

Information Security and Intellectual Property Protection of Digital Library under the Background of Cloud Computing

Li Zhangchun^{1, a}

¹China West Normal University Library, Nanchong City, Sichuan Province, 637000, China

^aemail

Keywords: Cloud Computing; Digital Library; Information Security; Intellectual Property Protection

Abstract. Cloud computing will not only make profound changes of digital library occur in the aspects of software environment, hardware storage, application platform and service pattern, but also leave information resources faced with a lot of security issues. Cloud computing will greatly improve the service patterns and functions of digital library, and bring challenges to the library, in which the security issue is the core of its success. In this paper, based on the author's learning and practical experience, we firstly analyzed the issues of information security of the digital library in the cloud computing environment, and then put forward the strategies of intellectual property protection of the digital library in the cloud computing environment.

Introduction

Cloud computing technology, an emerging and highly acclaimed technology, has received high praise from industry participants once introduced. Cloud computing is Google's new Internet application mode, and the realization of computer science concepts such as distributed processing, parallel processing and grid computing on the Internet. With the development of Web 2.0 technology, digital library has adopted more ideas and technologies of Web 2.0 to improve its services, expand advanced complex network applications, and move towards the Library 2.0. Therefore, the use of cloud computing mode as the underlying architecture of digital library can greatly improve library services in the aspects of software environment, application platform and data sharing, which is the most cost-effective, reliable and scalable solution. However, if the cloud computing wants to have a good prospects at the stage of early application, there are a lot of premature and questionable issues, in which the information security is of particular importance. We must seriously think about the security risks brought by the cloud computing in order to respond to the possible challenges in a timely manner.

1 Information Security Issues of Digital Library in Cloud Computing Environment

1.1 Safeguards provided by cloud service providers

The first issue is how to ensure the security and usability of users' information resources. Although the "cloud" can guarantee the high reliable services via the measures such as data multi-copies fault-tolerance and interchangeable computing nodes, it is revealed from the related reports that several network failure incidents such as the disruption of Amazon S3 services and Google Apps (online office application software), global outages of Gmail mailboxes, and breakdown of Microsoft's cloud computing platform Azure for about twenty-two hours have a relationship with the application of cloud computing, which make anxiety and doubt about the security and availability of cloud computing were generated again in the majority of insiders and users who are still in the "clouds".

The second one is how to provide standards, norms and risk-sharing services for the users. If we carefully study the Amazon cloud service contract, it will be found that a lot of terms are unreasonable. For example, it is regulated in section 7.2 that: "We are not responsible for any unauthorized access or the use, destruction, deletion, disposal or loss of any contents or application programs." In the contract, the service provider is not committed to bear any legal responsibility or obligation for the data leakage and sabotage behaviors. It can be seen that, currently, due to lack of security models and standards of cloud computing architecture, cloud computing service providers may be able to avoid most of the security risks, and pass the risk to the users.

The third one is how to obtain the users' trust. Trust issue is a big obstacle in the development of cloud computing. Professor Jin Hai from Huazhong University of Science and Technology claimed that the cloud computing was not easy to be popular. He mentioned that people would put their money into the bank, because the bank is state-owned. The bank has the government's legal guarantee. However, there is not any credible third-party guarantee in the system for data security in data center of the cloud computing vendor. Therefore, the users do not dare put the data into the operators' data center."

1.2 Information security requirements of digital library in the cloud environment

1.2.1 Secure storage of data resources

The greatest concern of the library on cloud computing is the security of data resources. Once the data such as bibliographic data, readers' data, circulation data or E-books and special collections database are lost, the consequences would be disastrous. Our data and program are not on the machine in our library in cloud computing environment. How can the accidental loss, damage, illegal collection, processing and use of the data be avoided? How can it be ensured that the "cloud" still exists and we have the normal access to the data in the library tomorrow? The most basic requirement is to guarantee the absolutely safe data.

1.2.2 Intellectual property protection

Intellectual property issues in the era of digital library not only remain, but also have new changes in the cloud era. After the library purchases the cloud computing service, the data will be sent to the cloud, and the cloud computing enterprises escrow these data. Theoretically, the users should have full ownership of the escrowed data. However, in reality, cloud computing enterprises know very well about the "data core" principle. Therefore, they will do everything possible to use these data, and ensure the legalization of the use of users' data in the name of data integration, data mining and knowledge services. In recent years, OCLC has developed some new products by using integrated collection data in World-Cat, such as the quarterly recommended bibliographies of university and research libraries, whose definition of intellectual property rights will become a new problem.

