the case of a large amount of data backup or recovery that needs to be centralized, cloud processing capacity will be greatly stressed due to the need to store hundreds of TB data. Once the storage capacity of cloud space is limited [2], data overflow will occur, which is easy to cause the security risks of external attack [3].

A large number of detection methods and defense methods are proposed in the existing technology [4]. The monitoring of BIOS start-up phase and operating system start-up phase is not perfect, especially for the existing concealed malicious attack technology has not been put forward a good solution. In order to solve the existing problems [5], this paper proposes a big data security management method and system.

[*] Corresponding Author

Virus detection is carried out before the system starts to realize the goal of virus-free quick startup of terminal equipment, improve the security of the terminal device startup, and construct a non-toxic operating environment [7].

The client cluster is built through multiple user nodes to save the copies of the file stored in the server, which not only ensures the security of data transmission, but also alleviates the load on the server.

2 Structural Design

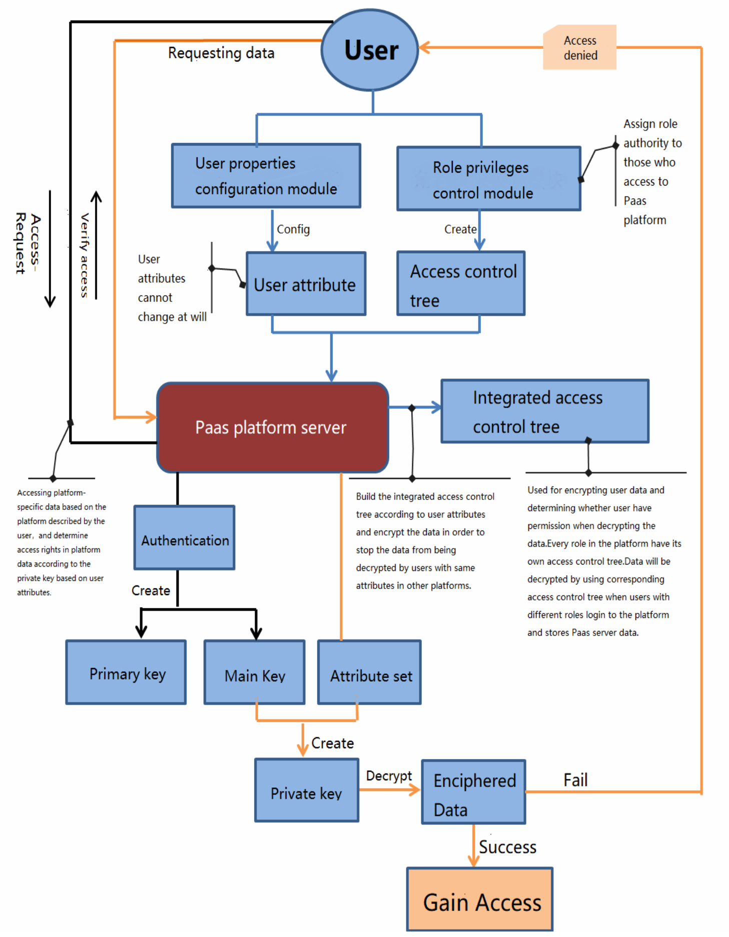
In order to solve the problems of security and load caused by the existing cloud computing system, the paper proposes a Power Grid Information Security Perception System on the basis of Artificial Intelligence technology. From the source hardware, security monitoring is carried out at the start of terminal to ensure that the operating environment is free from virus infection. The self-learning ability of the artificial intelligence technology, the trusted cloud security calculation and the load dispersing technology are used to improve the security of the system from the service terminal to the user side.

The system is mainly composed of service terminal layer, service operation management layer and service client layer.

2.1 Service Terminal Layer

Service user-side layer.

The structure is shown in Fig. 1, the core of which is the “Access control module”. In order to determine whether the user has access to the platform, the access control module needs to first obtain the user’s information and access role security policy. In the schema, user attributes and role control permissions are stored on the client and platform respectively. The access control module of the platform needs to judge the user’s rights control policy before the user can access the data.



Requesting data
User
Access denied
Assign role authority to those who access to Paas platform
User properties configuration module
Role privileges control module
Access-Request
Verify access
Config
Create
User attributes cannot change at will
User attribute
Access control tree
Paas platform server
Integrated access control tree
Accessing platform-specific data based on the platform described by the user，and determine access rights in platform data according to the private key based on user attributes.
Build the integrated access control tree according to user attributes and encrypt the data in order to stop the data from being decrypted by users with same attributes in other platforms.
Used for encrypting user data and determining whether user have permission when decrypting the data.Every role in the platform have its own access control tree.Data will be decrypted by using corresponding access control tree when users with different roles login to the platform and stores Paas server data.
Authentication
Create
Primary key
Main Key
Attribute set
Create
Private key
Decrypt
Enciphered Data
Fail
Success
Gain Access

Fig. 1. Cloud computing architecture for service user terminals

User attribute permission control policy implementation method.

