Research of cloud computing security in digital library

Qingjie MENG
Library
Shenyang Aerospace University
Shenyang, China
e-mail: mengqingjie@sau.edu.cn

Changqing GONG
School of Computer
Shenyang Aerospace University
Shenyang, China
e-mail: gongchangqing@sau.edu.cn

***Abstract*—The cloud computing security in digital library was analyzed, for the digital books borrow, cloud storage and other related issues, a specific application of homomorphic encryption mechanism about library cloud computing was proposed. Firstly, the cloud computing mode of library digital resources is defined, a variety of collections databases and network resources adopt cloud computing mode to provide their service, these resources and service are placed in the cloud. And then the cloud key distribution scheme to adapt to library applications was presented, the improved traditional PKI, the PKI-based cloud computing communication and privacy protection mechanisms for library are introduced. The corresponding solution detail are proposed also: library cloud computing key distribution, authentication and encryption methods, more secure homomorphic encryption mechanism for library information retrieval. Preliminary analysis indicates that, these measures can protect the privacy and information security of library cloud computing.**

Keywords-library; cloud computing; security; homomorphic encryption；library

I. INTRODUCTION

Cloud computing hope to offer computing resources as water, electricity, gas, to serve customers.Users do not need to build their own expensive software and hardware computing environment, but according demand to rent the cloud service provider's hardware, system and application software platform (IaaS , PaaS, SaaS), to complete their computing tasks.

Cloud computing leads the development of industry informatization and society informatization, along with the popularity of Internet of things and mobile internet, the permeation of cloud computing in various industries was becoming increasingly apparent. Library services using cloud computing can greatly reduce costs and improve efficiency, according with the development needs of library operations. But cloud computing security issue has become a bottleneck restricting its application, mainly related to information security and privacy protection issues, which involves encryption, information isolation, authentication, key management and access control and other issues, it is the current cloud computing security research hotspot also.

Google, Amazon, Microsoft, and Vmware, propose some cloud security technology about authentication, access control, encryption, integrity, data isolation and other aspects. Cloud Security Alliance put forward some cloud security issues should be concerned; domestic and foreign scholars have made preliminary exploration in cloud computing PKI system, homomorphic encryption and other aspects. But research only focus on library cloud computing security was limited.

For ensuring the security of Library cloud computing applications effectively, beyond taking basic IT system security technology, aiming at the application features of library cloud computing, there is need to further explore library cloud computing mode, key distribution, authentication, encryption and other security technical means, to build cloud computing security system for library applications.

II. RESEARCH SUMMARIZATION

A. *Communication encryption of cloud computing*

Communications can be encrypted in symmetric encryption, public-key encryption, iSCSI encryption. For just want to store the backup in the cloud, they can encrypt their data, and then sends the ciphertext to the cloud data storage provider. In IaaS environments, using a variety providers and third-party tools to encrypt static data are common.

Currently, most such solutions are based on the user's digital certificates for authentication and encryption. Users can use digital certificates to authenticate in cloud management system, using the symmetric key to encrypt data in local, while using digital certificates to encrypt the symmetric key and then sent encrypted data to the cloud for storage. When a user wants to get the data, firstly, the encrypted data in cloud should be downloaded to the local, user decrypt the data by themselves. This model's advantages are: Only the user can decrypt the data stored in the cloud, it can effectively ensure the confidentiality of data. The disadvantages are: the user's client requires a strong encryption power, while user data encryption key must be kept secure. Once lost, it will not restore user data. This mode only applies to user generated static data encryption. For IaaS, PaaS, SaaS, users dynamic data generated in the cloud can not be encrypted using this model.

Cloud storage can take data isolation, encryption, segmentation way to protect privacy; cloud software applications need data isolation, the virtual machine isolation and operating system isolation to avoid risks. Privacy of data transfer can be protected by transport layer encryption technology, such as SSL, VPN, etc.

978-1-4799-0245-3/13/$31.00 ©2013 IEEE

B. *PKI applications in the cloud computing*

PKI (Public Key Infrastructure) use public key techniques to provide security services， including data encryption, digital signatures, identification, as well as the necessary key and certificate management, and other security services.

Cloud server provides the user a large distributed data services, with convenient to access user's data. In order to ensure better security, it is need to provide a large scale authentication and secure transmission design in the cloud.

Some scholars apply PKI system to basic architecture of cloud computing platforms. The key measure is to integrate cloud computing platform services directory and PKI-RA into a single server, intending to protect the CA security, alleviating the burden of CA.

C. *Homomorphic encryption*

Homomorphic encryption (homomorphism) means for processing the encrypted data to obtain an output, and then decrypt this output, the right results can be obtained.

