Postprint: Security Assurance Architecture and Prevention and Control Measures for Cloud Storage of Academic Information Resources

Authors: QIU Rongrong, Hu Changping, Feng Yafei

Date: 2023-08-27T00:00:00+00:00

Abstract

[目的/意义] Information security constitutes a critical influencing factor for cloud storage of academic information resources. Effective information security assurance architectures and prevention and control measures can provide recommendations for cloud storage service providers to improve their storage services, and can also serve as a reference for users in selecting cloud storage service platforms. [方法/过程] Based on security requirement analysis for cloud storage of academic information resources, this study constructs a security deployment architecture and a security operation architecture for cloud storage of academic information resources, and investigates prevention and control measures for cloud storage security of academic information resources from five dimensions: application security assurance, content security assurance, data security assurance, virtualization security assurance, and infrastructure security assurance. Specifically, application security assurance encompasses four aspects: user identity authentication, user identity management, access control, and application and interface security; content security assurance comprises two aspects: content security detection and content security control; data security assurance includes five aspects: data encryption, data integrity verification, data deterministic deletion, data disaster recovery backup and restoration, and data migration; virtualization security assurance consists of three aspects: security domain isolation, user data isolation, and multi-tenant management; infrastructure security assurance covers three aspects: cloud storage facility security, physical environment security, and network security. [结果/结论] The security deployment architecture provides a reference for the secure deployment of cloud storage of academic information resources, the security operation architecture reveals the security assurance elements and processes for cloud storage of academic information resources, and the security prevention and control measures provide technical strategies for security assurance for cloud storage of academic information resources.

Full Text

Preamble

Research on Security Assurance Framework and Control Measures for Academic Information Resources Cloud Storage

Qiu Rongrong, Hu Changping, Feng Yafei
School of Information Management, Wuhan University, Wuhan 430072

Abstract

[**Purpose/Significance**] Information security is a critical factor affecting cloud storage of academic information resources. An effective information security assurance framework and control measures can provide recommendations for cloud storage service providers to improve their services and offer references for users when selecting cloud storage platforms. [**Method/Process**] Based on security requirement analysis for academic information resource cloud storage, this study constructs a security deployment framework and a security operation framework for academic information resource cloud storage. It investigates prevention and control measures from five perspectives: application security assurance, content security assurance, data security assurance, virtualization security assurance, and infrastructure security assurance. Application security assurance includes user identity authentication, user identity management, access control, and application program and interface security. Content security assurance encompasses content security detection and content security control. Data security assurance comprises data encryption, data integrity verification, data assured deletion, data disaster backup and recovery, and data migration. Virtualization security assurance includes security domain isolation, user data isolation, and multi-tenant management. Infrastructure security assurance covers cloud storage facility security, physical environment security, and network security. [**Result/Conclusion**] The security deployment framework provides a reference for secure deployment of academic information resource cloud storage. The security operation framework reveals the security assurance elements and processes. The security prevention and control measures provide technical strategies for ensuring academic information resource cloud storage security.

1. Introduction

In the era of big data, the diversification of data formats, complexity of data structures, and high-speed growth have led to continuously increasing demands for digital information resource storage space and rising complexity of storage forms. Cloud storage, characterized by low cost, convenience, easy management, high scalability, and elastic configuration, offers a new storage approach for the growing volume of massive digital information resources. Its widespread enterprise application has also provided a platform and practical space for rapid development and application. For academic information resources, cloud storage provides a new preservation model that well meets their evolving digital

preservation needs. However, frequent security incidents at Google, Amazon, Apple, and other cloud storage providers in recent years have constrained the rapid industry development of cloud storage. As an important component of digital information resources, academic information resources also face information security challenges during cloud storage.

Through comparative analysis of security requirements between traditional IT-mode academic information resource storage and cloud-based storage, several critical security issues emerge. In traditional IT environments, academic information resources are stored in institution-owned facilities or personal devices with clear physical boundaries, fixed and relatively independent. In cloud computing environments, the elastic and on-demand allocation of storage resources creates dynamically changing security boundaries that cannot be effectively demarcated. Academic information resource management systems no longer have clear physical boundaries or dedicated storage devices. Consequently, resources can only reside within logically bounded information management systems. A key security challenge involves integrating geographically dispersed academic information resources to form logically independent storage areas, currently addressed primarily through virtualization technology.

