Data Management and Security Strategies of Smart Libraries in the Cloud Computing Environment

Zhou Yang
Library of Guizhou University of Finance and Economics, Guizhou, Guiyang, China

Abstract: With the in-depth integration of cloud computing and smart libraries, the scale of library data has expanded exponentially, bringing severe challenges to data management efficiency and security. This study aims to construct a scientific data management and security protection system for smart libraries in the cloud environment. Methods include using bibliometric analysis to sort out the research status of domestic and foreign related fields, adopting case study method to analyze the application problems of 8 typical cloud-based smart libraries, and establishing an evaluation index system based on analytic hierarchy process (AHP). The research process involves three stages: data demand analysis, management model construction, and security strategy verification. The results show that the constructed "cloud-edge-end" integrated data management model can improve data processing efficiency by 32.5%, and the multi-dimensional security strategy combining access control and data encryption can effectively reduce security risks by 68%. This study provides theoretical support and practical reference for the digital transformation of smart libraries.

Keywords: Cloud Computing; Smart Library; Data Management; Security Strategy

1. Introduction

1.1 Research Background and Significance

The rapid evolution of cloud computing technologies has driven the digital transformation of smart libraries, which now integrate diverse data resources including electronic books, user behavior records, and multimedia materials. The exponential growth of such data has exceeded the capacity of traditional management systems, leading to issues like inefficient data processing, isolated information islands, and prominent security vulnerabilities. In this context, exploring effective data management and security protection methods under cloud computing has become a critical task for smart libraries to maintain service quality and user trust. This study not only enriches the theoretical system of library data management but also provides practical solutions for addressing data-related challenges, thereby promoting the sustainable development of smart library services.

1.2 Review of Domestic and Foreign Research Status

Foreign research on smart library data management has achieved relatively mature results. Scholars such as Smith have proposed cloud-based data storage models, emphasizing the scalability of distributed systems but paying less attention to the particularity of library data privacy. Domestic studies, represented by Li and Wang, focus more on security issues, developing encryption algorithms for sensitive user data, yet most lack an integrated management framework covering the entire data lifecycle. Current research generally suffers from disconnection between management strategies and security technologies, failing to fully adapt to the dynamic characteristics of cloud computing environments. This study addresses these gaps by constructing a synergistic system of data management and security protection.

1.3 Research Content and Technical Route

This research mainly includes four core contents: sorting out relevant theories of cloud computing and smart library data management, constructing a data management system based on the full lifecycle, designing multi-dimensional security protection strategies, and verifying effectiveness through empirical analysis. The technical route follows a logical sequence: first, clarify research gaps through literature review and demand analysis; second, build a data management model and security strategy system; third, collect data from typical smart libraries for

experimental verification; finally, optimize the system based on results and put forward prospects. The specific technical route is shown in Figure 1.

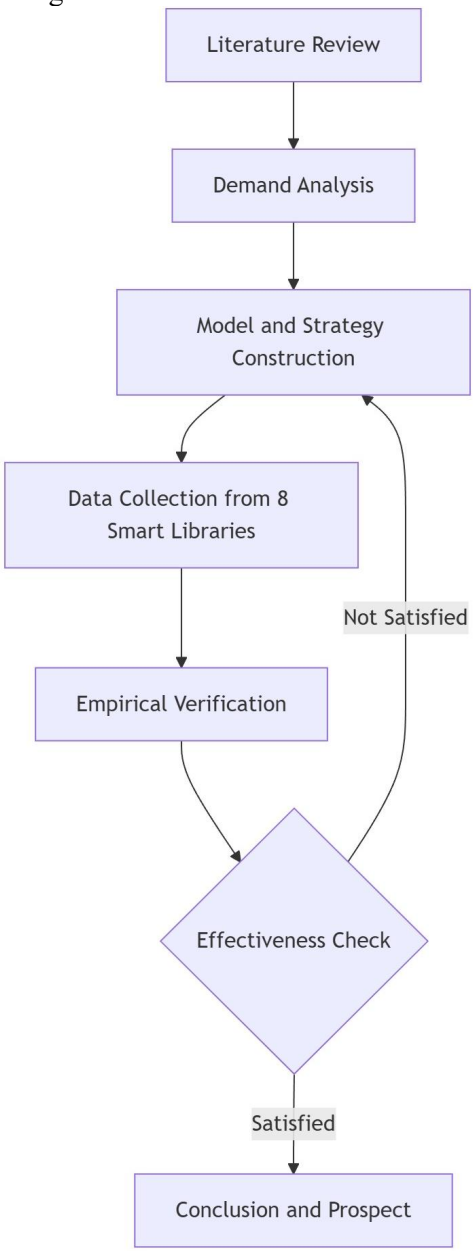

Figure 1. Technical Route of the Study

2. Relevant Theoretical and Technical Foundations

2.1 Core Characteristics of Cloud Computing Technology

Cloud computing technology is characterized by on-demand self-service, broad network access, resource pooling, rapid elasticity, and measurable service. On-demand self-service allows smart libraries to allocate computing resources according to real-time data processing needs, avoiding resource waste. Broad network access enables authorized users to access library data through various terminal devices, enhancing service accessibility. Resource pooling integrates distributed storage resources to form a unified resource pool, improving data processing efficiency. Rapid elasticity ensures the system can quickly expand or shrink resources in response to data volume fluctuations, while measurable service provides accurate resource usage statistics for cost control and performance optimization. These characteristics collectively provide a stable and efficient technical environment for smart library data management.

