Proceedings of CECNet 2022
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220533

Research on Security Sharing Model System of Power Digital Spatial Data

Aijun WEN, Zesan LIU, Di LIU, Chenghua FU[1] and Ziting GAO
State Grid Information and Telecommunication Group Co., Ltd., Beijing, 100032, China

Abstract. Digital transformation will promote the rapid progress of power digital space construction led by power data. Through the use of new digital information technology, we will give full play to the function of data integration and effectively support the construction of new power system. Data interconnection is the key link to release the value of data, but at present, there are still many urgent problems to be solved in the power digital spatial data sharing, such as the mismatch between data demand and data supply, weak security guarantee and so on. In order to study the security protection of power digital spatial information data sharing, according to the concept of privacy computing, a power digital spatial data security sharing model system based on privacy computing is designed. This model system has strong research and practical significance for realizing the secure circulation and sharing of new power system data.

Keywords. Power digital space, new power system, data security sharing, privacy-preserving computation.

1. Introduction

Through the application of a new generation of digital technology, the power digital space plays the role of data integration, realizes real-time mapping of new power systems, flexible and efficient allocation of power grid resources, and extensive aggregation of massive resources. How to effectively manage power grid data, do a good job in power grid data sharing, and give full play to the maximum value of new power system information resources is the basis for promoting the construction of power digital space. In data resource sharing, there are still problems such as difficulty in mutual trust between shared participants, high data security risks, weak protection of private information, and unclear data ownership [1]. The large limitation has become a key problem that urgently needs to be solved in the current data resource sharing [2]. In order to achieve a balance between data sharing applications and data privacy security protection, privacy computing has gradually entered the vision of the data industry. The privacy computing technology [3-7] guarantees the "available and invisible" of data in the process of circulation and fusion, so as to meet the needs of industrial development for the circulation of data elements under the premise that the private data is fully protected.[8-13]

[1] Corresponding author: Chenghua FU, State Grid Information and Telecommunication Group Co., Ltd., Beijing, 100032, China;E-mail:fuchenghua@sgitg.sgcc.com.cn.

By analyzing the challenges faced by power digital spatial data security sharing, combined with the theory of privacy computing technology, this paper proposes a model system of power digital spatial data security sharing based on privacy computing technology.

2. Research on Security Sharing of Power Digital Spatial Data

2.1. Challenges Faced by Power Digital Spatial Data Security Sharing

The demand of new power system for data fusion, sharing, development and circulation is increasing day by day, and the importance of power data security construction is also increasing. The security sharing of power digital spatial data mainly faces the following challenges:

(1) Challenges of various data types

Power enterprise data comes from development, transmission, transformation, distribution, regulation and other activities. It is different from multi-source heterogeneous data with different format standards, frequencies and definitions related to power supply operation, equipment management, business services and enterprise information management. There are a large number of enterprise data, a variety of data caliber, differences in professional caliber data, and the data are scattered in different units, different professional application systems, the data base is not unified, and the quality is uneven.

(2) Challenges of lack of process specifications

The management of power grid companies did not have detailed compliance guidance in all links of the whole process of sharing and opening up. The standards and methods of various institutions for the sharing needs of power grid related information were different, there was no clear understanding of the overall structure of power consumption information, and the information application mechanism after information circulation was not perfect.

(3) Challenges of immature technical solutions

Power grid information data has the characteristics of large volume and fast growth. With the continuous accumulation of power grid data information, the social demand for the ability of data information public sharing security protection technology will be higher and higher. At present, a relatively mature set of privacy protection technology scheme has not been established.

The use of privacy computing technology can realize the fusion and sharing of data from different data sources, and solve the dilemma of fusion and utilization of a wide variety of data sources that cannot be efficiently used; the use of privacy computing technology can realize the sharing and use of data under the condition that the data does not exceed the threshold, and the process of data circulation "Available is invisible, but it is not desirable" to ensure data privacy and security.

