TEST Engineering & Management

July - August 2020
ISSN: 0193-4120 Page No. 6101 - 6108

The Construction of a Computer-based Cloud Library Intelligent Service Platform

Lei Sun[1,*], Yingxia Li[2] and Yuli Lu[1]
[1]The First Affiliated Hospital, Hebei North University, Hebei, China, 075000
[2]HeBei University of Architecture, Hebei, China, 075000

Article Info
Volume 83
Page Number: 6101 - 6108
Publication Issue:
July - August 2020

Article History
Article Received: *25 April 2020*
Revised: *29 May 2020*
Accepted: *20 June 2020*
Publication: *28 August 2020*

Abstract

With the continuous development of cloud computing technology, library management has gradually introduced cloud computing technology, but due to its openness, there are still hidden security risks in operation. This paper builds a cloud library intelligent service platform based on KMI technology, which can effectively meet the needs of user authentication, secure access, data confidentiality, data retrieval, and security auditing, and can meet the basic needs of cloud library operation.

Keywords: *Public Library, Cloud Library, Visit Control, KMI, Cloud Computing;*

1. Introduction

With the continuous development of Internet technology, cloud computing technology has gradually become the hotspot and focus of computer industry research[1-2]. Cloud computing is the optimized interaction and use of IT resources, that is, end users can customize corresponding methods and configuration content on-demand, instant, personalized, and autonomously through network media to obtain the required cloud system hardware, platform, software, and service resources. The cloud resource operating environment can be divided into two types: public cloud and private cloud[3]. Because the cloud computing service model has the capabilities of supercomputing, high storage, efficient resource allocation, high-end network transmission, etc., it also has resource pool management that is safe, efficient and easy to dynamically expand and elastically carry, giving users great selectivity and deployment Space[4]. At present, mainstream cloud computing services can be divided into IaaS (infrastructure as a service) such as Huawei Cloud, Alibaba Cloud, etc., PaaS (platform as a service), SaaS (software as a service) three models. The continuous and in-depth application of cloud computing has also brought revolutionary changes to the library industry, such as ensuring high concurrent search and retrieval of books by users, and stable searching of electronic documents[5-6].

Although cloud computing helps to build a smart library, realize the sharing of document resources in a local area, and at the same time share cooperative services between each other. However, it is worth noting that it is precisely because of the open and cooperative nature of cloud computing that it also brings hidden dangers of insecurity to smart libraries. Therefore, it is necessary to use cloud computing to achieve convenient and high-quality services for users, but also to ensure the rights and obligations of libraries, document providers, and users.

This paper aims to solve the security problems in the operation of the cloud library intelligent service platform, construct a cloud library security access control platform design scheme based on KMI technology, and improve the cloud library system construction.

2. Cloud library application model

2.1. IaaS platform architecture

IaaS refers to the flexible delivery of IT infrastructure (servers, computing resources, storage resources, network resources, databases, memory, I/O equipment, etc.) and IT basic resources of cloud data centers through the network to users according to user resource requests, and The cloud service provider is responsible for the management, maintenance and upgrade of the IaaS platform, and the user pays the corresponding cloud service model based on the resource usage.