Since academic information resource cloud storage represents a service rather than traditional data storage, users must access cloud storage resources via networks. Providing secure access interfaces and preventing unauthorized access to cloud-based academic information resources constitute important aspects of security assurance. In traditional IT environments, data owners retain control over their data, managed by themselves or professionals. In cloud storage environments, resource owners lose data control, making cloud service providers critical security stakeholders with potential access privileges. Vulnerabilities in provider security policies or malicious insider operations can trigger security issues, substantially increasing information security risks. Furthermore, compared to other digital information, academic information possesses characteristics of professionalism, precision, and high innovative value, imposing higher requirements on accuracy, integrity, and usefulness. With diverse sources, academic information resources may contain non-compliant content, sensitive information, or even illegal content that could severely affect quality. Ensuring content professionalism and precision thus represents a significant challenge for academic information resource cloud storage security.

2. Research Status

Both domestic and international researchers have extensively studied storage security issues for academic information resources. International projects include the digital archive management system prototype CLOCKSS (Lots of Copies Keep Stuff Safe), the digital information resource storage system DPN, Stanford University' s LOCKSS system, DuraSpace' s DuraCloud, the preservation-aware storage service system PDSCLOUD, and the Dark Archive In The Sunshine State (DAITSS) digital archive information system. These systems employ

distributed preservation with multiple backups: CLOCKSS uses different preservation patterns across regions to ensure digital resource integrity; DPN stores data copies at least two geographically separate nodes with different storage structures to prevent catastrophic loss from technical, organizational, or natural disasters; LOCKSS employs Opinion polls mechanisms to regularly compare and monitor identical data across multiple nodes; DuraCloud stores user data across different cloud providers while ensuring synchronized updates across all copies and monitors data health and integrity to enhance consistency, security, and reliability; PDSCLOUD utilizes heterogeneous storage and computing platforms from different cloud providers to offer OAIS (Open Archival Information System) services, ensuring understandability of long-term preserved digital content amid dynamic preservation and technological changes; DAITSS implements multiple offsite backups and ensures long-term availability and integrity through secure storage, backup, updating, and migration; V. J. Sosa-Sosa et al. proposed a file storage architecture for private/hybrid cloud environments and compared fault tolerance and availability across replication technologies; K. Tang proposed a disaster recovery model for cloud-based digital libraries to ensure security and service continuity.

Domestic research primarily focuses on theoretical studies. Liu Wanguo et al. proposed a national digital academic information resource security assurance system framework from a collaborative management perspective, comprising policy layers, data layers, and cloud service platform layers under national policy and regulation protection. They also developed a hierarchical preservation model for digital academic resources from a tiered preservation perspective, covering four aspects: digital academic resource existence and preservation environment maturity, hierarchical standard systems (technical, format, value, responsibility, and other standards), lifecycle-based long-term preservation level strategies (priority, general, temporary, and other preservation levels), and long-term access services. Chen Chen et al. proposed a four-layer secure cloud storage architecture for digital libraries based on security requirement analysis, including an access layer (providing convenient interfaces for personalized services), application interface layer (developing different service interfaces for secondary application development and user authentication/authorization), basic management layer (managing storage facilities, data processing, and security assurance including encryption and disaster backup), and storage layer (integrating distributed storage resources with unified management logic and interfaces). Li Shuangshuang et al. proposed a five-layer security architecture for academic information resource cloud storage, including an access layer (account management, identity authentication, and authorization), application interface layer (network virtualization and security deployment for different service models), infrastructure layer (physical security boundaries), virtualization layer (virtualization technology for multi-tenant software and data sharing security), and data center layer (encryption and protection against tampering/attacks). Hu Changping et al. studied security prevention and control measures for domestic and international academic information resource cloud storage services, examin-