2.2. Application Prospect of Privacy Computing Technology in Secure Sharing of Power Digital Spatial Data

Data security in data sharing and circulation has become the focus of extensive attention in the academic circles [14], and privacy computing has also created a strong technical foundation for the development of modern security technology[15-19]. Privacy

computing, which has the dual characteristics of privacy protection and data application, has broad prospects in the field of data circulation. The use of privacy computing can effectively solve the data security problems in the sharing of power digital spatial information, and carry out the statistics and classification of information while protecting and securing the original data. In the process of multi-party information exchange and fusion, privacy computing technology has important advantages in ensuring security.

Through the application of new generation digital technology, power digital space plays a role in data integration, promotes the development of power grid digitalization and supports the construction of new power systems. Data sharing is also the development trend of the new power system at present. Privacy computing technology has become the main guarantee of security, and has a good and broad prospect in the power digital space. The secure multi-party computing and privacy computing technology in the power digital space data sharing and financing can solve the problems of information privacy and information security such as multi-party information exchange, resource interaction, privacy protection, use rights, etc., so that a large amount of information can be used effectively, which has laid a credible security cornerstone for the construction of China's power digital space, Combined with traditional digital desensitization technology and confidentiality means, it can effectively break through information security barriers, and effectively ensure the authenticity, perfection and information security of information under the cooperation of all parties.

In the future, privacy computing technology will be widely used in the secure sharing of power digital spatial data. Using the privacy computing technology of secure multi-party computing and trusted operating environment, it can carry out efficient statistical analysis without breaking away from the private domain of power digital spatial information, so as to ensure the security of private information and achieve the safe sharing of information across domains. Through the federal learning network, the power digital spatial data can realize highly trusted joint computing, and the information can be safely shared and used. Build a cross industry resource sharing system, provide data privacy protection measures to participating enterprises, establish a good information environment, and improve the overall security management level of power digital space.

3. A New Power System Data Security Sharing Model System Based on Privacy Computing Technology

3.1. A New Power System Data Security Sharing Model System Based on Privacy Computing Technology

While carrying out data fusion and sharing and establishing power digital space business collaboration, it is necessary to ensure the security of power digital space data and maintain the rights and interests of all participants in information and data sharing. Based on privacy computing technology, build a manageable, safe and efficient power digital spatial information sharing model system (as shown in Figure 1), realize the calculation of data in encrypted state, and protect the privacy data security of all participants. The model system of power digital spatial information sharing based on privacy computing adopts a secure multi-party computing framework. Multi party computing includes various roles such as task initiator, computing party, data user, data provider, etc. in actual use, each entity can concurrently serve two or more roles. In Figure 1, the task

initiator and data user can be merged into one party, and the roles of algorithm provider, calculator and dispatcher are all played by the privacy computing platform. This model system is mainly divided into three participants: data provider (input party), data user (result user), and privacy computing platform (Computing party). All systems, platforms, units and departments of the power system, as participants in the process of data sharing and circulation, are both data providers and data users; The privacy computing platform is responsible for providing and managing data security sharing space and providing data security sharing services based on privacy computing for power digital space. In addition to data circulation and sharing among systems within the power grid, data fusion and sharing can be realized between the power grid and social third-party platforms and government platforms by relying on the privacy computing basic platform, giving full play to the value of data elements and enabling the development of digital economy.

The implementation process of multi-party security computing consists of data input, task calculation and result analysis. The participating nodes of each data provider participating in the collaborative computing task will search the required data information in the local database system according to the requirements of the computing logic, and work together to carry out collaborative computing among the dense data information flows for the secure multi-party computing task. However, in the overall process, all their plaintext data information is saved locally and not submitted to other nodes. The security of the transmitted data is ensured by the combination of multiple security protocols, and the data information is kept secret through homomorphic encryption algorithm, so that under the premise of no trusted third party, multiple main participants will not disclose the secret data information while getting the correct calculation results. Among the main participants, the term "calculation result factor" is defined. The calculation result factor refers to the signal output by the data information provider after completing a key conversion. Its essence is to protect the secret security of data.

The data analysis service provider analyzes the data read from the local database system, generates the calculation result factor (input factor) after MPC data input processing, and uploads the entry factor to the operation node of the privacy statistics platform. Each operation node performs collaborative calculation based on the entry factor, and finally submits the secret calculation result factor (output factor) to the data user, The data user decrypts the calculation result and uses it.

The privacy computing platform includes core computing system, data quality management system and computing assistant management system.