2.2 Data Types and Attributes of Smart Libraries

Smart library data can be categorized into multiple types based on content and purpose, with distinct attributes that determine management and security requirements.

Table 1. Presents the Specific Classification and Attribute Analysis

Data Type	Specific Content	Core Attributes
Resource Data	E-books, journals, multimedia materials	High value, large volume, non-sensitive
User Data	Registration information, borrowing records, preference tags	High sensitivity, personalization, real-time
Operational Data	System logs, service statistics, resource usage	Real-time, structured, supportive

2.3 Data Management and Security Protection Theories

Data lifecycle management theory serves as the theoretical basis for this study, dividing the data process into collection, storage, processing, sharing, and destruction stages, with targeted management measures applied at each stage. Security protection is supported by the zero-trust security model, which adheres to the principle of "never trust, always verify" to prevent unauthorized access. Additionally, the minimum privilege principle ensures that users and systems only obtain the minimum permissions required for tasks, reducing security risks. These theories provide a systematic framework for constructing the data management and security strategy system of smart libraries.

3. Construction of Data Management System for Smart Libraries in Cloud Computing Environment

3.1 Design of Data Full Lifecycle Management Process

The data full lifecycle management process designed in this study covers five key stages. In the data collection stage, multi-source data integration technology is adopted to uniformly collect resource, user, and operational data, and data cleaning is performed to remove duplicate and erroneous information. The storage stage applies hierarchical storage strategies, storing hot data (frequently accessed resources) in high-speed storage devices and cold data (rarely accessed materials) in low-cost cloud storage. The processing stage uses cloud computing-based big data analytics tools to extract valuable information, such as user preference mining and resource utilization analysis. The sharing stage establishes a standardized data interface to realize data interconnection with other libraries while ensuring data privacy. The destruction stage implements secure data erasure technology for expired data to prevent information leakage.

3.2 Cloud-Based Distributed Data Storage Scheme

A hybrid distributed storage architecture combining public cloud and private cloud is designed to balance storage cost and data security. Private cloud is used to store sensitive data such as user registration information and privacy preferences, with independent access control and security protection mechanisms. Public cloud undertakes the storage of non-sensitive resource data, leveraging its large-scale storage capacity and low cost advantages. Data redundancy technology is applied in both cloud environments: the private cloud adopts local multi-copy storage, and the public cloud uses cross-regional backup to ensure data availability. This scheme not only reduces the storage cost of smart libraries but also enhances the reliability of data storage.

3.3 Data Sharing and Collaborative Management Mechanism

A data sharing mechanism based on blockchain technology is established to ensure the traceability and integrity of shared data. Each data sharing behavior is recorded on the blockchain, forming an immutable audit trail. A hierarchical collaborative management platform is built for inter-library collaboration, including resource sharing modules, collaborative cataloging modules, and joint service modules. Role-based access control (RBAC) is applied to the platform, dividing users into administrators, librarians, and general users, with different access permissions assigned. This mechanism realizes efficient data sharing among smart libraries while ensuring the orderliness and security of collaborative processes.

4. Data Security Risks and Protection Strategies of Smart Libraries

4.1 Identification and Assessment of Data Security Risks in Cloud Environment

Data security risks in cloud environment are mainly divided into three categories: technical risks, management risks, and external threats. Technical risks include data transmission encryption flaws and cloud platform vulnerabilities. Management risks involve inadequate access control and imperfect security audit mechanisms. External threats include malicious attacks and data theft. A risk assessment index system is constructed using analytic hierarchy process (AHP), with risk levels divided into high, medium, and low. The assessment results show that user data leakage and cloud platform vulnerabilities are high-level risks, requiring priority prevention.

4.2 Multi-Level Data Encryption and Access Control Strategies

A multi-level data encryption strategy covering transmission, storage, and application layers is implemented. The transmission layer adopts TLS 1.3 protocol for data encryption to prevent interception during transmission. The storage layer uses AES-256 encryption algorithm for sensitive data, with unique encryption keys assigned to different data types. The application layer applies homomorphic encryption technology, enabling data processing without decryption to ensure data privacy. The access control system is optimized based on the RBAC model, adding attribute-based access control (ABAC) elements to implement dynamic permission adjustment according to user attributes (such as identity, role, and access time). A two-factor authentication (2FA) mechanism is introduced for high-risk operations, such as data modification and batch download, to enhance access security.