ing data security controls (secure transmission protocols, static data encryption, authentication, access control, regular integrity checks) and disaster recovery measures (avoiding data lock-in, multi-copy offsite storage) across transmission, storage, and exit phases. Xu Guolan researched digital library cloud storage security through hierarchical key generation and allocation strategies for access control, attribute-based encryption algorithms, and virtualization security technologies for physical/logical isolation. Jing Dongke employed data fragmentation, block encryption, and self-healing mechanisms to ensure university library cloud storage security. The China Academic Library & Information System (CALIS), with its three-tier organizational structure (national center, regional centers, and member libraries), ensures academic information resource security through hierarchical management and distributed storage: member libraries (university libraries) deploy infrastructure and preserve catalog information, full-text databases, and user information; regional centers aggregate catalog and user information from member libraries, integrate academic information, and develop cloud service platforms based on member library APIs to reduce security risks while enabling secure resource sharing; the national center integrates all member library information through regional centers to provide unified cloud services, allowing users to access academic information from all member libraries through either the national portal or regional center portals.

3. Security Assurance Architecture for Academic Information Resource Cloud Storage

Academic information resources include reliable digital resources such as academic achievements (digital journals, dissertations, monographs, conference papers, reports), research data, and some network information resources. For instance, university library academic information resources comprise not only professional databases from information service providers but also characteristic academic resource databases (e.g., Wuhan University' s doctoral and master' s dissertation database, surveying abstract database), library catalog information, e-books, teaching videos, and learning software. Given the importance of these resources and their varying information security requirement levels, secure deployment and operation are critical for ensuring academic information resource cloud storage security. Based on security level protection and hierarchical protection concepts, this study constructs a security deployment framework from a cloud deployment perspective and a security operation framework from an implementation perspective.

3.1 Security Deployment Framework for Academic Information Resource Cloud Storage

Due to copyright or research confidentiality requirements, academic information resource cloud storage necessitates different security levels. By security level, academic information resources can be categorized into three tiers: general, relatively high, and very high security levels. Higher security levels entail greater

cloud storage costs and stronger information security assurance capabilities. By deployment model, cloud storage can be divided into public, hybrid, and private cloud storage, with information security assurance capabilities increasing progressively. Therefore, resources with different security levels can be stored in corresponding clouds: general security resources in public clouds, relatively high security resources in hybrid clouds, and very high security resources in private clouds with the highest assurance capabilities. Considering that resource security levels may change over time, requiring potential public-private cloud permission changes, the security deployment must ensure different cloud types can achieve interoperable security through security control management (e.g., user identity and permission management) and SLA formulation [Figure 1: see original paper].

3.2 Security Operation Framework for Academic Information Resource Cloud Storage

Analysis of security issues reveals that academic information resource cloud storage security assurance involves application, virtualization management, infrastructure, data, and content aspects. The security operation hierarchical framework primarily consists of four layers (user layer, application layer, management layer, storage layer) and five components (cloud storage application security, virtualization security, infrastructure security, data security, and content security). The elements and logical relationships are illustrated in Figure 2 [Figure 2: see original paper]. Application security refers to user access security and application/interface security during secure user-cloud storage interactions. Prevention and control measures include user identity authentication, user identity management, access control, and application/interface security. Content security ensures the safety of data content stored in the cloud, including content security detection and control. Data security, the core objective of cloud storage security assurance, includes data encryption, data integrity verification, data assured deletion, data disaster backup and recovery, and data migration. Virtualization security addresses security issues in logically unifying dispersed storage resources through virtualization technology, with measures including security domain isolation, user data isolation, and multi-tenant management. Infrastructure security covers cloud storage facility security, physical environment security, and network security, with cloud service providers responsible for infrastructure security in their offerings.

The secure cloud storage process for academic information resources comprises three stages: securely uploading resources to the cloud, ensuring stored resource security, and secure data destruction after service termination. Specifically, users log into the system via clients, upload resources after secure access authorization, and the system performs content security analysis. Upon passing content detection, the system decomposes resources into data packets with unique identifiers, encrypts and backs them up, and generates secure migration versions. The virtualization management module distributes packets to dispersed, hetero-

geneous cloud storage devices that have logically implemented security domain isolation and user data isolation. After storage, data integrity is regularly verified while ensuring facility, physical environment, and network security. Upon service termination, data assured deletion and migration security are guaranteed.

4. Security Prevention and Control Measures for Academic Information Resource Cloud Storage

Based on security requirements and the constructed operation framework, this section analyzes prevention and control measures across five dimensions: application security assurance, content security assurance, data security assurance, virtualization security assurance, and infrastructure security assurance.

