Research on Data Security Guarantee System for Digital Government Construction

Qiuyan Li[1a], Feifei Bu[1b], Yuanpeng Hua[1c], Haishan Wang[2d*]

[1]Economic and Technological Research Institute of State Grid Henan Electric Power Company, Zhengzhou, Henan, China
[2]Xi'an International Studies University, Xi'an, China

[a]hnlxy2003@163.com, [b]18236755923@163.com, [c]13783661352@163.com, [d*]1255202209@qq.com

Abstract: The construction of digital government plays a pivotal role in promoting the modernization of the national governance system and governance capabilities. In the process of digital government construction, data security guarantees are conducive to information sharing and interconnection among various rights systems. On the basis of elaborating the current status of digital government construction, the risks faced by government data security are discussed, followed by the analysis of the difficulties in building data security, and finally by constructing a classification and grading system for the entire process of government data, improving the technical level of data security, Improve data security laws and regulations and legalize data open procedures to think about the specific implementation path. To achieve "development-oriented, security-oriented", it is necessary to make government data play an important role in the construction of "Digital China" and "Digital Government", and establish a comprehensive data protection system.

Keywords: digital government; data security; guarantee system.

1 Introduction

In my country, more than 80% of the data is controlled by government departments at all levels. Establishing and improving the corresponding government data security and administrative responsibility system has a great foundation for building a "digital government" and promoting the modernization of the national governance system and governance capabilities. [1] My country's digital government construction is in a stage of rapid development, and many important progresses have been made. First of all, actively promote the construction of digital infrastructure to provide a solid foundation for digital government, and secondly, various government departments actively promote the application of information technology, and realize the digital transformation in administrative approval and public services. However, government data security issues frequently occur around the world today. Government affairs public data such as human resources and social security, industrial and commercial

C. Chen et al. (eds.), *Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023)*, Atlantis Highlights in Computer Sciences 17,
https://doi.org/10.2991/978-94-6463-304-7_14

taxation, etc. are crawled in batches, used for abnormal data application services, and offline illegal data sales [2] and other accidents have a great impact on government affairs. Data security issues present new challenges. On December 24, 2021, the National Development and Reform Commission issued the "14th Five-Year Plan for Promoting National Government Informationization", which clarified "strengthening government data security management and improving government data security supervision mechanisms", but only from the legislative level. Government data security is not enough. In order to deal with the security risks brought about by government data security, it is necessary to deeply understand the existing problems of government data security, and build a data security capacity-building system for government data from multiple perspectives. Government data security includes taking technical measures to ensure the security of government data, as well as taking timely remedial measures when government data security incidents occur or may occur [3], which mainly defines government data from static and dynamic perspectives Safety. In addition, my country's government data security currently has problems such as unclear boundaries between subjects' powers and responsibilities, and incomplete classification and classification. [4]

2 Government data security risks in digital government construction

The flow and sharing of government affairs between government data departments has triggered the opening up of the whole society, leading to continuous security issues. According to the "China Government and Enterprise Organization Data Security Risk Analysis Report", government agencies accounted for the highest rate of 16.1% in 2022. A data security risk organization is formed, as shown in Figure 1.

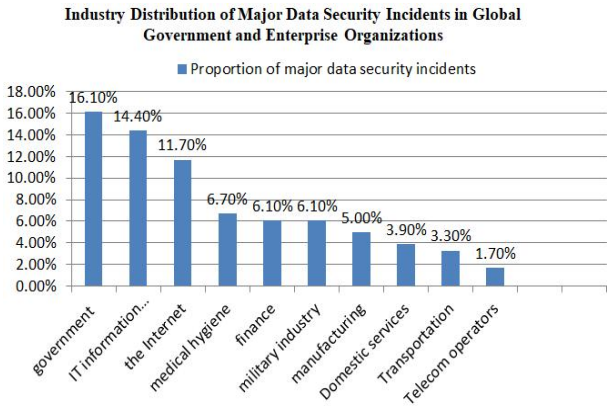

Fig. 1. Industry distribution of major data security incidents of global government and enterprise institutions

At present, government departments have taken corresponding protective measures for the security of government affairs data to reduce the risk of leakage. However,

after the government affairs data is aggregated, it will still be subject to attacks such as correlation analysis and statistical analysis, which will cause the risk of leakage. The main risk factors for government data security are listed below in Table 1.

