Comprehensive Security Assurance Mechanism for Academic Information Resource Sharing in Cloud Computing Environments (Postprint)

Authors: Shi Yu, Hu Changping

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] To construct a comprehensive security assurance mechanism for academic information resource sharing in cloud computing environments from both technical and managerial perspectives, thereby guiding the implementation of security assurance for sharing.
[Method/Process] By analyzing the sharing process and security elements of academic information resources in cloud computing environments, the design of a comprehensive security assurance mechanism for academic information resource sharing is carried out.
[Result/Conclusion] Constructs a technical security assurance mechanism based on the academic information resource sharing process and an organizational mechanism for security assurance of academic information resource sharing based on multi-stakeholder collaboration.

Full Text

Preamble

Vol. 63 No. 3
February 2019
ChinaXiv Partner Journal

Comprehensive Security Guarantee Mechanism for Academic Information Resource Sharing in Cloud Computing Environments

Shi Yu, Hu Changping
School of Information Management, Wuhan University, Wuhan 430072

Abstract

[**Purpose/Significance**] This paper constructs a comprehensive security guarantee mechanism for academic information resource sharing in cloud computing environments from both technical and management perspectives, thereby guiding the implementation of sharing security guarantees. [**Method/Process**] Through analyzing the sharing processes and security elements of academic information resources in cloud computing environments, this paper designs a comprehensive security guarantee mechanism for academic information resource sharing. [**Result/Conclusion**] The paper proposes a security technology guarantee mechanism based on the academic information resource sharing process, and a security guarantee organization mechanism for academic information resource sharing based on multi-agent collaboration.

Keywords: cloud computing environment; academic information resource sharing; security guarantee mechanism
Classification Number: G251
DOI: 10.13266/j.issn.0252-3116.2019.03.007

In cloud computing environments, the methods of academic information resource sharing have undergone significant changes, and security issues in each link of academic information resource sharing services have become increasingly complex. Traditional security guarantee strategies can no longer ensure the smooth progress of academic information resource sharing in cloud environments. Addressing this situation, this paper combines the characteristics of cloud computing environments with those of academic information resources to construct a security guarantee mechanism for academic information resource sharing from both technical and management perspectives, based on an analysis of the sharing processes and their security elements in cloud computing environments. Regarding the technology guarantee mechanism, it is necessary to construct a full-process technical guarantee mechanism based on the sharing service implementation process, covering security in resource release, organization, utilization, and revocation, to ensure the availability, confidentiality, and integrity of resources at each sharing stage. Regarding security guarantee organization, the paper utilizes the concept of multi-agent collaboration to construct an organizational mechanism for academic information resource sharing security, identifying various security guarantee agents and their positioning, and ensuring academic information resource sharing security through efficient collaboration among all parties.

1. Academic Information Resource Sharing Process and Security Elements in Cloud Computing Environments

Thorough analysis of the academic information resource sharing process and its security elements in cloud computing environments forms the foundation for constructing a security guarantee mechanism for academic information resource sharing. This section organizes the implementation process of academic

information resource sharing in cloud computing environments and analyzes the security elements and their interactions during the sharing process.

1.1 Implementation Process of Academic Information Resource Sharing in Cloud Computing Environments

The implementation process of information resource sharing refers to the process by which information resources flow from their owners to users through certain media [1]. In cloud computing environments, academic information resource sharing is concentrated on cloud platforms. Academic information resource owners upload shared resources from local storage to cloud platforms, which organize the resources, and users then utilize the shared resources on these platforms. The specific process is shown in Figure 1 [Figure 1: see original paper].