4.1 Application Security Assurance

Unlike traditional storage, cloud storage is an outsourced service model requiring remote access. Application security thus encompasses user access security and application/interface security. Traditional access security addresses security during data storage on trusted devices, whereas cloud storage environments involve users and storage devices in different trust domains. Insider attacks or malicious server control can cause unauthorized data usage, making access security more complex. Cloud storage access security measures primarily include identity authentication, user identity management, and access control. Identity authentication verifies whether the subject' s real identity matches the claimed identity to prevent unauthorized use. User identity management implements strict role-based classification to address the complexity of numerous user types and relationships. Access control restricts access permissions to prevent unauthorized use when users retrieve cloud data and ensures authorized data collection by applications. Application and interface security ensures software security, secure application development/testing, and effective API security to prevent threats from vulnerabilities or malware.

4.2 Virtualization Security Assurance

Cloud storage environments feature dynamic security boundaries, dispersed and heterogeneous hardware facilities, and scenarios where multiple users share physical devices. Virtualization must provide secure domains and effective user/data management to ensure logical storage area and subject security, achieved through security domain isolation, user data isolation, and multi-tenant management. Security domain isolation creates relatively stable, independent network environments for specific cloud storage or applications through network isolation and virtual firewalls, preventing compromised domains from affecting others. User data isolation primarily through virtual machine isolation prevents unauthorized access to other users' virtual machines on the same physical host when one virtual machine is breached. Multi-tenant

management addresses security issues in multi-tenant mode through tenant registration, classification, and virtual resource allocation measurement, ensuring tenants of different levels and categories obtain appropriate virtual resource permissions.

4.3 Infrastructure Security Assurance

Infrastructure security assurance provides a secure and reliable hardware environment for cloud storage system operation, including cloud storage facility security, physical environment security, and network security. Storage facility security ensures that system operations and human factors do not damage hardware components, servers, or other physical computing resources. Physical environment security ensures storage locations and sensitive information areas are safe and reliable, capable of resisting natural disasters (earthquakes, floods, fires) and implementing physical security boundaries with unauthorized access prohibition. Network security ensures network transmission security, primarily concerning switch, router, and data packet-level security in the cloud storage system' s network environment.

4.4 Data Security Assurance

The cloud storage model separates data ownership and management rights, increasing security risks such as academic information resource leakage and loss. Cloud service providers can access and search stored resources, and attackers may breach providers to obtain user data. To ensure security, data encryption, integrity verification, assured deletion, disaster backup/recovery, and migration security are crucial measures. Data encryption employs symmetric and asymmetric encryption during cloud storage, generating different ciphertexts based on algorithms and keys to prevent plaintext acquisition if data is stolen or leaked. Data integrity verification detects whether resources are damaged during transmission or storage, representing an important security measure. Data assured deletion ensures complete removal of resources confirmed for deletion by owners. Data disaster backup/recovery performs offsite backups with regular updates to enable effective restoration after damage. Data migration security ensures resources can be securely migrated and exported in standardized formats for future import into other cloud storage services.

4.5 Content Security Assurance

With diverse sources and complex cloud storage environments where information dynamically binds to publishing carriers making server locations difficult to trace and massive data flows challenging for online content review, academic information demands high professionalism and precision. Ensuring content security to provide users with accurate, effective knowledge requires detection, control, and standardization of academic information resources. Content security detection identifies non-compliant content (political, health, confidentiality, privacy, property, protection-related), sensitive information, and illegal content,

primarily through content filtering (keyword-based and semantic-based). Content security control prevents content-based usage, destruction, and attacks. Preventing content-based usage protects intellectual property through watermarking or copy prohibition. Preventing content-based destruction eliminates malicious virus codes within content.

5. Conclusion

Through analysis of academic information resource cloud storage security requirements, this study constructs security deployment and operation frameworks to provide a secure and reliable system model. It analyzes prevention and control measures across five dimensions: application security, virtualization security, infrastructure security, data security, and content security. The limitation lies in presenting only theoretical frameworks and measures without practical system implementation or specific control application research.