The process of secure cloud computing methods and systems is shown in the figure:

After the server authenticates the user, the public parameters and the primary private key are generated.

Public parameters and the primary private key are generated through the following procedure:

The generation of bilinear parameter G, G_0, G_1, E, Z_P. G_0 and G_1 are multiply cyclic groups of two orders of large prime numbers P.

G is the generating element of group G_0. $E: G_0 \times G_0 \to G_1$ is an efficient bilinear mapping.

Z_P is a set of $P - modulo$, which contains all the less than P.

P is a positive integer of the reciprocal element. Generates a collection of properties for all user attributes $U = \{a_1, a_2, \ldots, a_n\}$,

Randomly selects $T_i \in Z_P$ for each attribute $a_i (i \in n)$, selects $A \in Z_P$ randomly,

and randomly selects $Z_P, \ldots, U_1$ in U_{2m}, each $i \in \{1, \ldots, 2_m\}$, setting $U_i = GU_i$;

Generating public parameter $P_K: G, T_I = GT_1, \ldots, T_n = Gt_n, y = e(g, g)a, u_1, \ldots, u_{2m}$ Generate Master Key

$M_K: A$, $t_i (1 \le i \le n)$, $U_1 (1 \le I \le 2m)$.

When the user requests to read the data, the platform service first generates the private key according to the master key M_K and the attribute set S, using the private key to decrypt the encrypted data that needs to be accessed, and if the decryption succeeds, the user has access rights, otherwise the access is denied.

Master key M_K and attribute set S generate private keys, including the following procedures:

Select a random number for each attribute R_j, select random number $R' \in Z_P$; for each $i \in n$, randomly set, so $G_i^0 = g^{\frac{w^i}{u^i}}$, $G_i^1 = g^{\frac{w^i}{u_{m+1}}}$, Set "$r = r' + \sum_{i+1}^{m} W_i$" Setting order "$D = g$"; The generated user private key is as follows: $S_K = (D = ga - \gamma, \forall \alpha_i \in S : D_i = g^{r^1 t_i^{-1}} \cdot g^{r_j}) i \in n : G_i^0 G_I^0$

And, in the decryption process, input public parameters P_K, ciphertext C_T and the private key S_K, when and only when S satisfies access policy A, the private key produced by the attribute set S will decrypt the C_T and return the plaintext message M.

3 Experimental Results

To verify the effectiveness of this method, we configured 400 terminals and 10 applications to create two users User1 and User2 respectively, in units 1 to 8, System 1 to System 10, where User1 has two roles u1r1 and U1R2, Corresponding to the PAAs platform of the data block DataU11 and DataU12 Read permissions; User2 has two roles u2r1 and U2R2, corresponding to the platform block DataU21 and DataU22 Read permissions respectively. To record the data before and after the system method is used in this paper. In order to ensure the accuracy of the experimental data, open the firewall strategy in advance, allow anti-virus tools and leak detection equipment testing, daily data backup 15 times, weekly data backup 7 times, daily data restore 4 times, week data restore 2 times, the experimental data to take the average. The results are as follows.

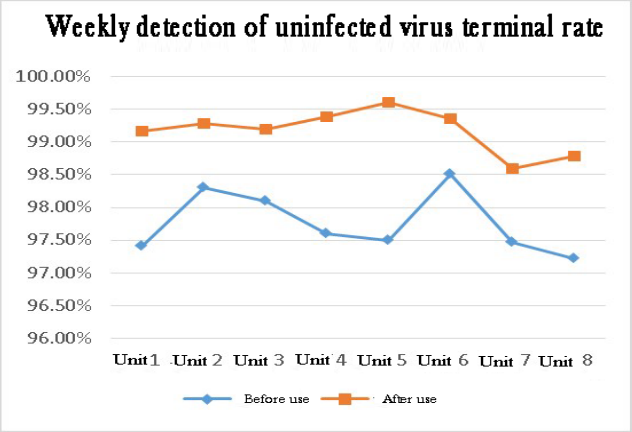


Fig. 2. Monthly detection of the terminal rate uninfected virus

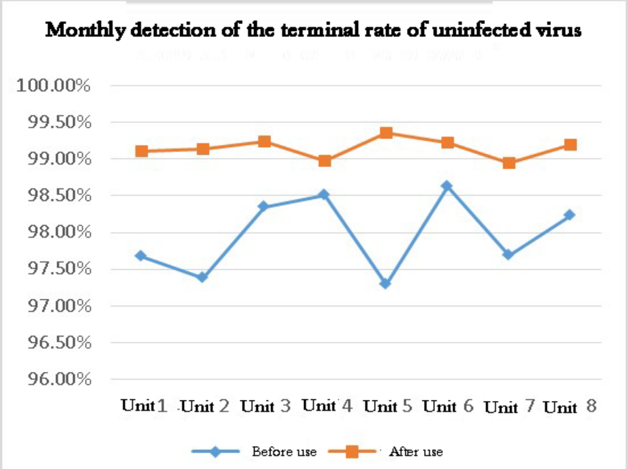


Fig. 3. Monthly detection of the terminal rate uninfected virus

Weekly detection and monthly detection indicators have been promoted, including weekly detection of the terminal rate of uninfected virus 1.41%, monthly detection of the terminal rate of uninfected virus 1.18%.