Overall, the academic information resource sharing process in cloud computing environments encompasses the entire process from resource owners initiating sharing to users utilizing the resources, including initiating academic information resource sharing, organizing shared resources in the cloud, utilizing shared resources, modifying shared resources, and revoking or deleting shared resources. First, resource owners initiate academic information resource sharing. The shared resources include not only academic resources such as academic literature and scientific research data, but also various software tools, user-shared knowledge information, and partial personal information involved in the scientific research process. Sharing methods may involve users uploading and simultaneously setting resources as shared, or setting existing private resources in the cloud platform as shared resources. During sharing, the scope and permissions of sharing must be clearly defined. Second, cloud platforms manage and organize shared resources, including associating and organizing stored resources, storing shared academic information resources, and performing deduplication during storage. Third, in the utilization stage, academic information resource utilization in cloud computing environments occurs primarily within the cloud platform, with utilization methods becoming faster and more efficient. Users can obtain required shared resources through search and browsing services provided by the platform, and utilize them through methods such as transfer, online browsing, and editing. Finally, in the modification, revocation, or deletion stage, modifications to shared resources are generally performed by resource owners or authorized users within the cloud platform. After modification, the scope and permissions of resource sharing must be redefined. Additionally, resource owners can revoke sharing or delete resources according to their needs. When shared resources are revoked to private status or deleted by owners, sharing links simultaneously become invalid. Cloud platforms can also control the dissemination scope and perform associated deletions of other copies according to owners' requirements to protect intellectual property rights.

1.2 Security Elements and Their Interactions in Academic Information Resource Sharing

Vulnerability, security threats, and guarantee measures are three types of elements that directly affect information security [2]. In cloud computing environments, academic information resource sharing fully utilizes the powerful computing capabilities and rapid scalability advantages of cloud computing, demonstrating characteristics of resource concentration, process flexibility, and service reliability during sharing—providing unified, stable, and efficient services for resource release, acquisition, and modification on cloud platforms. However, in its security implementation process, it still faces influences from these three elements. Meanwhile, security guarantee objects and security guarantee subjects directly affect the formation of these three elements. Therefore, when analyzing security elements and their interactions, this paper focuses on analyzing the influence of security guarantee objects and security guarantee subjects.

Vulnerability generally refers to links that may be attacked by attackers and cause security incidents, typically determined by security guarantee objects and their security requirements. As shown in Figure 2 [Figure 2: see original paper], academic information resource sharing security guarantee subjects may be sources of vulnerabilities and security threats. For example, when security awareness is insufficient, operational errors occur, or management is inadequate, vulnerabilities and security threats arise. Simultaneously, security guarantee measures are generally implemented by security guarantee subjects, with shared resource owners and cloud service providers cooperating to develop security measures targeting vulnerabilities and threats during the academic information resource sharing process. Security guarantee objects are the main sources of vulnerabilities, with their characteristics and security requirements determining vulnerability. When security threats bypass or break through protective measures and attack vulnerabilities in certain links of the academic information resource sharing process, security incidents occur. To prevent such incidents, security guarantee measures can be applied at vulnerable links to counter targeted attacks.

From the preceding analysis, we can conclude that academic information resource sharing security guarantees must start from vulnerabilities and security threats, analyze vulnerabilities and threats at each stage of the sharing process, and apply security measures. Corresponding security measures must fully consider the timing of security attacks and their impacts, deploying comprehensive arrangements—namely, arranging preventive measures against security attacks, taking timely measures to identify attacks and prevent incidents and damages, and establishing targeted solutions to ensure rapid recovery of shared resources and services after incidents. Meanwhile, when deploying security measures at each stage, a security guarantee organization mechanism combining technology and management must be adopted. In terms of technology, deployed security measures should focus on defense, selecting targeted and effective defense technologies for identified vulnerabilities and threats to avoid similar incidents, while

employing monitoring measures and disaster recovery management for undiscovered threats and vulnerabilities to prevent incident escalation. In terms of management, since security guarantee subjects are diversified in cloud environments, multi-agent collaborative management must be emphasized to ensure smooth implementation of academic information resource sharing. These insights provide design ideas for security guarantees of academic information resource sharing in cloud computing environments, which will serve as the basis for the following discussion on security guarantee mechanisms.

2. Security Technology Guarantee Mechanism Based on Academic Information Resource Sharing Process

Based on the academic information resource sharing process in cloud computing environments and the analysis of security elements and their interactions, security measures are deployed at each sharing stage to form a security technology guarantee mechanism based on the sharing process, as shown in Figure 3 [Figure 3: see original paper].