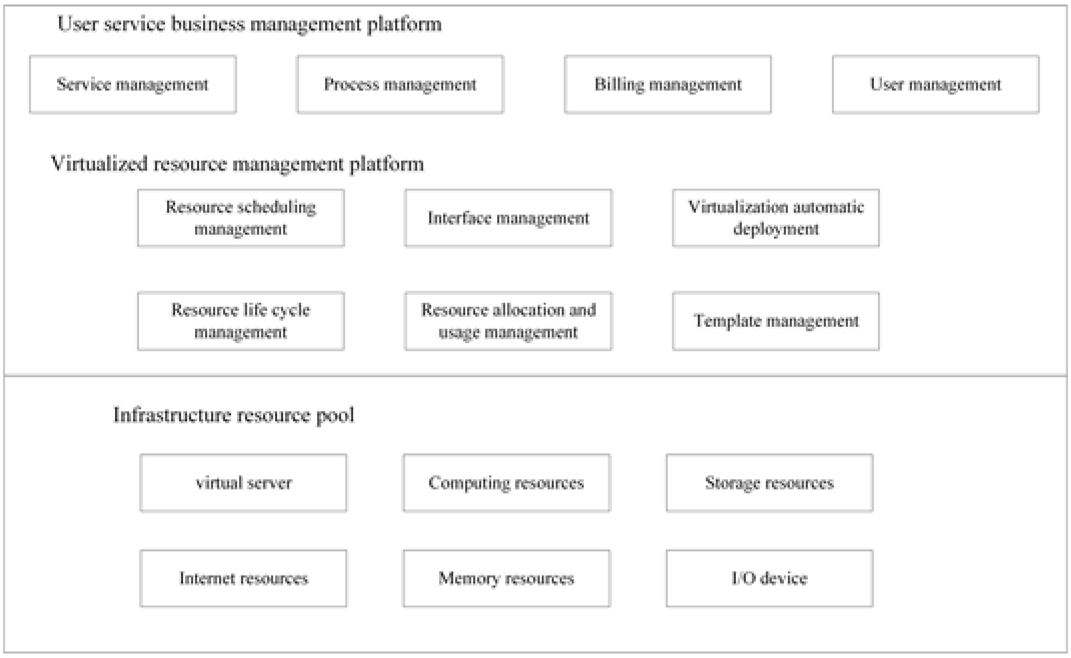
User service business management platform
Service management
Process management
Billing management
User management
Virtualized resource management platform
Resource scheduling management
Interface management
Virtualization automatic deployment
Resource life cycle management
Resource allocation and usage management
Template management
Infrastructure resource pool
virtual server
Computing resources
Storage resources
Internet resources
Memory resources
I/O device

Figure 1. IaaS platform architecture.

The infrastructure resource pool is the underlying structure of the IaaS cloud service platform, which is composed of virtual servers, computing resources, storage resources, network resources, memory resources, and II0 devices, providing users with virtualized infrastructure resources. The IaaS management platform is mainly composed of a virtualized resource management platform and a user service business management platform. The virtualized resource management platform is composed of modules such as resource scheduling management, interface management, virtualized automatic deployment, resource lifecycle management, resource allocation and usage monitoring, template management, etc. It is responsible for dividing physical resources and virtualized resources into a unified resource pool for scheduling And management to ensure the safe, efficient, fast and economic management of IaaS resources. The user service business management platform is mainly composed of user service management, service process management, billing management, and user management modules. It is responsible for encapsulating resource virtualization into various cloud service models and assigning them to users on demand, ensuring that IaaS services have high security Performance, efficiency and user satisfaction.

2.2. PaaS (software as a service) platform architecture

The PaaS platform is an intelligent application software development platform built on the IaaS cloud service platform. It is a service model that presents the library software development environment as a basic platform to users. Based on the IaaS cloud platform service, developers do not need to manage the infrastructure of the cloud system's underlying computing, network, and storage platform, nor do they need to purchase the hardware and software required for development activities. They can pay a lower fee to the cloud service provider. Complete the application design, application development, application testing and application hosting activities of the software and system required for the development of services by renting the PaaS platform cloud service, and complete the creation, testing and deployment of cloud reading applications and service activities.

2.3. SaaS (software as a service) platform architecture

The SaaS service platform refers to the establishment of cloud library management systems, user application software service systems, network and database management systems, reader access and resource management systems by leasing software service systems from SaaS service providers. Digital libraries do not need to perform Application software development, purchase and software system management and maintenance activities, while the SaaS service provider is responsible for the platform's pre-construction, management, maintenance and software update.

3. The hidden dangers of cloud library operation

The entire cloud library system consists of a data center, virtualization platform, cloud service, cloud interface and cloud terminal. Due to its own characteristics of virtualization, borderlessness, and fluidity, it also determines that there are corresponding new security risks from the physical layer to the virtualization, basic services and application layers. In summary, it mainly includes: improper use of cloud computing, insecure interfaces and APIs, rights management, human mistrust, data leakage, hidden intellectual property rights, account and service hijacking, unknown risk scenarios, etc. Avoiding these risks can be solved technically by establishing a security system and building a regional cloud library security platform.