Table 1. Major Risk Factors of Government Data Security

The main risk factors	Performance characteristics
Manage system risks	The responsibilities of management departments are vague
	The use of data is chaotic
	Security audit is insufficient
Risk of data leakage	A large amount of government data is gathered
	The safety accident accountability system is not perfect
Risk of data sharing	Insecure shared access
	There are security management and technical measures based on the boundaries of the government system
	The boundaries between data systems is unclear

Based on the information security risk assessment (ISRA), in the risk assessment model, the calculation of the risk value involves three elements: the importance of assets, the severity of vulnerabilities and the frequency of threats. The formula is expressed as follows.

$$\mathrm{R} = f(A,V,T) = f\big(f(A,V,),L(V,T)\big)$$

Among them, R is the risk value, V is the vulnerability, T is the threat, and A is the asset; L(V,T) indicates the possibility of security incidents, and f(A,V) indicates the loss of security incidents. This formula can roughly calculate the risk value, which is a macro model for risk assessment.

3 The dilemma of data security in the construction of digital government

Data security management is the key to ensuring the overall security of the country. With the continuous advancement of the government's digitalization process, the construction of digital government has not only improved the efficiency of national data governance, but also triggered new national data security governance issues.

3.1 There are major deficiencies in the classification and grading mechanism of government data

The government data classification and grading system can better balance the convenience of data use and the security of data protection, and promote the construction of data security capabilities to reduce costs and increase efficiency. At present, my country has not yet established a set of norms for government data

classification, which is not conducive to the storage, processing, sharing, and opening of government data.

3.2 The traditional security supervision assessment is insufficiently adapted to the security of government affairs data

Government data has mobility in different carriers and scenarios, and its security protection requirements also change dynamically according to factors such as magnitude and periodicity. Traditional information security risk assessment is mainly for data security carrier assets in the network environment. Setting evaluation items based on a certain standard as a benchmark and carrying out a relatively static and fixed risk assessment cannot meet the security assessment requirements of different environments and different goals in the data flow process, and the network security boundary is becoming increasingly blurred.

3.3 The coordination of the legal liability system is uneven

In my country, the "Data Security Law" has set up a special chapter on the investigation methods for violations of data security protection obligations to stipulate relevant legal responsibilities. However, in the process of implementing the legal responsibility for government data security protection, the coordination aspect and protection liability exemption clauses stipulated in the security regulations need to be clarified through more detailed implementation regulations [5].

4 Digital government builds a data security guarantee system

In order to effectively prevent the above possible security risks, the digital government needs to construct the security guarantee of the digital government from the aspects of constructing a classification and grading system for the whole process of government affairs data; improving the level of data security technology; improving data security laws and regulations; legalizing data open procedures, etc. system. See Fig.2. for details.

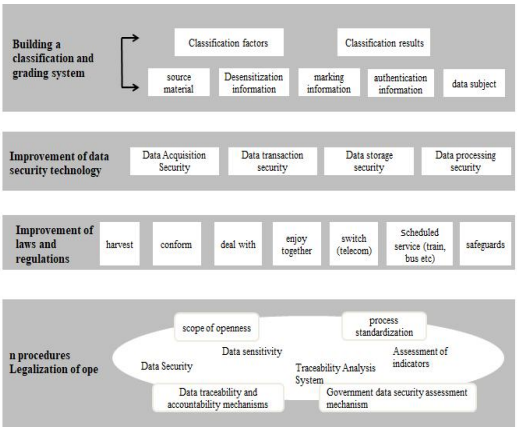

Fig. 2. Mechanism diagram of data security guarantee for digital government construction

4.1 Constructing a classification and grading system for the whole process of government affairs data

First, take the smallest data category as the classification object, comprehensively consider the classification factors and classification results, divide it into 1-5 levels, and finally combine the data open form and hierarchical management and control principles to form the implementation standards for data opening to the outside world. In terms of the nature of security, the nature of security is judged from four aspects: national security, public interest, citizen interest, and legal interests of enterprises. Second, the "data open format" is divided into original data, desensitized data, marked data, authenticity data and group data. In addition to the original data, the other four formats are data products formed by processing and processing the original data. Five types of data, the risk of their public format is from large to small and from small to large, the higher the data, the easier it is to be used.

4.2 Improving the technical level of data security

4.2.1 Data collection security.

Data collection security technology: Through the deployment of data collection systems or related tools, access control and access control are performed on data collection equipment, and a unified government data collection strategy is set at the same time. During the collection process, the authorization consent and information are logged, and technical means such as encryption, desensitization, and access control are used to prevent data leakage. Data source identification and recording: Use data collection identification and recording tools and data lineage management tools to sort out the government data collected by data collection equipment, analyze and mark the source and destination of government data, and form a security capability for blood lineage tracing with data flow as the main line.