2.1 Resource Sharing Release Security Mechanism

When academic information resource owners release resources for sharing, security technology guarantee mechanisms can be employed to ensure security, including academic information resource content security detection mechanisms, resource secure transmission mechanisms, and information resource ownership verification mechanisms. User-initiated shared academic information resources come from diverse sources, including personal knowledge summaries or internet-based materials. When compiling internet materials, users may include confidential content or malicious code that requires detection before resource sharing. The academic information resource content security detection mechanism primarily ensures that shared academic information resources do not involve sensitive information concerning national defense, economy, or people's livelihood, while also ensuring that shared resources are not embedded with malicious code to prevent security intrusions when users utilize shared resources [9]. Although users initiate academic information resource sharing for mutual exchange and efficient utilization, protection of resource owners' intellectual property rights must also be ensured to avoid infringement, such as unauthorized secondary distribution or modification. Therefore, during resource release, an information resource ownership verification mechanism must be established to identify resource owners and issue ownership certificates, ensuring resource security in cloud platforms [10]. Additionally, during resource transmission, building dedicated network transmission channels is costly and difficult to implement. Therefore, general networks typically adopt academic information resource secure transmission mechanisms to establish encrypted communications between parties, ensuring data transmission confidentiality.

2.2 Cloud Shared Resource Organization Security Mechanism

Shared resources stored in cloud platforms should adopt reasonable association organization mechanisms to ensure security during storage. Corresponding academic information resource security technology guarantee mechanisms include multi-copy association mechanisms and deduplication mechanisms. Shared resources differ significantly from ordinary resources owned by single users during storage. Ordinary resources in private storage or cloud platforms belong to users and their storage and modification are determined individually. However, shared resources' access and editing are jointly determined by multiple parties, and other authorized users may further share, download, or transfer shared resources. Consequently, multi-copy files commonly exist for academic information resources in cloud platforms. The multi-copy problem not only increases cloud platform storage overhead and user difficulty in resource selection, but also causes shared resources to escape owners' constraints and control, such as losing control over access time and objects, creating intellectual property disputes. Therefore, controlling the multi-copy phenomenon is necessary. During shared resource storage, deduplication mechanisms can control the number of copies [11-12]. The number of shared resource copies should relate to application scope and quantity—when many users request shared resources, copy quantity can be appropriately increased to improve processing efficiency. Simultaneously, multi-copy association mechanisms manage multi-copy resources in cloud platforms, ensuring orderly storage organization of academic information resources and guaranteeing shared resource security [13].

2.3 Cloud Shared Resource Utilization Security Mechanism

The resource utilization stage is a crucial link in academic information resource sharing. Security issues at this stage include shared resource unavailability, unauthorized users illegally obtaining resource information, illegal tampering with shared resources, and user permission revocation security. Without control, these issues adversely affect resource sharing security. Therefore, resource secure transmission mechanisms, access control mechanisms, and academic information resource secure dissemination mechanisms can be employed for control. The secure transmission mechanism is identical to that during resource release, ensuring integrity and confidentiality during transmission. Academic information resource sharing in cloud environments can be either wide-ranging or limited-scope. If users access resources beyond their authority or modify shared resources without authorization, security incidents may occur. Therefore, fine-grained access control mechanisms must be designed. Access control is an important user identity management method for providing effective and secure resource access, allowing users with different needs to access authorized information through unified methods, preventing unauthorized access, and providing centralized digital identity management and authentication [14-15]. Cloud environment access control mechanisms can ensure user identity security, helping cloud service providers verify user authenticity and legitimacy, gener-

ally completing authorization for different users during account registration and verifying identity through submitted login information. The academic information resource secure dissemination mechanism primarily protects intellectual property rights of resource owners and prevents mining of related sensitive information during propagation, mainly implemented through user permission control.

2.4 Shared Resource Revocation Security Mechanism

Shared resource revocation is the final stage in the academic information resource sharing process. This stage primarily employs academic information resource multi-copy association mechanisms and shared resource deterministic deletion mechanisms to ensure security. When academic information resource owners complete sharing and revoke shared resources, their intellectual property rights should be protected by implementing associated deletion operations for all copy resources according to owners' requirements. The academic information resource multi-copy association mechanism acts after shared resources are revoked by owners, with cloud platforms using related technologies to process copy files of shared resources, deleting all copies and backup files. Since cloud service providers store shared resources uniformly, when stored data is deleted, providers allocate corresponding storage space to other tenants, potentially allowing new tenants to recover original cloud storage data. Additionally, original data backups may not be deleted immediately, leading to leakage of academic information resource sharing resources. Therefore, deterministic deletion mechanisms are required to ensure that no institution or individual, including cloud service providers, can recover data when shared resources are revoked [16]. Implementation can be based on the confidentiality level of shared resources.