(1) Core computing system

The core algorithm system is also an important computing party in the application of privacy computing, which realizes the "input privacy" and "output privacy" that should be paid attention to in private computing. Input privacy refers to the input information and intermediate results that the main participants cannot extract and analyze without permission, and output privacy refers to the fact that the main participants cannot reverse the data results to sensitive data. The privacy computing technology adopted here is secure multi-party computing technology. [20-21]

(2) Data quality management system

Data analysis quality supervision and management provides data quality control services at all stages of data provision, analysis and application, including data analysis specification management, quality plan management, data analysis quality index management, data analysis quality evaluation, and data analysis standardization,

perfection, accuracy, unity, timeliness, uniqueness and usability shall be supervised and managed.

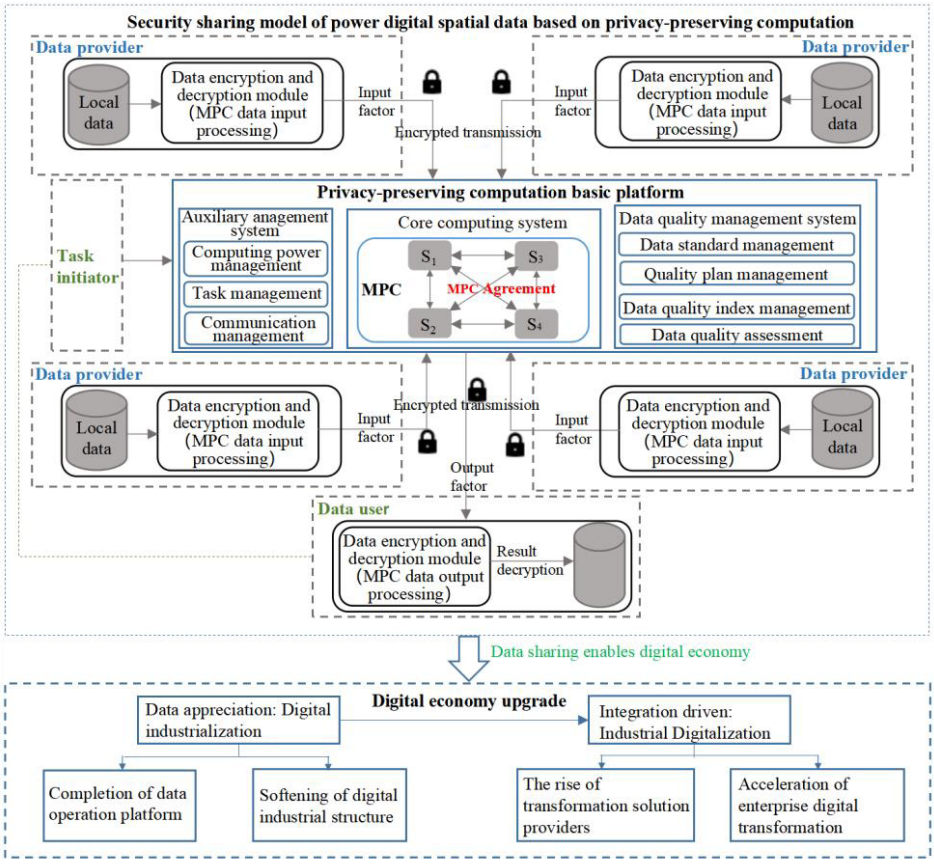

Figure 1. A model system of electric power digital spatial data safe sharing based on privacy-preserving computation

(3) Computer aided management system

Computer aided management system includes computing power management, task management and communication management. Privacy computing requires a lot of computing power. Computing power management realizes the optimal match between computing power demand and computing power resources through intelligent monitoring resources. Task management realizes task scheduling, and calculates task resources and computing resources in a balanced manner, while network control realizes scheduling control between cross platform process communications. The task scheduling part realizes the parallelization of the system, thus reducing the resource time used to complete the task [22]. Load balancing is achieved through task scheduling, and more efficient communication mechanism is used for communication scheduling, which reduces the processing time of transactions between cross platforms, thus improving the efficiency of the platform [23].

The new power system information resource sharing mode based on privacy computing technology uses the basic platform of privacy computing technology as the

intermediate medium to realize the secure cooperative resource sharing between data providers and data applications, and enable the development of digital economy.

