Research on Global Security Sharing of Power Grid Information Based on Differential Privacy Model

Cui Li¹, Fei Wu¹, Wenqin Lin¹

¹Economic and Technological Research Institute, State Grid Fujian Electric Power Co. LTD., Fuzhou, China, 350012

*Corresponding author e-mail: licui@fj.sgcc.com

Abstract. With the advancement of science and technology, intelligent power transmission technology is also constantly developing. Among them, the information security of the transmission grid in the power system is an important content that cannot be ignored. This article first analyzes the current status of power information security issues, including research on the current status of foreign power information security. Secondly, it studies the differential privacy model, finally it studies the power grid security domain information sharing technology.

Keywords: Intelligent Power Transmission Technology, Power Information Security, Power Grid Security Domain Information Sharing

1. Introduction

With the continuous development of the information society, data security has increasingly become a topic of concern. In today's information age, the Internet has been widely used in all aspects of life. In our daily lives, data leakage has caused all kinds of troubles and losses. At the same time, we will also face serious consequences such as huge legal liabilities and reputation damage compensation. All these deserve people's attention [1].

2. Current status of power information security issues

2.1. Electric power information security issues

A large number of devices of the smart grid are connected to small or microcomputers on the grid. Therefore, many criminals will use these devices to maliciously attack the internal code of the power grid system, which causes the internal data of the power grid system to be lost or destroyed, and this may even cause the system to crash. Electric power information security, like computer network security, must face both objective and subjective threats [2].

The information communication of the intelligent transmission network has the characteristics of centralized management, and the transmission network has high requirements for the real-time and reliability of information. The smart transmission grid transmits a large amount of electric energy through long-distance transmission lines. It is connected to the distributed energy and charging center in the smart grid, and it has high-voltage energy storage facilities and distributed energy access. The
intelligent control center controls the intelligent transmission network and the intelligent substation through the intelligent transmission communication network, and controls the flow of information with the flow of information. Therefore, information security directly affects the physical security of the power grid [3].

2.2. Current status of foreign research
In order to meet the needs of power systems and other public utilities, the International Electrotechnical Commission’s 57th Technical Committee (IECTC57) has developed a series of standards such as IEC60870-5, IEC 60870-6, IEC61970 and IEC 61850. Figure 1 is a simple schematic diagram of grid data exchange [4].

![Figure 1. Simple schematic diagram of grid data exchange](image)

In foreign countries, the IEC standard is adopted by nearly 90% of SCADA systems, integrated substation automation systems and intelligent protection systems. Standardized and open protocols have brought security risks, so it is necessary to take corresponding security measures to prevent damage caused by hidden dangers. As early as 1993, experts put forward the concept of "data security" in the power energy management system [5].

3. Differential privacy model

3.1. Definition and nature
The differential privacy model was originally proposed to protect the security of the database. Consider two data sets D, D' that differ only in one record. Although there are differences between them as the input of the query function, if there is no obvious difference between the query results of the two, then the difference between them cannot be deduced from the output [6]. Such a data set D, D' is called a "neighboring data set", and the strict definition of a neighboring data set is as follows:

Assuming that the attribute structure of data set D, D' is the same, if D, D' differ by at most one record, they are called adjacent data sets. On the basis of the adjacent data set, give the definition of $(e,0)$ and $(e,\delta)$-differential privacy.
Definition 1 (\((\varepsilon, 0)\)-differential privacy): The set of all possible outputs of random algorithm \(A\) is denoted as \(\text{Range}(A)\). If \(A\) has any data set \(D, D' \approx D'\) and any \(B \subseteq \text{Range}(A)\), it is as shown in formula (1):

\[
\Pr[A(D) = B] \leq e^\varepsilon \cdot \Pr[A(D') = B]
\]  

(1)

It is said that Algorithm \(A\) satisfies \((\varepsilon, 0)\)-differential privacy.

Definition 2 (\((\varepsilon, \delta)\)-differential privacy): The set of all possible outputs of random algorithm \(A\) is denoted as \(\text{Range}(A)\). If \(A\) is for any adjacent data set \(D, D'\) and any, as shown in formula (2):

\[
\Pr[A(D) = B] \leq e^\varepsilon \cdot \Pr[A(D') = B] + \delta
\]  

(2)

It is said that Algorithm \(A\) satisfies \((\varepsilon, \delta)\)-differential privacy.

Definition 3 (Global Sensitivity): For the algorithm \(f_{DP}\) acting on the data set \(D\), the global sensitivity \(\Delta f\) is defined as shown in formula (3):

\[
\Delta f = \max_{(D, D')} |f_{DP}(D) - f_{DP}(D')|
\]  

(3)

3.2. Related implementation mechanism
Differential privacy defines a strict privacy protection model, but its definition is not convenient for direct use in algorithm design. In order to facilitate the construction of related algorithms, some mature differential privacy implementation mechanisms have been developed [7].