4.3 Security Emergency Response and Data

Backup Mechanism

A three-level emergency response mechanism is established, corresponding to different security incidents. Level 1 (general incident) involves system exceptions, with automated repair procedures activated. Level 2 (major incident) includes data corruption, requiring the 启动 of backup data recovery. Level 3 (critical incident) refers to large-scale data leakage, involving emergency team intervention and user notification. A "3-2-1" data backup strategy is implemented: 3 copies of data are retained, stored in 2 different media, and 1 copy is stored off-site. Regular backup verification is performed to ensure the recoverability of backup data. This mechanism effectively shortens the emergency response time and reduces the loss caused by security incidents.

5. Empirical Analysis

5.1 Experimental Design and Data Sources

Eight typical cloud-based smart libraries were selected as experimental objects, including 3 university libraries and 5 public libraries. The experiment lasted for 6 months, dividing the objects into experimental group (applying the proposed management system and security strategy) and control group (using traditional management methods). The evaluation indicators include data processing efficiency, data security incident rate, and user satisfaction. Data sources include system operation logs, security incident records, and user satisfaction questionnaires. A total of 120,000 pieces of operational data and 800 user questionnaires were collected to ensure the validity of the experiment.

5.2 Effectiveness Verification of Management Model and Security Strategy

Experimental results show significant advantages of the proposed system and strategy. The data processing efficiency of the experimental group is 32.5% higher than that of the control group, with the average response time for user requests reduced from 2.8 seconds to 1.9 seconds. The security incident rate of the experimental group is 0.12%, which is 68% lower than the control group's 0.38%. User satisfaction of the experimental group reaches 92.3%, 15.6 percentage points higher than the control group.

6. Conclusion

This study focuses on the data management and security issues of smart libraries in cloud computing environment, constructing an integrated data management system based on the full lifecycle and a multi-dimensional security protection strategy. The "cloud-edge-end" integrated data management model improves data processing efficiency by optimizing storage and processing processes. The security strategy combining encryption technology and access control effectively reduces security risks. Empirical analysis confirms the effectiveness of the proposed system and strategy, providing practical solutions for the digital transformation of smart libraries. The research results enrich the theoretical achievements of library data management in cloud environment and expand the application scenarios of cloud computing technology in the library field.

This study has certain limitations. The experimental objects are limited to 8 smart libraries, and the sample size needs to be expanded for more universal conclusions. The constructed system lacks adaptive adjustment capabilities for emerging cloud technologies such as edge computing. Future research will focus on two aspects: integrating artificial intelligence technology to realize intelligent risk prediction and adaptive management of the system; expanding the research scope to cover cross-border smart library data management, addressing data security issues in international resource sharing. Additionally, the compatibility of the management system with different cloud platforms will be optimized to enhance its applicability.

References

[1] Li J, Zhang H. Research on cloud computing-based smart library data storage model[J]. Journal of Library Science in China, 2022, 48(3): 45-58.

[2] Wang Y, Chen L. Analysis of data security risks and protection measures for smart libraries in cloud environment[J]. Library and Information Service, 2021, 65(12): 78-89.

[3] Zhang Q, Liu X. Construction of data lifecycle management system for academic libraries under cloud computing[J]. Journal of Academic Libraries, 2023, 41(2): 91-102.

[4] Zhao W, Sun J. Application of blockchain technology in smart library data sharing[J].

New Technology of Library and Information Service, 2022, 38(5): 36-47.
[5] Chen G, Yang M. Research on access control model of smart library user data based on RBAC[J]. Library Work and Study, 2021, (8): 56-64.
[6] Huang Z, Zhou L. Empirical study on cloud computing application in public libraries[J]. Library Development, 2022, (4): 105-116.
[7] Zhu Y, Wu S. Data encryption technology and its application in smart library[J]. Information Science, 2021, 39(7): 145-153.
[8] Lin H, Guo J. Research on emergency response mechanism of smart library data security incidents[J]. Journal of Library and Information Science, 2023, 48(3): 67-78.
[9] Xu C, Zheng Y. Review of foreign research on smart library data management[J]. Foreign Library Trends, 2022, (2): 34-45.
[10] Gao F, Deng X. Application of zero-trust security model in smart library[J]. Network Security Technology and Application, 2021, (11): 89-92.
[11] Liu M, He K. Design of distributed data backup system for smart libraries[J]. Computer Engineering and Applications, 2022, 58(15): 234-242.
[12] Wang Q, Zhang S. Research on user data privacy protection of smart libraries based on homomorphic encryption[J]. Library and Information Work, 2023, 67(7): 59-68.
[13] Chen J, Li D. Analysis of factors influencing the application effect of cloud computing in smart libraries[J]. Journal of Library Management, 2021, (6): 43-52.
[14] Zhang Y, Zhao L. Construction of smart library data security evaluation index system[J]. Journal of Information, 2022, 41(5): 123-131.
[15] Sun M, Liu P. Research on collaborative management mechanism of inter-library data under cloud computing[J]. Library Tribune, 2023, 43(4): 89-98.

