Data Security Governance Practices under the Background of AI Era

Guisheng Na

Beijing Teret Certification Co., LTD., Beijing 100015

Abstract: ***As the world enters the "digital economy," big data has become the most significant production factor, and various big data application environments pose new demands on data security. Consequently, ensuring data security has become a topic of concern in numerous industries. This article aims to analyze the practice of data security governance and hopes to provide some assistance to relevant personnel.***

Keywords: Data security; Characteristic; Governance.

1. PREFACE

Currently, with the rapid development of technology and industry, the digital economy, which primarily utilizes data as a production factor, is experiencing rapid growth. It is profoundly transforming people's production and lifestyle patterns, and exerting a significant impact on economic and social development. In the digital economy, data serves as the foremost production factor, as well as the most fundamental and valuable asset. As data plays an increasingly important role, its security issues have become increasingly prominent, and their impact has extended from individuals and enterprises to industries, and even the entire country. Therefore, it is imperative to effectively manage data security. Diao et al. (2025) pioneered optimized Bi-LSTM networks for lung cancer detection accuracy [1], while Yuan (2025) developed contrastive multimodal learning for chest X-ray analysis using text-image fusion [8]. Complementary medical innovations include Xu's (2025) GCN-based healthcare facility sustainability optimization [9] and Liu et al.'s (2025) capsule neural network system for controlling spider-like medical robots [10]. Yang Jinzhu (2024) further enhanced medical knowledge extraction through LLM-knowledge graph integration [12]. Urban systems research features Li, Evans & Zhang's (2025) user-centered framework for smart city analytics [2] and Wang's (2025) predictive modeling for e-commerce logistics optimization [3]. Infrastructure innovations include Feng et al.'s (2025) green building renovation strategies [11] and Tu's (2025) reliable vehicle platooning via 5G link aggregation [15]. Industrial applications show Bohang et al. (2025) advancing image steganalysis through active learning [4], while Zhao et al. (2024) optimized steel production scheduling via deep learning [5]. Financial AI progresses with Yang, Lin, Xue & Wang's (2025) CNN-based stock sentiment prediction [6], Yang Jie et al.'s (2025) LLM-driven derivatives hedging [7], and Jiang et al.'s (2025) deep neural networks for personalized financial robotics [13]. Chen & Xie (2025) additionally demonstrated generative AI for augmented advertising decisions [14].

2. THE CONNOTATION OF DATA SECURITY

In the International Organization for Standardization, computer system security is defined as the technical and managerial security protections established and utilized for data processing systems, aimed at safeguarding computer hardware, software, and data from accidental and malicious impacts that could lead to damage, alteration, and leakage. Therefore, the security of computer networks can be defined as the utilization of various technical and managerial means to ensure the normal operation of network systems, thereby guaranteeing the availability, integrity, and confidentiality of information within the network [1]. Consequently, the goal of establishing network security protection is to ensure that the data transmitted and exchanged over the network does not experience phenomena such as addition, modification, loss, or leakage. Information security or data security encompasses two contradictory connotations: one is the security of the data itself, which is achieved through the use of "data confidentiality," "data integrity," and "two-way strong authentication"; the other is the security of data protection, which refers to actively protecting data through the use of "advanced data storage technology," such as ensuring data security through disk arrays, data backups, and off-site disaster recovery.

3. MAIN CHARACTERISTICS OF DATA SECURITY

3.1 Usability

The usability of data security is a user-centered design philosophy, the core of which is to enable users to design according to their own habits and needs. For example, in web design, it is important to avoid any tension or frustration for users when browsing the web, while also allowing users to achieve maximum effectiveness at minimal cost. Because of this, many countries in the world, including the United States and China, have been advocating for the free flow of information.

3.2 Completeness

One of the three fundamental aspects of data is information integrity, which refers to ensuring that information or data is not modified without permission during transmission and storage, or that any modifications can be promptly detected. In practical applications, it is often confused with confidentiality boundaries.

3.3 Confidentiality

Confidentiality, also known as secrecy, refers to the condition that the information of an individual or an organization cannot be disclosed to others. Many software applications in computers, including email software and web browsers, have settings related to confidentiality, which are designed to ensure the confidentiality of user information [2]. In addition, some spy files or hackers can also pose confidentiality issues.

4. BASIC SYSTEM OF DATA SECURITY GOVERNANCE

4.1 Purpose of data security governance

The goal of data security governance discussed in this article remains confined within one or multiple organizations. Measures related to data security management and control for important data or sensitive information are most commonly seen in the context of digital government, specifically in the data security governance of various government departments. This encompasses both the data security governance within individual departments and the data security management at the inter-departmental data sharing level. The objectives of data security governance are as follows.

(1) Purpose of data security compliance: To meet the requirements of various national, local, and industry-specific data security regulations.