4. Power grid security domain information sharing technology

4.1. Original information sharing technology
The core idea of the propagation-based security information sharing method is to bind attributes and strategies to the object, and then in the system, the owner of the object passes the object to other users to realize information sharing. This method is based on the attributes of the object to authorize and decide which users can access the object, which partially reflects the advantages of autonomous access control and usage control. However, the information transmission lines are too fine, which is not conducive to the scale and efficiency of information sharing [8].

4.2. Independent access control technology
Discretionary access control technology (DAC) is the simplest method of access control. Users have the right to manage the objects they own, and they can grant other users the right to access this object through authorization. It can also be said that user owners choose other users to share their own resources, and they can also take back the sharing rights of these users. In general, users have absolute management rights over their own resources.

4.3. Mandatory access control technology
Mandatory access control (MAC) refers to strict system-level management. The system makes hierarchical constraints on the access operations between the subject and the object by formulating a rigorous and fixed rule. For example, this determines which level of information users can access. Even if it is a file created by the user, the user must follow the system rules to determine the access rights to this object.

4.4. Role-based access control
The core idea of role-based access control (RBAC) is that users are associated with permissions, and users get a certain role and get all the permissions that they have on the role. This simplifies authorization management, thereby improving system security. RBAC supports three important
principles in permission semantics: the principle of least permission, the principle of separation of responsibilities, and the principle of data abstraction [9].

The principle of data abstraction can be embodied through abstraction of permissions. In the permission configuration of RBAC, the elements of role-based access control include basic definitions such as users, roles, and permissions, as shown in Figure 2:

![Figure 2. RBAC configuration model](image)

It can be seen from the figure that the authorization management of RBAC mainly includes: the assignment of users and roles; the assignment of roles and permissions. A user can have multiple roles, and a role can be used by multiple users. A role has multiple permissions, and each permission can be assigned to multiple roles. RBAC has undergone more than 20 years of research, and NIST is its typical standard. The RBAC model of the NIST standard is shown in Figure 3 [10].

![Figure 3. RBAC model](image)

4.5. Use control
Usage control (UCON) has received a lot of attention due to its comprehensive model and flexibility. In recent years, its research work has led to the tremendous development of UCON. It has the flexibility of authorization and the attribute as an authorization decision condition, and it is the most widely used access control technology. The structure diagram of UCON model is shown as in Figure 3.
Figure 4. Structure diagram of UCON model

5. Conclusion
With the rapid development of computer technology, people pay more and more attention to information management and security issues. Due to the development of Internet technology, people like to share information, but there are also many network security issues when information is shared. This paper studies a global security sharing technology of power grid information based on a differential privacy model. This technology effectively improves the security of global power grid information sharing. Of course, there are still some problems, researchers need to continue to improve.

References
[1] Chen Xiaonan. Analysis of Information Sharing and Network Security Research [J]. New Business Weekly, 2018:293.
[2] Rulin. Research on Information Security of Resource Sharing Network Based on Local Area Network [J]. Computer Security, 2013:54-55+58.
[3] Su Yonghong, Zhang Yurong. Research on the Construction of Excellent Resource Sharing Course of "Network and Information Security" [J]. Education Teaching Forum, 2017.
[4] Hua Yantao, Yu Biao. Research on the Security and Privacy Protection of Internet of Things Information Sharing [J]. Information and Computer (Theoretical Edition),2011:11-12.
[5] Ye Bin. Study on the security of file information resource sharing in Suichang Electric Power Bureau [J]. China High-tech Enterprise, 2012:162-163.
[6] Liu Xiaobo. Study on the content security of science and technology information resource sharing under the network environment [J]. Modern Information, 2010:168-171.
[7] Wu Houchun, Hu Nan, and Qin Yan. Analysis of a smart grid information security protection model based on hierarchical protection [J]. Communication World, 2018:166-167.
[8] Guo Feijun. A safe sharing method of ship cloud data copy based on differential privacy [J]. Ship Science and Technology, 2018:130-134.
[9] Ren Jun, Xiong Jinbo, Yao Zhiqiang. Security control scheme of cloud data copy based on differential privacy model [J]. Journal of Network and Information Security, 2017:42-50.
[10] Wei Yuyang, Ma Kai, Wu Xiang, Mao Yaqing. Design and Implementation of a Security Sharing Platform for Differential Privacy DNA Phantom Recognition [J]. Computer Measurement and Control, 2018:240-243.