References

[1] Fu Yingxun, Luo Shengmei, Shu Jiwu. Survey on secure cloud storage systems and key technologies[J]. Journal of Computer Research and Development, 2013, 50(1): 136-154. [2] CLOCKSS[EB/OL]. [2018-05-01]. https://clockss.org/clocksswiki/files/CLOCKSS_{{{Handout}}}_{{Chinese}}}.pdf. [3] DPNCore[EB/OL]. [2018-05-01]. http://dpn.org/about. [4] LOCKSS Preservation Principles[EB/OL]. [2018-05-01]. https://www.lockss.org/about/principles/. [5] Features[EB/OL]. [2018-05-01]. http://www.duracloud.org/details/features. [6] Rabinovici-Cohen S, Marberg J, Nagin K, et al. PDSCLOUD: long-term digital preservation in the cloud[C]//CAMPS B E L L R, LEI H, MARKL V. Proceedings of the 2013 IEEE international conference on cloud engineering. Redwood City CA: IEEE, 2013: 38-45. [7] Caplan P. Building a Dark Archive in the Sunshine State: a case study[C]//SOCIMAGING SCI&TECHNOL. Archiving 2005 final program and proceedings. Washington DC: Society for Imaging Science and Technology, 2005: 9-13. [8] Sosa-Sosa V J, Hernandez-Ramirez E M. A file storage architecture for private cloud/hybrid cloud computing environments and digital libraries[J]. Information technology & libraries, 2012, 31(4): 34-45. [9] Tang K. Research on disaster recovery model of cloud-based digital library[J]. Applied mechanics and materials, 2013, 336(1): 2134-2137. [10] Liu Wanguo, Sun Bo, Liu Ding, et al. Current status and countermeasures of natural science academic achievement loss in China—based on statistical analysis of 2015 National Natural Science Award preliminary evaluation winners' academic papers[J]. Library and Information Service, 2016, 60(20): 20-26, 35. [11] Liu Wanguo, Zhou Xiuxia, Huang Ying. Research on hierarchical preservation model construction for digital academic resources[J]. Information and Documentation Services, 2018(2): 43-47. [12] Ma Xiaoting, Chen Chen. Research and implementation of digital library cloud storage application system[J]. Library Theory and Practice, 2012(5): 8-13. [13] Li Shuangshuang, Hu Changping. Security assurance for digital academic infor-

mation resource cloud storage[J]. Digital Library Forum, 2017(7): 8-13. [14] Hu Changping, Wang Lili. Research on foreign cloud storage service security for digital academic resources[J]. Information Studies: Theory & Application, 2018, 41(3): 156-160. [15] Xu Guolan. Research on security and prevention of cloud storage in digital library applications[J]. Modern Information, 2012, 32(4): 57-59. [16] Jing Dongke. Countermeasures for basic storage layer architecture security issues in university library cloud storage[J]. Research on Library Science, 2014(1): 38-41. [17] Wang Yuding, Yang Jiahai, Xu Cong, et al. Survey on cloud computing access control technologies[J]. Journal of Software, 2015, 26(5): 1129-1150. [18] Zhang Yuqing, Wang Xiaofei, Liu Xuefeng, et al. Survey on cloud computing environment security[J]. Journal of Software, 2016, 27(6): 1328-1348. [19] Feng Chaosheng, Qin Zhiguang, Yuan Ding. Cloud data security storage technology[J]. Chinese Journal of Computers, 2015, 38(1): 150-163. [20] Li Hui, Sun Wenhai, Li Fenghua, et al. Survey on data security and privacy protection techniques in public cloud storage services[J]. Journal of Computer Research and Development, 2014, 51(7): 1397-1409. [21] Fu Yingxun, Luo Shengmei, Shu Jiwu. Survey on secure cloud storage systems and key technologies[J]. Journal of Computer Research and Development, 2013, 50(1): 136-145. [22] Wei L F, Zhu H J, Cao Z H, et al. Security and privacy for storage and computation in cloud computing[J]. Information sciences, 2014, 258(10): 371-386. [23] Lei Wanyun. Information security defense: enterprise information security construction strategy and practice[M]. Beijing: Tsinghua University Press, 2013: 164-165.

Author Contributions: Qiu Rongrong designed the research and wrote the paper; Hu Changping guided and revised the paper; Feng Yafei revised the paper.

Keywords: academic information resource; cloud storage; security assurance framework; security control measures

Note: Figure translations are in progress. See original paper for figures.