The prevention and control of security risks in this area, such as data leakage, is an important content of the cloud library security platform construction. In terms of specific implementation, there are many technologies. Through comparative analysis, we propose a joint security authentication system based on KMI, which is based on identity authentication. In the above, role-based security access control is added to efficiently and securely solve the problems of regional cloud library authentication management and access control.

4. Foundation of KMI joint safety certification system

To ensure the confidentiality, integrity, verifiability and non-repudiation of data, the traditional method of "signature before encryption" is adopted. This method has a large amount of calculation, low efficiency, and high communication cost. Digital signcryption technology can effectively overcome its shortcomings, not only has higher efficiency, higher security, but also reduces communication costs, etc., and has good application prospects. Signcryption systems are divided into KKI-based signcryption systems, identity-based signcryption systems and certificateless signcryption systems. Among them, the KKI-based signcryption system can not only provide confidentiality, integrity, authentication and non-repudiation, but also improve efficiency and cost, and is easy to implement. It is reasonable to use this technology in the regional cloud library security platform.

4.1. KKI technology

KKI's core technical foundation is "encryption" and "signature" technology based on public key cryptography. The combination of "decryption" and "signature" technology can realize identity authentication in the network; the integrity of information transmission and storage, the confidentiality of information transmission and storage; the non-repudiation of operation. The process of encryption, decryption and signature verification is shown in Figure 2.

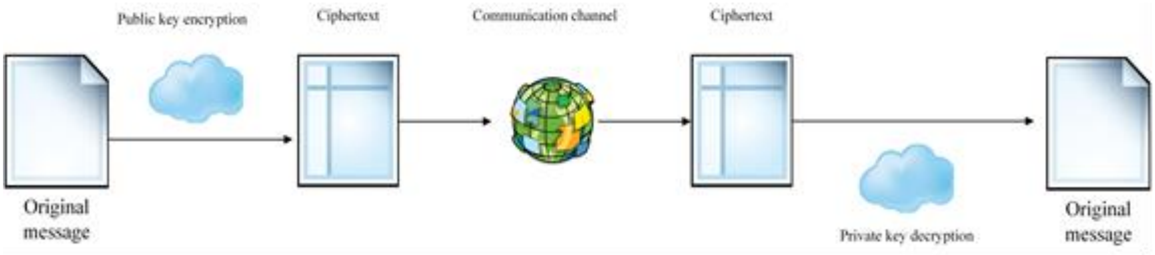

Figure 2. KKI encryption and decryption process.

The sender encrypts the original text of the message to form a ciphertext of the message. Except for the sender and receiver, no one knows the encryption algorithm, and there is no decryption private key. Even if the ciphertext information is obtained, it cannot be read. Only the receiver with the private key can correctly "translate" the original information and read it. Thereby ensuring the security and confidentiality of information.

The signature verification process is exactly the opposite of the encryption and decryption process. The signer uses the digest operation to extract the digest from the original message, encrypts the digest with the private key to form a signature, and then sends the original message and signature to the receiver, and the receiver uses the same digest The calculation generates a digest from the original message, and at the same time uses the public key to decrypt the signature. If the decrypted digest is consistent with the digest generated by the calculation, it proves that the message is the information sent by the sender.

Based on KKI's signature secret system, its deployment is mainly composed of CA, RA and directory services.

(1) Certification center CA

The certification authority acts as a trusted third party and is responsible for the issuance, renewal, and revocation of user keys or certificates.

(2) Registering authority RA

RA is an extension of CA's certificate issuance and management. The function can be replaced by CA.

(3) Directory service

A database of active digital certificates in the CA system. Provide a method for certificate distribution, storage, management, and update.

4.2. KMI technology

KMI expands the connotation of authorization. Based on KKI, cross-application, cross-system, and cross-organization user authority management can be realized. KMI provides support for role-based access control (RBAC). Permissions are not directly assigned to users, but to roles. Roles are an indirect means of assigning permissions. The KMI system is mainly composed of attribute certificates, attribute authorities, and attribute certificate libraries.

(1) Attribute certificate

The attribute certificate is a data structure, signed by the attribute authority AA, and the certificate holder's authentication information is bound to some attribute values. The issuing authority of the attribute certificate and the subject public key certificate are two independent organizations, and it may not be the same organization.