1.2.3 Data confidentiality requirements

After the data of library readers, borrowing and finance are sent to the cloud computing service providers, the control of confidentiality belongs not to the library, but to the cloud computing service providers. With the diversity of information service, the required confidential information in the cloud computing environment will possibly appears in all aspects of the collection, transmission, processing, utilization, storage and dissemination of the whole information services, which will seriously threaten the information security of the library. Although each cloud computing provider emphasizes the use of encryption technology to protect users' data, it only refers to the fact that the data is transmitted with encryption on the network, and the data protection in the process of processing, storage and dissemination is still

not resolved.

1.2.4 Users' rights management

Users' rights denotes the specific operations which can be carried out by the legitimate users. After the users log into the digital library in the cloud environment, the available operations are browsing, searching, downloading, creating and updating (including modifying and deleting). However, not every user can do all the operations, and different users will have different authorities. In the cloud environment, the library is still responsible for the creation, update and integration of library data such as the update of a large number of readers' data each year, maintenance of bibliographic data and library collection and ordering information needed to be submitted at any time, which requires that the cloud computing environment can conduct reasonable authority division and management for ordinary users, librarians and cloud computing service providers to guarantee data security.

1.2.5 Access management control

The purpose of access management control is to ensure that the library information resources are not illegally accessed and used. Cloud computing environment is very attractive to the hackers, because the cloud itself not only has stored a variety of resources, but also provides convenient conditions for the hiding of malicious software. Given the high complexity of the cloud environment, it is inevitable to give some opportunities to the hackers. The hackers can steal users' information or destroy the stored information including various data in the library via seeking for the security vulnerabilities of the cloud environment. Therefore, the related effective measures must be taken.

2 Strategies of Intellectual Property Protection of Digital Library in Cloud Computing Environment

2.1 The necessary technical safeguards

In order to prevent the unauthorized use of the copyright owner's resources, and protect the interests of information owners and users, the necessary technical measures need to be used to guarantee the information security. The first one is common basic control measures such as the limitation of use times, use methods, download words and use time. The second one is the access control technology such as setting up the access IP address and the password. The users with access to the IP address are restricted, and the password is set up. When the users want to access the network, they need to input the corresponding password. The third one is encryption and key management technological pattern. The encryption techniques are used to prevent the network information from being stolen and destroyed during the process of transmission. In this manner, the sender and the receiver need to use the decryption key to obtain the relevant information of the cipher text while the third party cannot obtain the related information content, which is the most common encryption pattern. Its completion through the use of hardware in the network link layer and physical layer can prevent the information in the system being deciphered, which can guarantee the information integrity and confidentiality.

2.2 Improve the relevant legal system

The library, an information communication organization, is the main channel for the public to obtain the information resources. The legal rights and interests of the library should be protected by the relevant laws, which needs to formulate and perfect the relevant legal system. The legalization of the library system has three meanings: the first one is the special legislation of the library, the second one is the library-related legal system, and the third one is the

library-related international law and practice.

Faced with the constant change of the digital library, the relevant laws and regulations are lagging behind, and difficult to keep up with the needs of the development of the situation. Therefore, the construction of digital library is a technical problem. Additionally, with the development of the Internet, it poses a greater challenge to managers, which needs the joint efforts of the library community and the legal community to continuously explore and formulate the corresponding intellectual property protection system so that the intellectual property protection of the digital library really have laws and rules to follow. Only if the laws and regulations, administrative regulations, normative documents and methods related to the development of the library are fully utilized, can we not only bring the active role of the library into full play, but also protect the various powers and interests in the process of sharing the resources, which can make the digital library develop in a healthy and orderly direction.

Summary

Cloud computing will not only greatly improve the digital library service patterns and functions, but also bring challenges to the library, in which the security issue is the core of its success. Reasonable and complete library security framework for cloud computing must fully consider interests and their relevance of the library, users, cloud computing providers, and the third party audits, and rationally allocate security attributes in order to solve security issues of this complex giant system.

References

- [1] FAN Min. Application and bottleneck problem of cloud computing in digital library [J]. *Modern Information*, 2012, (02): 147-150.
- [2] LIU Dan. Intellectual property risk and prevention countermeasures of digital library in cloud computing environment [J]. *Chinese Journal of Medical Library and Information Science*, 2015, (03): 23-25.
- [3] TAO Rui, TU Yunjie. Research on digital library security service in cloud computing environment [J]. *Lantai World*, 2015, (05): 100-101.
- [4] XU Xinqiao, LIU Hua, XU Li. Literature review of cloud computing in domestic libraries [J]. *Library Science Research*, 2015, (02): 17-21+34.
- [5] LI Chaofeng. Construction of digital library information security system under cloud computing environment [J]. *Henan Science and Technology*, 2012, (11): 54-55.
- [6] LIU Lijuan. Management and service of digital library under the cloud computing mode [J]. *Journal of Library Science*, 2013, (05): 99-101.
- [7] GENG Lili, ZHOU Peng, SONG Xiaodan. Study on library development strategy in cloud computing environment [J]. *Library*, 2012, (06): 42-46.