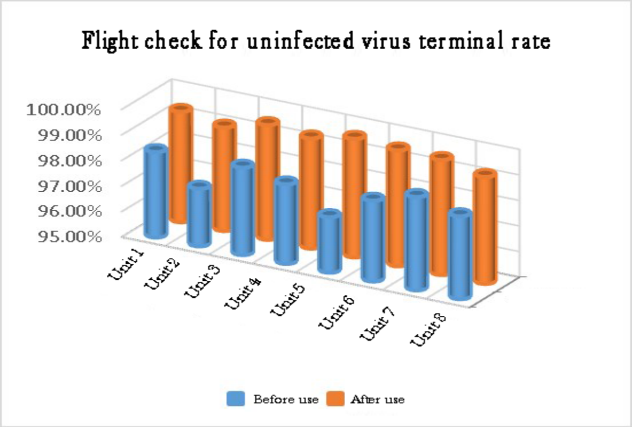


Fig. 4. Flight check for uninfected virus terminal rate

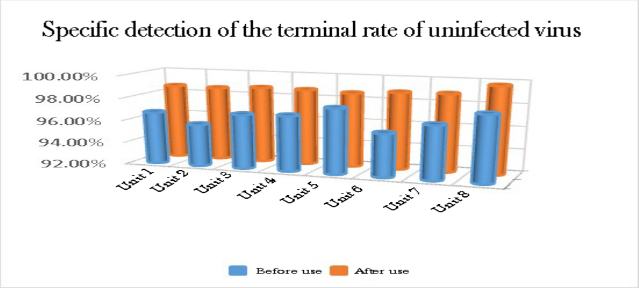


Fig. 5. Specific detection of the terminal rate of uninfected virus

Flight inspection, special testing is the nature of sampling, the use of manual detection and tool detection methods, for malicious software, Trojan detection than relying on the method of leak-sweeping tool more stringent. Using this article to describe the system after the virus has not infected terminals have been promoted.

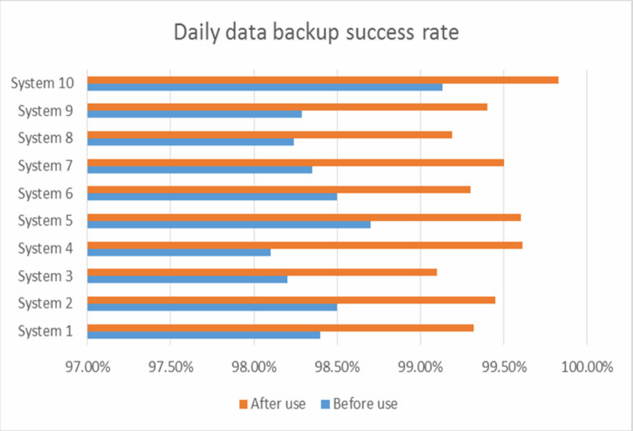


Fig. 6. Comparison of the results of daily data backup success

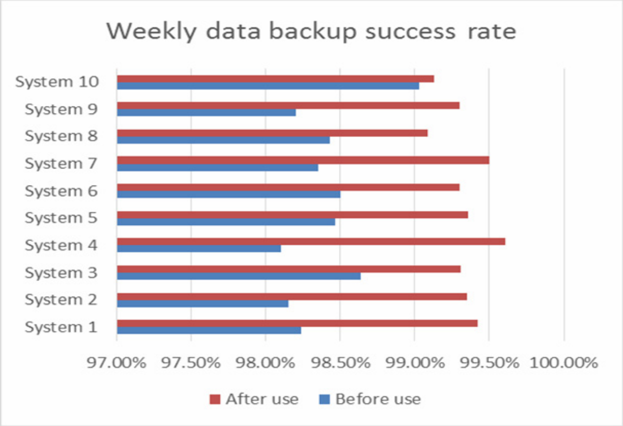


Fig. 7. Comparison of the results of weekly data backup success

The experimental results show that the average daily data backup success rate is increased by 0.99% and the weekly data backup success rate is increased by 0.93% after using the data security management method and the system mentioned in this paper.