4.2.2 Data transaction security.

There is a bilateral trust dilemma in data transactions, and establishing a trust relationship between data suppliers and demanders is the key to realizing data transactions. According to the analysis diagram of the overall architecture design, the network layer and the storage layer are located at the upper end of the overall architecture, respectively responsible for point-to-point communication and information recording tasks; the extension layer mainly includes SM2 algorithm, credit certificate, and data blocks, etc., and is responsible for providing information for the entire system. Multiple security mechanisms; service layer. It mainly includes log, cache, security and data verification, etc., aiming to provide support for various applications; the application layer aims to meet the needs of users and provide them with many functions such as interfaces, transactions, and member joining. See Fig.3. for details.

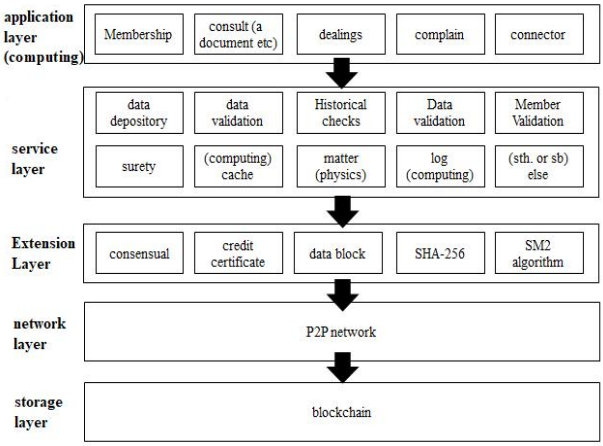

Fig. 3. The overall structure of the asset trading platform

Data transactions often involve the evaluation of the value of data assets. The income method estimates the value of data assets by predicting the benefits brought by them. This method is relatively easy to operate in practice. The basic calculation formula for its evaluation is:

$$P = \sum_{t=1}^{n} F_t \frac{1}{(1+i)^t}$$

Among them: P—appraisal value; Ft—the income amount of the data asset in the tth future income period; n—the remaining economic life; t—the future t year; i—the discount rate. According to the basic formula of the income method, on the basis of obtaining relevant information of data assets, according to the historical application situation and future application prospects of the data assets or similar data assets, combined with the business model of data asset applications, focus on the analysis of

the predictability of the economic income of data assets , considering the applicability of the income method.

4.2.3 Data storage security.

Data storage security is to protect the security of government affairs data during storage. Specifically include the following aspects:

Database encryption: Use the database encryption device to convert the plaintext data into ciphertext storage, decrypt and restore the original data when needed. Logical storage security: Regularly scan the security configuration of the business system, perform access control and monitoring on the storage system, and regulate user login and use of government data. Data backup and recovery: To back up the government affairs data, different levels and types of backup mechanisms are adopted to ensure the availability and integrity of the data.

4.2.4 Data processing security.

First, Data desensitization: Desensitization techniques include static and dynamic. Static desensitization technology is applied in non-production situations, using static desensitization systems or tools to desensitize and protect sensitive information in data; in scenarios where data is used in a production environment, use dynamic desensitization systems or The tool judges the requester based on information such as the role, authority, and level and type of the data being used, and desensitizes and protects sensitive information in the data in real time. Second, the data processing environment is safe: Use bastion hosts and testing equipment, use the data processing platform to manage them in a unified manner, and adopt strict access control, monitoring and auditing, and separation of duties to ensure the security of the government data processing environment of the government business platform system.

4.3 Improving data security laws and regulations

First, accelerate the introduction of regulations and policies related to digital government construction. Promulgate, formulate, and implement local regulations, local government regulations, or normative documents that are synchronized with the construction of digital government as much as possible, and the methods, scope, standards, security, Requirements and regulations have been made in terms of security and other aspects to effectively prevent public privacy leaks, information theft, user attacks, and data theft from occurring. Secondly, relying on the existing self-regulatory organizations of the Internet industry, all stakeholders can be encouraged to jointly formulate a code of conduct for the collection and use of personal information, conduct security assessment, testing and certification of information collectors such as platforms, and determine the standards for dividing the boundaries between data and information disclosure and non-disclosure , to determine the level of government data openness and use, so that it meets the platform protocol compliance [6].