With the homomorphic encryption in cloud computing, the interpret and operational of information can be isolated, and decrypted information will only be visible to the entity that really need interpretation, cloud server compute encrypted information. Homomorphic encryption operations can be eliminated in many information sharing and encryption and decryption operations.

Homomorphism was proposed by Rivest et al in 1978, it allows direct operation of the ciphertext encryption transform, and later improved by Domingo. Homomorphism technology was first used to encrypting statistical data, the homomorphic of algorithm ensure that the user can manipulate sensitive data but do not disclose data. With the development of cloud computing, it was suggested in the cloud using homomorphic encryption, some researchers have proposed a real number, integer range homomorphic encryption scheme.

Fully homomorphic encryption can process ciphertext in any calculation with high complexity. Using fully homomorphic encryption may protect data privacy of cloud computing user, store and manipulate confidential data at any place.

IBM researcher Craig Gentry uses the "ideal lattice" mathematical objects, proposed a scheme of fully homomorphic encryption. Bristol University Professor Nigel Smart and University of Leuven in Belgium cryptography researcher Frederik Vercauteren, modify the most primitive technical proposal, and make the implementation and testing, they improved the encryption algorithm, so that the data can be easier operated. However, there are limitations to this scheme, with the calculation step increasing, the quality of calculation result will decline.

III. CLOUD COMPUTING SECURITY PROGRAM FOR LIBRARY

A. *Cloud computing model and related cloud security strategy for libraries*

Firstly, it is need to define cloud computing mode of library digital resources, a variety of collections databases and network resources adopt cloud computing mode to provide their service, these resources and service are placed in the cloud. The library need not to set the physical equipment maintenance departments, and can focus on the library's core business, save equipment investment funds also. Whether at anytime, users can access this "library service cloud", librarians can archive data collection with "cloud storage", reader can gain entry into library cloud to access digital resources, such as digital journals, dissertations, books and so on. Advisory librarian may at any time access cloud services to provide related consulting services.

The entire life cycle of books can also be achieved by cloud management: including publication, distribution, warehousing, retail, cataloging, archiving, restoration, appointments, borrow, return, cancellation, etc. It always needs to access the "cloud" in order to feedback data, support services.

It is need to study these various library cloud computing security policy issues, such as authentication, security level, communication encryption, data encryption, data isolation, privacy protection, access control, key distribution strategies. The following selection of its typical application cases are analyzed throughly, aiming at its cloud security needs some solutions will be proposed.

B. *Cloud computing key distribution, authentication and encryption methods for library applications*

Traditional communication encryption is to ensure encrypted information can be decrypted by receiver; while the encrypted communication of library cloud storage may need to be unreadable for cloud. Therefore, the original system of communication encryption even the key management system needs to be changed accordingly, such as PKI work mode requires improvement.

Research the cloud key distribution scheme to adapt to library applications, with improved traditional PKI, the PKI-based cloud computing communication and privacy protection mechanisms for library are introduced:

Certification authority center can manage user information, the user information and location information can be binded to form a certain period virtual identity ID. True identity and login location information stored in the authentication center, accessed only by authorized users. User access to library service only using virtual identity, thus user privacy can be protected effectively.

Current communication encryption use specific packet keys to encrypt each packet, if eavesdropper had gathered sufficient packets, he would carried out exhaustive crack. So, library data cloud storage can be "broken up" scrambling at file units, we may learn communication systems "interleaved coded" principle, to take "convolution Encryption" or "holographic encryption" approach to implementation. While IPSec-based multi-security level cloud storage authenticated encryption scheme can be adopted, then the forwarder along the communication path can not tampering with information packet, in order to respond that the library cloud communications needs to across untrusted network.

C. Homomorphic encryption in library cloud computing

Cloud platform services can use a virtual machine isolation technology, there have been some research results; but cloud software services can not be easy to deal with. The typical example of cloud software in library applications, may be electronic literature search, e-book lending and so on. Retrieve data entered by user need to be kept confidential, but also need to understand by cloud computing retrieve software, just do not need to "others" know. At this point it needs "encryption process", the user wants to have complete control over the entire calculation process: registers, memory, hard drive. But contrary to logic of cloud, cloud computing is characterized by a cloud service customers do not need to understand the background of the details, only interested in the quality of services and so on.

Different with virtual machine isolation strategy, our program attempts such a "transformation": client made pre-transform of input data, and then deliver to cloud computing virtual machine, the results returned to client, and then through the inverse transform. Transform parameter is equivalent to the encryption key, therefore, the cloud can only see "transformed" input data and output data calculated, can not know the true data and results of customer, even the real object. So the privacy can be protected. Homomorphic encryption mechanism can provide basic algebra encryption, but cloud computing solutions involving library also needs careful study.