(2) Purpose of data security governance and protection: To ensure data security, the management of data security covers the operational security of data within business systems, encompassing requirements for data reliability, data leakage prevention, and data misuse prevention [3].

(3) The purpose of data security control is to establish a system for data security control, encompassing both technical and management aspects, in order to safeguard the security of data and ensure the sustainable growth of data-driven businesses.

4.2 Institutional system for data security governance

This article proposes a framework for data security governance that integrates management, technology, evaluation, and operation. It conducts research on data security governance mechanisms from multiple perspectives, primarily encompassing technology, operation, management, and evaluation. The data security governance mechanisms primarily include the following aspects of data security governance practices:

(1) Guarantee of data security and related standard system for information security.

(2) Data security management technology: including discovering data, classifying data, dividing data into security levels, and implementing data security protection strategies.

(3) In assessing the effectiveness of data security governance, special attention should be paid to the evaluation results, and improvements should be made based on the conclusions drawn from the evaluation.

5. DATA SECURITY GOVERNANCE PRACTICES

5.1 Establish a data security governance system

5.1.1 Ensure effective organizational construction

It is necessary to establish a data security governance organizational structure that elaborates on the relevant responsibilities and specific requirements of the organizational teams involved in the business scope of data security governance. Therefore, at least the following data security governance organizational roles should be established:

(1) Data Security Decision-making Layer. It is composed of senior management or data security officers from the entire organization. It is responsible for the data security objectives and planning of the entire organization, resource support throughout the data security governance process, coordination and decision-making for major events, and ultimately bears the responsibility for the data security of the organization.

(2) Data security management layer. It is composed of management personnel from each specific business department within the organization, who are responsible for providing comprehensive guidance on the implementation of data security measures and decisions for that specific business department. This includes, but is not limited to, formulating data security management standards, organizing the development and implementation of data security technical solutions, organizing the development and implementation of data security incident monitoring and handling, data security vulnerability investigation and remediation, data security incident tracing and analysis, etc. [4].

(3) Data security supervision layer. It is composed of third-party personnel within an organization who have no subordinate relationship with the business department. Its main task is to monitor and audit the process and results of data security governance, thereby ensuring the effectiveness of the implementation by the data security governance organization.

5.1.2 Establish standardized systems

Data security management involves many standard systems, among which the most important ones are:

(1) Develop the "Data Security Management System", which stipulates the responsibilities and personnel for data security under each business model, and formulates relevant protective measures.

(2) The "Data Classification and Grading Standards" provides a detailed classification of various business data within enterprises, especially for personal and critical data, and assigns corresponding confidentiality levels.

(3) The "Data Security Management Specification" provides a detailed description of various types and levels of data, as well as a detailed elaboration on the collection, transmission, storage, processing, exchange, and destruction of data.

(4) The "Data Security Operation Management Specification" provides detailed descriptions of monitoring measures for data security risks, response and emergency handling measures for data security risks, investigation and recovery of data security vulnerabilities, as well as backup and recovery of data security.

5.1.3 Ensure adequate human resources

In addition to the relevant technical tools and products, data security governance also relies on corresponding personnel support. In organizational construction, the role of each data security governance organization should be clearly defined, with detailed responsibilities and assessment requirements. At the same time, to ensure that the data security business skills of staff are consistent with the requirements of data security governance, relevant personnel should be provided with skills training and career development planning [5].

5.2 Actively apply various data security governance techniques

5.2.1 Data security protection technology

An important measure for data security management is to adopt differentiated data security protection strategies for different levels of data, generally including data encryption, data desensitization, data access control, etc. In data security management, data security protection strategies must achieve security protection throughout the entire lifecycle of data, that is, based on the classification and level of data, data security protection should be controlled according to category and level to ensure that the same data security control measures can be taken at every stage of data flow. For example, when sharing data, if data from Department A is shared with Department B, Department B must adopt the same security control measures as Department A based on the type and level of its data.

5.2.2 Data discovery technology

The goal of data security management is data, so it is particularly important to accurately and effectively mine the core data required for data security management. So far, a lot of achievements have been made in research on static data, but there are still many technical challenges in mining and monitoring dynamic data, as well as in accurately identifying sensitive and important data of individuals [6]. Among them, the mining of dynamic data relies on data-related data, while the accurate identification of corresponding data relies on feature matching techniques such as regular expressions. However, existing technical methods still face issues such as false positives, false negatives, and system performance bottlenecks.

5.2.3 Data security operation technology

Data security operation is a crucial component of data security management, encompassing numerous specific techniques, among which data security status analysis and early warning reporting stand out as the most common technical means. The purpose of data security status analysis is to gather data pertaining to data security protection and data security risk management, and based on the impact of these data security statuses on data services, determine the level of danger, ensuring that high-risk security incidents can be addressed promptly. Data security status analysis also necessitates closed-loop tracking of data security statuses, implying that data security status managers must establish communication with data service personnel under data security statuses, thereby enabling emergency response to data services under basic security statuses. The objective of data security status analysis is to identify and report potential data security threats in data services based on data security vulnerability investigations and intelligence on data security threats, thus enabling effective prevention of data security threats in advance.