3.2. Core Security Technology

The core information security technology used in this paper is secure multi-party computing. Secure multi-party computing (MPC)[24], the main purpose of information security multi-party computing is to overcome the problem of the ability of untrusted participants to work together under the condition of ensuring the information security of both sides [25]. The advantage of secure multi-party computing is that all participants have absolute control over their basic data to ensure the disclosure of basic data and personal information. Figure 2 is the logic diagram of secure multi-party computing. User C1 has private data x, and user CN has private data y, and they do not know each other's data. In order to achieve cooperation between the two users, they distribute encrypted data fragments (x_1, x_2... x_n, *etc.*) to the server through secret sharing protocol; The server has several computing nodes (S_1, S_2, *etc.*) to calculate the encrypted data fragments according to the privacy computing protocol, and the calculation results are returned to the user. Secret sharing refers to the concept of hiding secret value by dividing secret value into random shares, and then giving these shares to different parties.

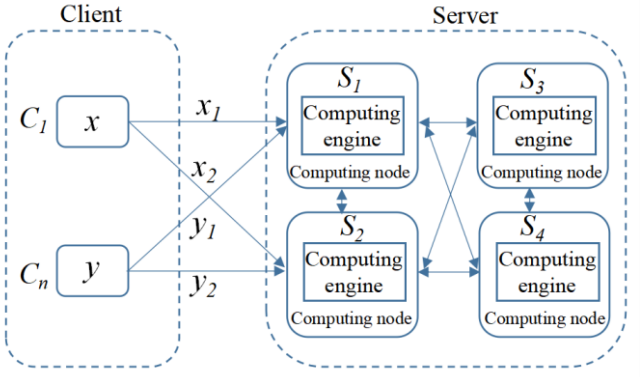

Figure 2. Logic diagram of secure multi-party computation

3.3. Application of Power Digital Spatial Data Security Sharing Based on Privacy Computing

The power digital space with secure multi-party computing technology and its data sharing mode are mainly used in order to realize joint data analysis. Due to the vigorous development of big data analysis technology, the amount of various data information and materials formed and obtained in the economic society has increased significantly. The acquisition of sensitive information data analysis, the cooperation of cross-border organizations and the business operation of cross-border enterprises have provided new challenges to the traditional data analysis algorithms, and the existing data analysis algorithms may cause a lot of privacy exposure, Therefore, privacy and information security in data mining have also received great attention. Introducing secure multi-party computing technology into the field of traditional data mining can alleviate this problem to a certain extent. By using multi-party data source collaborative data analysis algorithm, a large number of sensitive information data analysis can not be disclosed.