3. Multi-Agent Collaborative Security Guarantee Organization Mechanism for Academic Information Resource Sharing

Academic information resource sharing security guarantees must adapt to diversified guarantee subjects. In traditional IT environments, academic information resource sharing occurred within various academic information resource service institutions, with security guarantees also relying on these institutions. In cloud computing environments, some security guarantee measures are transferred to cloud service providers for unified deployment, and resource utilization processes also shift to the cloud, involving cloud service providers and resource users in security guarantees. Therefore, in cloud computing environments, academic information resource sharing security guarantee organizations involve multi-agent collaboration, forming a multi-agent collaborative security guarantee organization mechanism, as shown in Figure 4 [Figure 4: see original paper].

3.1 Collaborative Subjects and Their Positioning in Academic Information Resource Sharing Security Guarantees

Various subjects in academic information resource sharing security guarantees include shared resource owners, cloud service providers, and shared resource users. Among them, shared resource owners hold a dominant position in sharing security guarantees, while cloud service providers and users participate as collaborators.

Shared resource owners are ultimately responsible for academic information resource sharing security. Therefore, during security guarantee organization, owners should fully exert their leading role, establishing technical and management specifications for sharing security, and ensuring smooth security guarantees through collaboration with cloud service providers and users. Shared resource owners consist of academic information resource service institutions and ordinary users. Academic information resource service institutions include commercial academic information service institutions, public libraries, university libraries, and scientific and technical information centers, with resources primarily comprising standardized academic papers, research data, and tool software. Ordinary users complete academic information resource sharing by uploading resources to cloud platforms, including personal knowledge summaries and experimental data. When exercising their leading role, owners must clearly define the scope and system of academic information resource sharing security management, including security strategy formulation, security risk assessment and content, risk control objectives and method selection, while considering cloud computing environment impacts to develop security technology guarantee mechanisms and management approaches for cloud-based academic information resource sharing.

Cloud service providers and shared resource users participate as collaborative security guarantee subjects in academic information resource sharing security guarantees from multiple aspects. Cloud service providers participate directly by deploying security measures, while users primarily participate by ensuring their own account security, utilizing permissions properly, and conducting various forms of security supervision. Cloud service providers possess relatively complete technical resources and management capabilities, serving as collaborative institutions in academic information resource sharing security guarantees that directly participate in security implementation. Specific work includes ensuring basic environment security for sharing services and shared resource security during the sharing process. Basic environment security includes physical environment, hardware, virtualization, network, transmission, service subject accounts, and business sustainability security, with specific requirements determined by service conditions and cloud service types. Shared resource security during the sharing process primarily involves resource organization and personnel management from a service perspective, using combined technical and management measures to standardize operation processes and organizational storage of shared resources in cloud platforms, ensuring sharing process secu-

rity. Additionally, cloud service providers should proactively support shared resource security management controls, including providing management operation guidelines, offering security protection tools to resource owners, and conducting account security monitoring and anomaly alerts.

Shared resource users, referred to as users in academic information resource sharing cloud platforms, are the final destination of shared resources. In shared resource security guarantees, users must not only focus on ensuring their own account security and avoiding leaking personal information or using identical passwords across multiple accounts, but also pay attention to proper permission utilization and not abusing permissions by lending accounts to others. Since users are generally the first to discover various security problems, they typically participate as supervisors in academic information resource sharing security guarantees, including reporting security issues to cloud service providers and resource owners.

3.2 Collaborative Mechanisms for Academic Information Resource Sharing Security Guarantees

The collaborative mechanism for academic information resource sharing security guarantees is a multi-agent collaborative mechanism under the leadership of shared resource owners, including collaboration between owners and cloud service providers, owners and users, and between cloud service providers and users.