(2) Property authority

Attribute Authcxity (AA) is an authentication agency that distributes authority by issuing attribute certificates. AA and CA are completely logically independent, and in many cases, they are also physically independent.

The attribute authority (AA) assigns attribute certificates by issuing roles. When the user accesses the target resource, the user presents the role assignment attribute certificate to the verifier, and the verifier obtains the corresponding role specification attribute certificate through the system settings, so as to judge the user's access according to the role's authority, and realize the user's access control.

(3) KMI model

It gives a description method, there are mainly 4 models: general model, control model, transfer model and role model.

4.3. Relationship between KKI and KMI

KKI is the foundation of KMI, and KMI is an extension of KKI. The two are closely related: when KMI grants a certificate, the user needs to provide an identity certificate to ensure the correctness of the identity; when AA issues an attribute certificate, the attribute certificate must be bound to the user’s public key certificate information; Before verifying user rights, KKI must be called to authenticate their identity. In addition, KMI has nothing to do with KKI. KMI and KKI are transparent. KMI interacts with KKI through certificates and some functional interfaces, and calls function modules and API functions in the KKI system to complete user requests.

5. Construction of KMI-based cloud library joint security authentication system

Based on the above understanding and analysis of KMI technology, combined with the open, shared and efficient operation characteristics of regional cloud libraries, the establishment of a KMI joint security authentication system platform in regional cloud libraries is an ideal technical choice in terms of security control. The design and realization of the system structure, technical framework and authorization method are introduced in detail.

5.1. Cloud library joint security authentication system structure

In the regional cloud library, security identity authentication and cloud service access control are designed as an important system module, which is connected with each service cloud system through middleware. The system structure design of the system module is shown in Figure 3, and the specific workflow is shown in Figure 3. 4 shown.

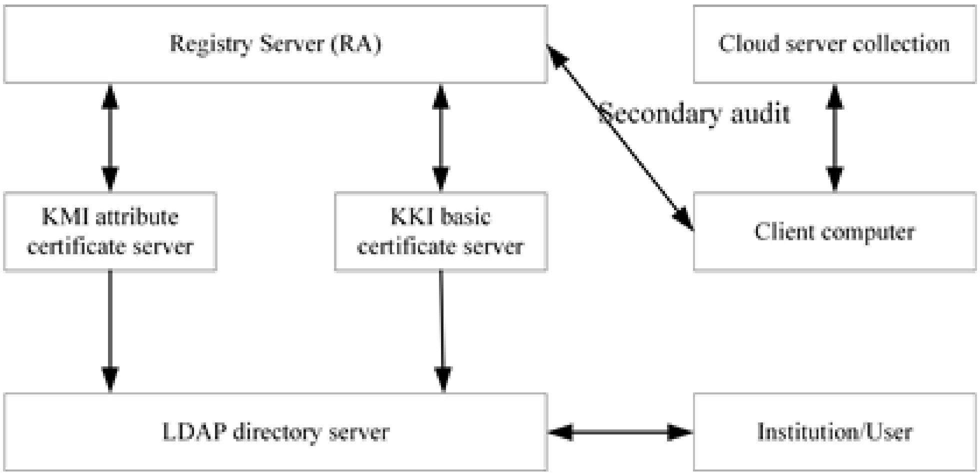

Figure 3. Cloud library KKI and KMI joint authentication and access control system structure.

If users from different libraries in the area want to access the resources of the cloud center, first go to the designated service page to register and apply for identity certificates and attribute certificates to the registration center server under the guidance of the staff of the library. After the registration center server design is reviewed by the unit manager and the second level review by the cloud center manager, the user request is forwarded to the attribute certificate server and the basic certificate server. After the certificate server has issued the certificate, the certificate is stored in the LDAP directory server, and the user is notified of the URL of the certificate through E-mail; after receiving the E-mail, the user can quickly get the certificate at the specified URL and store the certificate on the client The corresponding application.