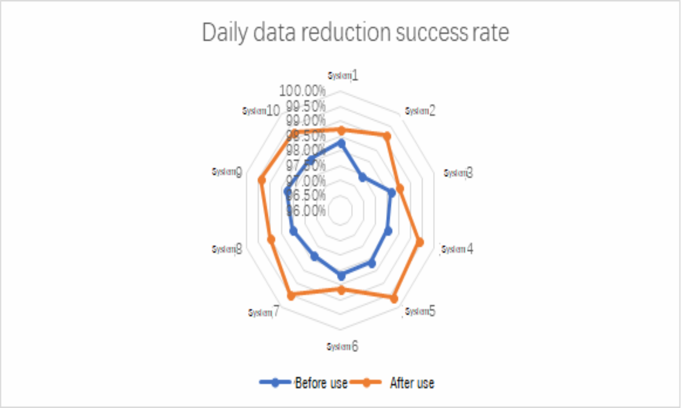


Fig. 8. Comparison of daily data reduction success rate results

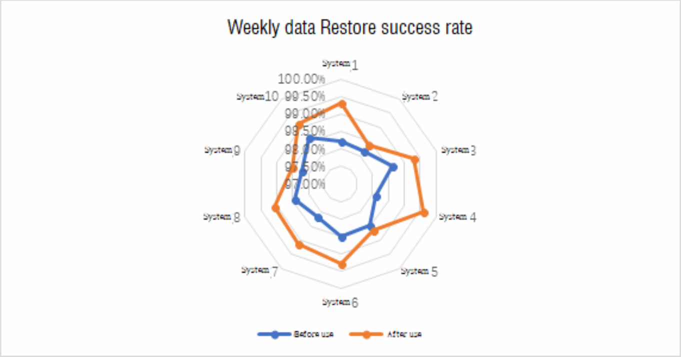


Fig. 9. Comparison of the results of weekly data reduction success

The experimental results show that the average daily data reduction success rate is increased by 1.07% and the weekly data reduction success rate is increased by 0.7% after using the data security management method and system mentioned in this paper.

Table 1. User security

User	Roles	Data	Operation
User1	U1r1	DataU11	R
	U1r2	DataU12	R
User2	U2r1	DataU21	R
	U2r2	DataU22	R

Using the illegal intrusion platform to obtain user login information, but the user properties of the client or access the tree cannot be obtained, so that the user cannot decrypt user data through the server. The test results show that U1R1 cannot access DataU12 files belonging to U1R2 under this user, and vice versa, U2R1 cannot access u2r2 files belonging to the DataU22 under this user, and vice versa.

Similarly, the two roles in User1 cannot get the blocks of data in User2, and vice versa.

The result of realization shows that:

(1) The strong isolation of data between users. In the PAAs of each data access, all need to compare user role permission set. Decryption success or not, strictly restrict other users data access.

(2) Flexible user data security control. Each user in the PAAs can define the data access permissions by customizing the user attributes and the role permission tree, which satisfies the user's access control security requirements for different roles.

4 Conclusion

To sum up, this paper creates a kind of information security situational awareness system based on artificial intelligence, improves the big data transmission method based on cloud computing, and configures the controller, backup memory, protection memory. The control machine in the BIOS starts up Virus detection prior to the operating system. The cloud server cluster extension uses user nodes to build a client cluster to handle file downloads, updates, and encryption based on user attributes, while cloud server clusters focus on providing reliable indexing and backup.

By using this double-layer structure, this paper realizes the migration of load from cloud to client, so that the server can prevent user data leakage and improve the usability and reliability of the system under the attack.

Reference

[1] F.-H. Hsu, M.-H. Wu, C.-K. Tso, C.-H. H., C.-W. Chen, Antivirus software shield against antivirus terminators, IEEE Transactions on Information Forensics and Security 7(5)(2012) 1439-1447.

[2] P.H.B. Las-Casas, V.S. Dias, W. Meira, D. Guedes, A big data architecture for security data and its application to phishing characterization, in: IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), 2016.

[3] G. Palak, T. Nidhi, Digital security implementation in big data using Hadoop, International Journal of Research Studies in Computing 5(1)(2016) 3-9.

[4] V. Changa, Y.-H. Kuob, M. Ramachandrana, Cloud computing adoption framework: a security framework for business clouds[J], Future Generation Computer Systems 57(2016) 24-41.

[5] V. Chang, M. Ramachandran, Towards achieving data security with the cloud computing adoption framework, IEEE Transactions on Services Computing 9(1)(2016) 138-151.

[6] A. Tupe, A. Priyadarshi, Data mining with big data and privacy preservation, International Journal of Advanced Research in Computer and Communication Engineering 5(4)(2016) 1121-1124.

[7] N.H. Hussein, A. Khalid, A survey of Cloud Computing Security challenges and solutions, International Journal of Computer Science and Information Security 14(1)(2016) 52-56.