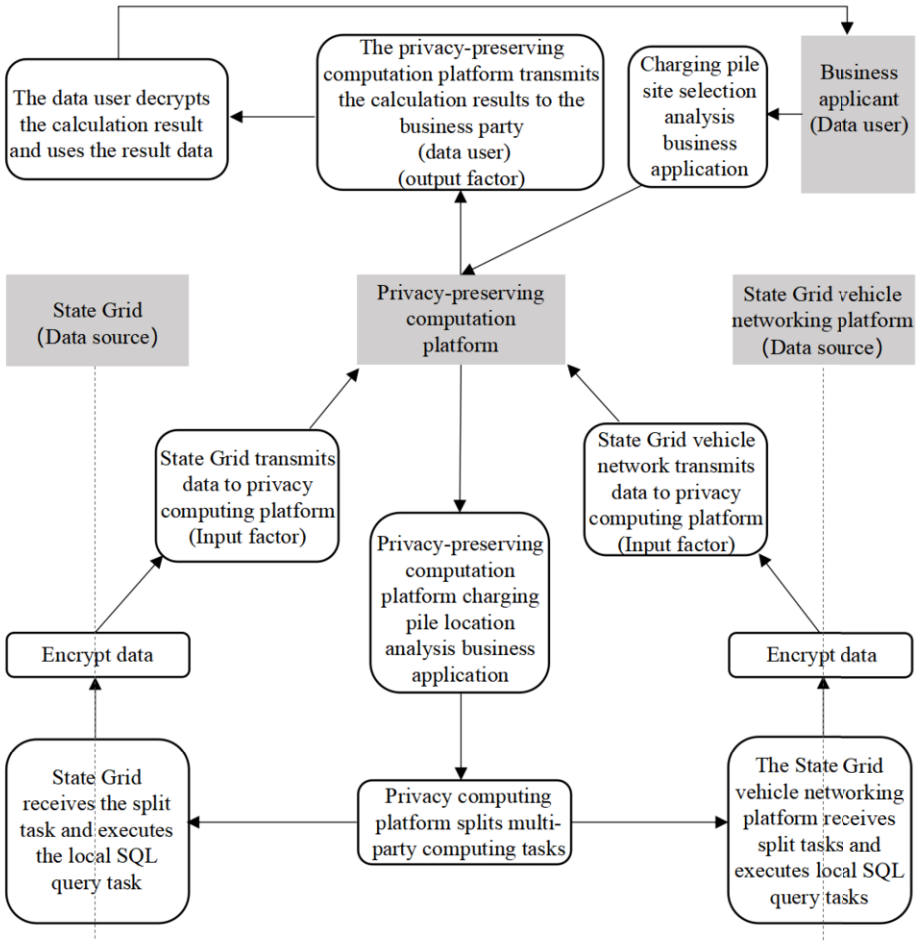

Figure 3. Business process of charging pile site selection

In the new power system design under the digital transformation of power digital space, the application of data sharing and fusion analysis is increasingly prominent. The application of using the information of multiple information providers to realize fusion data analysis and make power grid investment decisions is very extensive. Such as: intelligent operation of power grid, refined demand side management, internal and external data fusion and sharing of state grid energy big data center, business data sharing among provincial energy big data centers, information interaction and sharing between electric vehicles - charging piles - operators - power grid and other scenarios. Typical scenario analysis is as follows:

Using privacy computing technology in charging pile marketing, location and other scenarios, and with the support of proprietary data such as activity range, driving trajectory, driving habits, charging habits, etc., we can help the construction party determine the location without disclosing user sensitive data, and carry out customized marketing and bidding marketing in combination with owner data in subsequent charging pile operations, Improve the utilization rate of charging piles and improve the overall benefits; In the use of charging piles, account verification can be carried out in

combination with the owner's track and other information to prevent the occurrence of malignant events such as user account theft.

The business process is shown in Figure 3, and the key steps are described as follows:

(1) The privacy computing platform receives the application of charging pile location analysis business, which is disassembled into multiple multi-party computing tasks according to the business joint statistics and computing task request;

(2) The State Grid and the State Grid vehicle networking platform need to perform local SQL query tasks and obtain local query results according to the query tasks split by the privacy computing platform;

(3) The State Grid and the State Grid vehicle networking platform encrypt the local query results and transmit the encrypted results to the privacy computing platform;

(4) The privacy computing service platform performs the calculation and feeds back the calculation results to the business demander.

Data sharing and fusion analysis involves data interaction between multiple departments of the State Grid, and even with other industries. Data sharing and circulation are faced with privacy protection issues, so it is necessary to build a safe and reliable computing environment to ensure that all participants cannot obtain data outside their authority, so as to achieve the purpose of obtaining results through secure computing.

4. Conclusion

In this paper we analyze the challenges faced by the safe sharing of power digital spatial data, summarizes the application prospects of privacy computing technology in the safe sharing of electrical digital spatial data, and proposes a model system for the safe sharing of electrical digital spatial data based on privacy computing technology. Under the new power system, data elements are shared and exchanged more frequently between power and related social enterprises, departments and regions, and the circulation of data elements is wider. Through collaboration with external data, power data can not only empower and upgrade the power grid business itself, improve quality and efficiency, but also play a major role in promoting the economic development of the whole society, national governance, pollution prevention and carbon reduction, etc. However, with the increasing number of external cooperation and open sharing environment, serious deficiencies in data production factor governance capability and privacy protection capability have been exposed. Building a privacy computing service platform is a necessary way to reasonably use sensitive information of the power grid to solve related problems, and it is an effective way to rationally use the sensitive information of the power grid. The State Grid big data center, the data centers of various network provinces, and the energy big data center involve internal and external data interaction scenarios, and privacy computing technology can be applied to the current multi-level big data center scenarios. The platform can access multiple data sources or business demand platform data such as data from various platforms of the power grid, social platform data, and government system data.