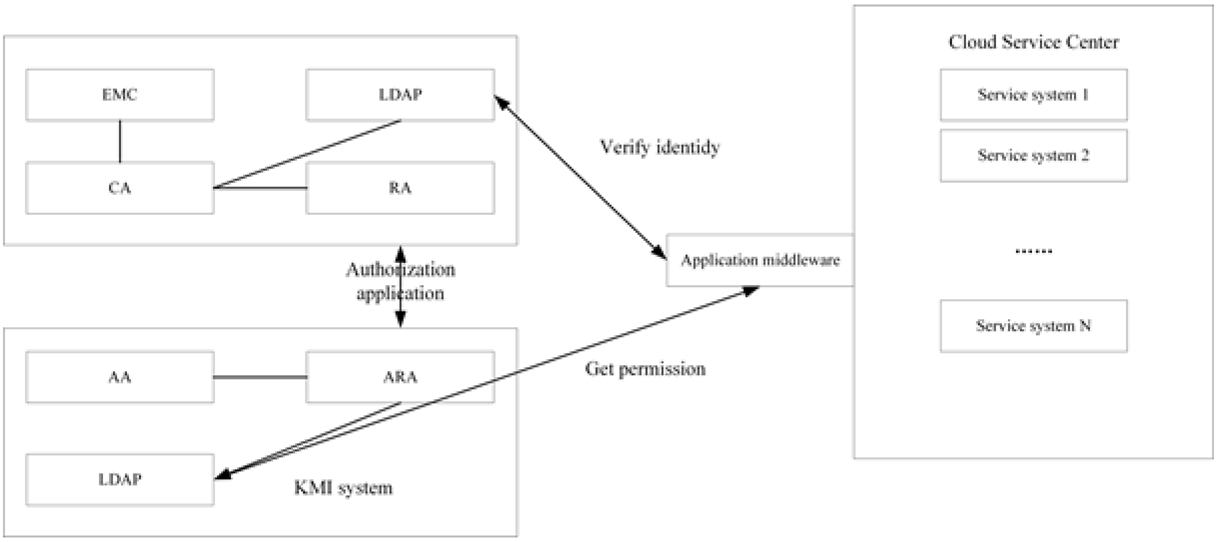

Figure 4. Cloud library KMI joint authentication visit control workflow.

When a user with an authorized certificate requests access to a service from a cloud resource server through a terminal, if the service requested by the user requires access rights, the corresponding cloud server will require the user to provide an attribute certificate and, if necessary, an identity certificate. After the client's application receives the certificate request from the cloud server, it sends the certificate stored in a specific location to the server. The cloud server checks the certificate provided by the user and checks whether the user has the right to the resource according to its access control policy. Access rights, grant users the access rights to the corresponding resources after passing the inspection.

This kind of identity authentication and access control method is very convenient for the development of cloud library services without specific space restrictions. As long as there is a network, the library will be with you. In addition, for the computers in the libraries, you can open more simple access methods such as IP control to meet the use of temporary readers. At the same time, Cocoa uses the Hamming distance to measure the similarity through the Bloom filter. The method to solve the Hamming distance is relatively simple, mainly calculating the number of different corresponding bits in the two binary sequences. In addition, there are four methods for solving similarity, including Cosine and Overlap, as shown in equations (1) and (2):

$$\cos ine\_sim(x,y)=\frac{\overline{X}\cdot\overline{Y}}{\left\|\overline{X}\right\|\cdot\left\|\overline{Y}\right\|}=\frac{\sum_{i=1}^{n}X_iY_i}{\sqrt{\sum_{i=1}^{n}X_i^2\sum_{i=1}^{n}Y_i^2}}$$

(1)

$$Overlap\_sim(x,y)=\frac{\overline{X}\cdot\overline{Y}}{\min\left(\left\|\overline{X}\right\|,\left\|\overline{Y}\right\|\right)}=\frac{\sum_{i=1}^{n}X_iY_i}{\min\left(\sum_{i=1}^{n}X_i^2,\sum_{i=1}^{n}Y_i^2\right)}$$

(2)

It can be seen from the above formula that the number of $\overline{X}\cdot\overline{Y}=\sum_{i=1}^{n}X_iY_i$ digits is equivalent to the number of 1 in the two Bloom filter data structures; the number of 1 digits in the Bloom filter data structure is represented as $\left\|\overline{X}\right\|^2$.