5.2.4 Data partitioning technology

Rational classification and grading of data is fundamental to data security governance. Different data security controls should be implemented for different types and levels of data. This approach can help prevent the application of uniform security measures to all data, thereby reducing overall data security management costs and enabling precise management of important data. The prerequisite for data classification and grading is the establishment of standards for data classification and grading. Next, data should be labeled according to its category and level. The challenge in implementing this technology lies in ensuring that data labeling can be performed without any impact on normal data operations as the data flows, and that the data labels are not discarded or tampered with during the data flow process.

5.3 Improve the data security governance evaluation system

The data security governance assessment mechanism is the most effective method to test the effectiveness of data security governance. It comprises two parts: one is the object of assessment and evaluation, and the other is the improvement and enhancement of results.

The main content of data security assessment measures includes: defining the objects to be assessed and the involved application systems and personnel, organizing the entire lifecycle process of data and the related data security technologies and management measures, analyzing the effectiveness of data security measures in each data flow link, and outputting the results. In addition, the DSMM standard can also serve as an important basis for data security assessment and evaluation. The 30 security process areas extracted from this standard basically cover every step in the entire data security assessment process, and the grading of the data security capability maturity model in the standard can also serve as an important basis for evaluation results.

In response to issues arising from data security assessment and evaluation, it is necessary to propose timely methods for improvement and enhancement. The work content includes: defining the responsible person for improvement and enhancement, formulating a plan and work schedule for data security improvement and enhancement, and auditing and summarizing the results after improvement and enhancement. If the development of data business is relatively stable, an assessment can be conducted once every quarter.

6. CONCLUSION

Overall, data is an important production factor, and the development and application of big data will play a positive role in promoting the development of China's digital economy. Throughout the entire data development process, there are various data security issues that must be taken seriously. Data security is no longer just a technical issue; it also involves multiple aspects such as law, policy, management, and talent theory. Therefore, it faces more new challenges, which requires people to deepen their understanding and strengthen scientific research and innovation in practical work.

REFERENCES

[1] Diao, Su, et al. "Optimizing Bi-LSTM networks for improved lung cancer detection accuracy." PloS one 20.2 (2025): e0316136.
[2] X. Li, L. Evans, and X. Zhang, “Interactive data exploration for smart city analytics: A user-centered perspective,” 01 2025.
[3] Wang, J. (2025). Predictive Modeling for Sortation and Delivery Optimization in E-Commerce Logistics.
[4] Bohang, Li, et al. "Image steganalysis using active learning and hyperparameter optimization." Scientific Reports 15.1 (2025): 7340.
[5] Zhao, H., Chen, Y., Dang, B., & Jian, X. (2024). Research on Steel Production Scheduling Optimization Based on Deep Learning.
[6] Yang, W., Lin, Y., Xue, H., & Wang, J. (2025). Research on Stock Market Sentiment Analysis and Prediction Method Based on Convolutional Neural Network.
[7] Yang, Jie, et al. "Dynamic Hedging Strategies in Derivatives Markets with LLM-Driven Sentiment and News Analytics." arXiv preprint arXiv:2504.04295 (2025).
[8] Yuan, J. (2025). Contrastive Multimodal Learning for Chest X-ray Analysis: Leveraging Text and Image Synergy. Authorea Preprints.
[9] Xu, Haoran. "Sustainability Enhancement in Healthcare Facility Design: Structural and Functional Optimization Based on GCN." (2025).
[10] Liu, Z., Jian, X., Sadiq, T., Shaikh, Z. A., Alfarraj, O., Alblehai, F., & Tolba, A. (2025). Efficient control of spider-like medical robots with capsule neural networks and modified spring search algorithm. Scientific Reports, 15(1), 13828.
[11] Feng, Zhang, et al. "Research on old building renovation strategies by using green building technologies." 2024 6th International Conference on Civil Architecture and Urban Engineering (ICCAUE 2024). Atlantis Press, 2025.
[12] Yang, Jinzhu. "Integrated application of llm model and knowledge graph in medical text mining and knowledge extraction." Soc. Med. Health Manag 5 (2024): 56-62.
[13] Jiang, Gaozhe, et al. "Investment Advisory Robotics 2.0: Leveraging Deep Neural Networks for Personalized Financial Guidance." (2025).
[14] Chen, Shujian, and Minhui Xie. "Augmenting Advertiser Decision Support with Generative AI and Interactive Analytics." (2025).
[15] Tu, Tongwei. "Reliable Vehicle Platooning via Redundant 5G Link Aggregation in Smart Roads." (2025).