Regarding collaboration between shared resource owners and cloud service providers, security guarantees are conducted through division of labor, with each deploying security measures. Owners should supervise cloud service providers' security guarantee work from both management and technical perspectives. When security incidents occur, comprehensive cause analysis should be conducted first, followed by responsibility determination. Additionally, owners and providers must establish efficient security issue communication mechanisms. In security guarantee practice, some security measure deployments and incident handling require cooperation. To optimize work efficiency, response and cooperation mechanisms should be improved to facilitate timely security issue communication and avoid incidents.

Regarding collaboration between shared resource owners and users, users' permissions are limited, so they do not directly guarantee shared resource security. However, as direct users of shared resources and services, users can more comprehensively perceive various security issues. Therefore, while ensuring user account and permission utilization security, collaborative mechanisms should be established between owners and users to encourage proper supervision of security guarantee measures through appropriate channels, enabling timely discovery and resolution of security issues.

Regarding collaboration between cloud service providers and users, user feedback mechanisms can be established. When encountering problems, users can

report to cloud service providers through specific channels such as dedicated feedback platforms, complaint emails, or online customer service. After obtaining user feedback on various security issues, cloud service providers should respond promptly to prevent incidents or expansion.

References

[1] Wen Tingxiao, Chen Nenghua. Research on information resource sharing and its social coordination mechanism [J]. Journal of Library Science in China, 2007, 33(3): 78-81.

[2] National Information Security Standardization Technical Committee. Information security technology - Information security risk assessment specification: GB/T20984-2007 [S]. Beijing: Standards Press of China, 2007.

[3] Jithin R, Chandran P. Virtual machine isolation [M]// Nezpez G, Thampi M, Kor, et al. Recent trends in computer networks and distributed systems security. Berlin: Springer, 2014: 91-102.

[4] Birjem N, Challagidad DPS, Goudar RH, et al. Cloud computing review: concepts, technology, challenges and security [J]. International journal of cloud computing, 2017, 6(1): 32-57.

[5] Jiang Jie. Cloud data security risks and regulatory framework [J]. Information and Documentation Services, 2013(1): 57-60.

[6] Zhang Yuqing, Wang Xiaofei, Liu Xuefeng, et al. Survey on cloud computing environment security [J]. Journal of Software, 2016, 27(6): 1328-1348.

[7] Ali M, Dhamotharan R, Khan E, et al. SeDaSC: secure data sharing in clouds [J]. IEEE systems journal, 2017, 11(2): 395-404.

[8] Wang Yuding, Yang Jiahai, Xu Cong, et al. Survey on cloud computing access control technology [J]. Journal of Software, 2015, 26(5): 1129-1150.

[9] Liu Meiyan, Huang Gaijuan. Research on text filtering model for information content security [J]. Journal of Chinese Information Processing, 2017, 31(2): 126-131.

[10] Barsoum AF, Hasan MA. Provable multicopy dynamic data possession in cloud computing systems [J]. IEEE transactions on information forensics & security, 2017, 10(3): 485-497.

[11] Yang C, Ren J, Ma J. Provable ownership of files in deduplication cloud storage [J]. Security and communication networks, 2015, 8(14): 2457-2468.

[12] Xiong Jinbo, Zhang Yuanyuan, Li Fenghua, et al. Research progress on secure data deduplication in cloud environments [J]. Journal on Communications, 2016, 37(11): 169-180.

[13] Xiong Jinbo, Shen Weiwei, Huang Yangqun, et al. Secure multi-copy data sharing and associated deletion scheme in cloud environments [J]. Journal on

Communications, 2015, 36(S1): 136-140.

[14] Xu S, Yang G, Mu Y, et al. Secure fine-grained access control and data sharing for dynamic groups in cloud [J]. IEEE transactions on information forensics & security, 2018, 13(8): 2101-2113.

[15] Song Guofeng, Liang Changyong. A cloud security access control model based on user behavior trust [J]. Chinese Journal of Management Science, 2013(S2): 669-676.

[16] Feng Guilan, Tan Liang. Cloud storage data deterministic deletion scheme based on trust value [J]. Computer Science, 2014, 41(6): 108-112.

Author Contributions

Shi Yu: Designed the research plan and wrote the paper.
Hu Changping: Proposed the research question, guided the research, and revised the paper.

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