5.2. Overall technical framework

The KKI system mainly includes CA certificate issuing center, RA certificate registration center and KMC key management center. The key system adopts its own soft library encryption based on economic considerations. It is mainly responsible for managing the issuance, annotation, freezing, etc. of users' digital identities. The legal digital certificate issued by the user through the KKI system identifies the real identity in the application system for relevant operations. Among them, the KKI directory service system stores the legal user identity certificate issued by the KKI system, and provides external legal user identity queries.

KMI system mainly includes AA attribute certificate issuing center and ARA authorized management center. Authorization is based on digital certificates and published to the directory service system in the form of attribute certificates. Among them, the KMI directory service system stores the legal user attribute certificates issued by the KMI system, and provides external legal user authorization queries.

The security support platform is mainly composed of various application middleware, including services such as digital certificate analysis, trust domain verification, certificate authentication and authorization acquisition. Use it to realize the integration of various cloud service systems with KKI/KMI systems, provide identity authentication and authorization information acquisition, and transfer the information to various cloud service systems. The directory service system is used to store digital certificates and provide certificate information and authorization query services to the security support platform.

5.3. Authorization method analysis

The cloud library KKI and KMI joint authentication and access control platform, its authorization management is specifically realized through the way of "user attributes → user group → authority/role code → actual authority". Users who need special handling can also be authorized separately.

Each authorized user must have the support constraints specified in the relevant agreement. In terms of specific implementation, user information includes account number, library user, authority level, work unit, contact address, and so on. Especially the belonging library and authority level belong to the attributes of the user. Use different attribute values to divide users into corresponding groups. Each group corresponds to its own service acquisition permissions, that is, which resources can be accessed and which resources cannot be accessed. These rules are expressed by certain parameter variables and values.

Once you have groups, you need to authorize these groups. In the security prevention and control system platform, some permissions or role codes that only the cloud service system can resolve can be associated with user groups, which is authorization. The KMI system will pass the authority/role code to the cloud service system through the application support platform, and the corresponding cloud service system will control the authority.

In the process of accessing and controlling the entire regional cloud library, the KMI system plays a very important role. It is responsible for the combination of user attributes to form corresponding groups, expressing different user groups through authority/role codes, and parse user groups and authority/role codes Relationship. The cloud service system provides users with what they can do by analyzing the permission code before requesting, and then judging the result to achieve the visit control goal.

6. Conclusion

Cloud computing is a new stage in the development of the Internet. It is a technology, a new service concept, and an emerging business computing model. Since its birth, in a short period of time, there has been considerable development. Its application in the library field is also progressing very rapidly; cloud computing has outstanding advantages in building regional cloud libraries and making use of multi-library cooperation and sharing. However, while cloud computing brings high-quality services, there are also various problems, especially the serious security problems. In order to avoid the negative effects of its insecurity, technical protection is an important solution.

Based on this, this paper proposes a security solution for user identity authentication and access control using KMI technology to construct regional cloud libraries. This solution can well meet the needs of the cloud library intelligent service platform in terms of user identity authentication, access control, information confidentiality, data integrity protection and security auditing. Practical tests show that the scheme is safe and efficient.

Acknowledgments

The research on the influence of library development for the Class A tertiary comprehensive hospitals in Zhangjiakou (Project number: 1521141I).

References

[1] Kim J, Jeon Y, Kim H. The intelligent IoT common service platform architecture and service implementation [J]. Journal of Supercomputing, 2016, 44(3): 134-141.

[2] Kim K I, Bae S Y, Lee D C, et al. Cloud-based gaming service platform supporting multiple devices [J]. Etri Journal, 2017, 35(6): 960-968.

[3] Dong J, Zhang J W, Zhu H H, et al. A remote diagnosis service platform for wearable ECG monitors [J]. IEEE Intelligent Systems, 2019, 27(6): 36-43.

[4] Luo R C. Enriched indoor map construction based on multisensor fusion approach for intelligent service robot[J]. IEEE Transactions on Industrial Electronics, 2017, 59(8): 1-10.

[5] Deventer M O V, Keesmaat I, Veenstra P. The ITU-T BICC protocol: the vital step toward an integrated voice-data multiservice platform [J]. IEEE Communications Magazine, 2018, 39(5): 140-145.

[6] Chen Y F, Huang H, Jana R, et al. iMobile EE – An enterprise mobile service platform[J]. Wireless Networks, 2017, 9(4): 283-297.