References

[1] Bian WL. Privacy-preserving computation: Industry Applications have Huge Potential. 21st Century Business, 2021-11-11(012).
[2] Xu W, Wang Y, Jin C, et al. Thoughts on interconnection of data circulation platform based on privacy-preserving computation. Financial Computerizing, 2021, 9:72-73.
[3] Kubicek H, Cimander R, Scholl HJ. Organizational interoperability in E-Government: Lessons from good practice cases all over Europe. Berlin: Heidelberg, 2011:135-141.
[4] China M. White paper on privacy-preserving computation Applications. China Mobile, 2021.
[5] Privacy-preserving computation alliance, Institute of Cloud Computing and Big Data, China Academy of Information and Communications Technology. White paper on privacy-preserving computation. China Academy of Information and Communications Technology, 2021.
[6] Konecny J, McMahan HB, Felix XY, et al. Federated learning: strategies for improving communication efficiency. [2021-03-10]. https://arxiv.org/abs/1610.05492.
[7] Tian L, Sahu AK, Talwalka A, et al. Federated learning: challenges, methods, and future directions. IEEE Signal Processing Magazine, 2020. https://arxiv.org/abs/1908.07873.
[8] China Information and Communication Institute. Research report on computing applications of data value release and privacy protection[R]. China Information and Communication Institute, 2021.
[9] Yan GX, Liu B, Cheng, H, et al. Research on data sharing security framework. Information Security Research, 2019, 5(2):309-317.
[10] Zhu H, Liu JY. Research on the privacy-preserving computation model of users' online disclosure of personal information in the sharing era. Books and Information, 2019(2):76-82.
[11] Dong, X.Q., Guo, B., Shen, Y., et al. An efficient and secure decentralized data sharing Model[J]. Chinese Journal of Computers, 2018, 41(5): 1021-1036.
[12] Zhang, Y.T., Xia, L.X..Research on the integration model of E-Government information Information, 2009, 8(7): 161-165.
[13] Zhang CY. Outlook on the development trend of key technologies in privacy-preserving computation. Science &Technology Industry of China, 2021, 10:16-22.
[14] Yang J.. Research on data security application based on privacy-preserving computation technology. China Technology Industry, 2021, 10:61-63.
[15] Mao YL, Hong WB, Wang H, et al. Privacy-preserving computation offloading for parallel deep neural networks training. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7):1777-1788.
[16] De Cristofaro E, Tsudik G. Practical private set intersection protocols with linear computational and bandwidth complexity. [2021-03-10]. https://eprint.iacr.org/2009/491.pdf.
[17] De Cristofaro E, Tsudik G. On the performance of certain Private Set Intersection protocols, 2012. https://eprint.iacr.org/2012/054.pdf.
[18] Freedman MJ, Nissim K, Benny P. Efficient Private Matching and Set ntersection, 2004. https://iacr.org/archive/eurocrypt 2004/30270001pmeurocrypt04-lncs.pdf.
[19] Johnson T, Dasu T. "Data quality and data cleaning." ACM SIGMOD International Conference on 2003.
[20] Hardy S, Henecka W, Ivey-Law H, et al. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption. [2021-03-10]. http://arxiv.orgabs/1711.106 77.
[21] Yang S, Ren B, Zhou X, et al. Parallel distributed logistic regression for vertical federated learning without third-party coordinator. [2021-03-10]. http://arxiv.org/abs/1911.09824.
[22] Duan XY, Han XL, Wu XL. Non-real-time buffer information based scheduling algorithm in LTE system. Journal of Harbin Institute of Technology, 2016, 48(11):142-146,154.
[23] Lv PP, Zhao JQ, Li DC, et al. A consensus-based collaborative algorithm for realtime dispatch of island microgrid in cyber physical system. Proceedings of the CSEE, 2016, 36(6):1471-1480.
[24] Yao A, "Protocols for secure computations". 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982).1982 Nov; l(1):160‑164.
[25] Smart NP. Cryptography sade simple. Berlin:Springe, 2016:439-450.