For example, we can use additive homomorphic for mobile users and library key distribution operations.

Addition homomorphism principle means that, there is operation:

$$E\ (a + b) = E\ (a) + E\ (b);$$

encryption algorithms:

$$E\ (x) = (x + r) \bmod (n) = y,\ n = pq,$$

p and q are two large prime numbers, r is a random integer.

Decryption algorithm:

$$x = D\ (y) = y \bmod (q);$$

the transfer of q and n use each public key encryption.

Solutions described as follows:

User-generated temporary partial encryption key K1, and sent to the cloud storage access point:

$$E\ (K1) = (K1 + r * q) \bmod (n);$$

Cloud storage access point generates temporary partial encryption key K2, and sent to the user:

$$E\ (K2) = (K2 + r * q) \bmod (n);$$

Calculating each temporary communication key:

$$K = (E\ (K1) + E\ (K2)) \bmod (q) = D\ (E\ (K1) + E\ (K2));$$

Because satisfying homomorphic encryption:

$$E\ (K1) + E\ (K2) = E\ (K1 + K2);$$

Therefore:

$$K = D\ (E\ (K1 + K2)) = K1 + K2;$$

Both sides through homomorphic encryption obtained same temporary communication key.

The efficiency of additively homomorphic key agreement algorithm needs to be improved, need to research more efficient, robust homomorphic encryption algorithm so that:

$$E_{\text{key agreement}}\ (K1 \oplus K2) = E_{\text{key agreement}}\ (K1) \odot E_{\text{key agreement}}\ (K2).$$

IV. Feasibility Demonstration

A. Cloud computing key distribution, authentication and encryption methods for library applications

PKI-based library cloud computing communications and privacy protection mechanisms: there is no difficulty in principle to build cloud security privacy protection mechanisms. Because the current PKI system was mature, the certification center HASH function can be constructed without difficulty, PKI security is also not reduced.

IPSec-based library cloud storage authenticated encryption scheme: IPSec algorithms was mature, symmetric keys and RSA can be used, application can gradually expand, there is no difficulty in principle.

B. Homomorphic encryption in library cloud computing

Homomorphic encryption can be applied to cloud computing, foreign literature has proved the feasibility of integer and real arithmetic operations. Our program's electronic document retrieval and electronic books borrowing although complicated, but the implementation of the processor always simple addition, there is no difficulty in principle. The efficiency of the algorithm need attention. The project started from the linear equations, to study the impact of linear transform, having rich matrix computation theory as supported.

V. Conclusion

This paper analyzed the security problems faced by library cloud computing, proposed the corresponding solution: library cloud computing key distribution, authentication and encryption methods, more secure homomorphic encryption mechanism for library information retrieval. Preliminary analysis indicates that the library program performance can meet the security needs of business applications.

Acknowledgment

This paper is supported by Natural Science Foundation of Liaoning Province of China, No. 201102171.

References

[1] FENG Dengguo, Zhang Min, Zhang Yan and Xu Zhen, "Cloud computing security research," Journal of Software, vol. 22 (1), pp. 71-83, 2011.

[2] Li Jian, Zhang Ji, "PKI applications in cloud computing research," Information security thematic studies, vol. (8), pp. 44-47, 2011.

[3] Wang shurong, Zhong Ping, "Cloud internal secure communication model," Computer Engineering and Applications. vol. 47 (10), 2011.

[4] N. Santos, K.P. Gummadi, and R. Rodrigues, “Towards trusted cloud computing,” In Proceedings of the Workshop on Hot Topics in Cloud Computing, June 2009.

[5] Rivest R L, Adleman L, Detrouzos M L, “On Data Banks and Privacy Homomorphism,” Foundations of Secure Computation New York:Academic Press，1978：169-179.

[6] Domingo F J, “A New Privacy Homomorphism and Applications,” Information Processing Letters， vol. 60(5), pp. 277-282, 1996.

[7] Xiang guangli, Chen Xinmeng, Ma Jie, etc, “Homomorphic encryption mechanism on the real number range,” Computer Engineering and Applications, vol. 20, pp. 12-14, 2005.

[8] Hu Yanzhi, Ma Dawei, Tian Zengshang, etc, “Wireless group key distribution protocol based on homomorphic encryption mechanism,” Computer Engineering, vol. 35 (7), pp. 158-160, 2009.

[9] C. Gentry, “Fully homomorphic encryption using ideal lattices,” In Proceedings of the 41st Annual ACM Symposium on Theory of Computing, vol. 1, pp. 169-178, 2009.