4.4 Legalize data opening procedures and strengthen data security supervision

4.4.1 Statutory data open procedures.

The legalization of government data opening procedures needs to be mainly reflected in two aspects: defining the scope of opening and standardizing the process. The scope of government data opening is not static, and it is replaced and updated according to social development and the actual needs of the people; the norms and specific mechanisms of the government information disclosure process, including the classification of information disclosure and information acquisition [7]. The first is to comprehensively establish and improve the data classification and classification mechanism. The so-called data level is to divide the data level according to the security and sensitivity of the data. The second is to form a legalized government data acquisition mechanism. The process of government information disclosure and acquisition must be carried out in accordance with statutory procedures [8].

4.4.2 Strengthen the supervision of data security.

Mechanism for keeping data traces for future reference: In order to deal with the risk of missing data, it is necessary to build a whole-process data traceability analysis system for tracking, monitoring, prevention and improvement, so as to control the risk within an acceptable range. The digital rights subject develops and processes the data it designs and uses, and keeps traces of the collected and processed data [9].

Government data security assessment mechanism: In terms of evaluation indicators, evaluation indicators are the core content of evaluation. Government data security assessment should examine the four aspects of government data quality evaluation, openness, application and risk disposal at a macro level. The ultimate goal of government data security assessment is to guide and guide the smooth development of government data openness and sharing [10]. Through the evaluation, we can grasp the overall process, level and existing problems of government data openness, and timely discover and guide relevant entities to correct deviations in direction and practice, expand The demonstration effect of building a digital government, and finally through the establishment of a feedback mechanism for government data security assessment results, strengthens the function of government data security assessment to promote construction.

5 Conclusions

In recent years, digital government, as an important foundation of digital China and digital economy, has become an important strategic measure to enhance the country's modern governance capabilities and a powerful tool to promote the construction of a service-oriented government. Government data security is also closely related to my country's national sovereignty, security and development. Interests are closely related, but the current government data security is facing a complex and severe situation. This paper jumps out of the existing research on the three aspects of government data

security management, technology, and operation. Under the framework of digital government construction, data security and data development are combined to construct a classification and grading system for the entire process of government data; improve data security. Technical level; improve data security laws and regulations and legalize data open procedures, etc., and start to propose a guarantee system to provide a cornerstone guarantee for the construction of a national integrated government big data system.

Acknowledgment

This research was supported by Management Consulting Project of State Grid Corporation of China (Project's Number: 8117L0230001)

References

1. Hu, J., Qi, Y. (2023) Research on government data security governance system based on blockchain cross-chain mechanism [J/OL]. Modern Intelligence. https://kns.cnki.net/kcms2/detail/22.1182.G3.20230616.1437.004.html
2. Luo, L., Fan, W.F., Jin, J. (2021) Data dissemination issues and governance strategies in digital government construction [J]. Leadership Science, No.797(12): 18-20. DOI: 10.19572/j.cnki.ldkx.2021.12 .005.
3. Shao, J.J. (2020) The editorial department of this journal, Solidly promote the construction of digital governmen t [J]. Chinese Administration, No.424(10): 5.
4. Teng, H.Q., Wu, S.S. (2023) Research on the Government Data Security Guarantee System of Digital Government Construction in my country [J]. Exploration, No.281(02):88-97. DOI: 10.13996/j.cnki.taqu.2023.02 .012.
5. Wang, G.H., Guo, W.B. (2022) Multiple Risks Faced by Digital Government Construction and Their Avoidance Strategies [J]. Reform, No.337(03):146-155.
6. Wang, L. (2022) Countermeasure Research on Government Data Security Management [J]. Network Security Technology and Application, (02):78-80.
7. Wu, J.G., Luo, Z. (2022) E-government data anti-reptile solution [C]//China Network Security Industry Alliance. Proceedings of the 2022 Network Security Outstanding Innovation Achievement Competition. "Information Security Research" Magazine, 2022: 49-52 .DOI:10.26914/c.cnkihy.2022.026877.
8. Wu, S.P., Li, P., Zhang, Z.F. (2019) Design of Data Governance Framework in the Environment of Government Big Data [J]. E-government, (02): 45-51. DOI: 10.16582/j.cnki.dzzw.2019.02.005.
9. M. T H ,Felipe L R L . Cultivating Trustworthy Artificial Intelligence in Digital Government[J]. Social Science Computer Review,2022,40(2).
10. Isabel S . When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis[J]. Government Information Quarterly,2023,40(1).