Cloud Computing Security in Digital Archives

P. Penchala Prasad¹, Y. R. Janardhan Reddy², A. Vineela³
¹,²,³Computer Science and Engineering, INDIA

ABSTRACT
The cloud computing protection in digital library was analyzed, for cloud storage, digital books borrow, and other related issues, a specific application of homomorphic encryption method cloud computing was suggested. First, the cloud computing mode of files digital resources is defined, a variety of collections databases and network resources take on cloud computing mode to give their service, these resources and service are positioned in the cloud. And then the cloud input allocation format to get used to library applications was presented, the developed conventional Public Key Infrastructure, the PKI-based cloud computing message and privacy security mechanisms for annals are introduced. The corresponding solution explained in detail proposed system. Those are library cloud computing key distribution, authentication and encryption methods, homomorphic encryption mechanism for library information recovery. These measures can care for the privacy and information security of library cloud computing.

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

I. INTRODUCTION

Cloud computing expect to suggest computing resources as electricity, water, gas, to serve customers. Users do not need to construct their own costly software and hardware computing setting, but according require to rent the cloud service provider's hardware, system and application software platform, to complete their computing tasks.

Cloud computing directs the development of production informatization and society informatization, along with the reputation of Internet of things and mobile internet, the penetration of cloud computing in various industries was becoming increasingly perceptible. Library services using cloud computing can significantly decrease costs and develop efficiency, according with the progress needs of library procedure. But cloud computing security issue has develop into a block confining to its request, mainly related to information security and isolation safety issues, which involves encryption, information separation, validation, key management and access control and other issues, it is the current cloud computing security research hotspot also.

Google, Microsoft, VMware, and Amazon, suggest some cloud security technology about verification, access control, encryption, reliability, data seclusion and other characteristics. Cloud Security association ahead some cloud security issues must be concerned; household and foreign scholars have ready beginning exploration in cloud computing PKI system, homomorphic encryption and other characteristics. But research only focus on library cloud computing security was restricted.

For make sure the security of Library cloud computing applications efficiently, away from taking basic IT system security technology, focusing at the application features of library cloud computing, there is requirement to further explore library cloud computing mode, key allocation, verification, encryption and other security technical means, to build cloud computing security system for library applications.

II. SUMMARIZATION

A. Communication encryption of cloud computing
Messages can be encrypted in public-key encryption, symmetric encryption. For immediately would like to store the endorsement in the cloud, they can encrypt their data, and then sends the ciphertext to the cloud data storage supplier. In IaaS environments, using a selection providers and third-party tools to encrypt fixed data are widespread.

At present, the majority solutions are based on the user's digital certificates for verification and encryption. Users can use digital certificates to validate in cloud management system, using the symmetric key to encrypt data in local, while using digital certificates to encrypt the symmetric key and then send encrypted data to the cloud for storage. When a user required getting the data, first of all, the encrypted data in cloud should be downloaded to the confined, user decrypt the data by themselves. This model's rewards are: Only the user can decrypt the data stored in the cloud, it can effectively make sure the privacy of data. The disadvantage is: the user's client requires a tough encryption power, while user data encryption key must be reserve to protected. Once gone, it will not restore user data. This mode only applies to user generated static data encryption. For IaaS, PaaS, SaaS, users lively data generated in the cloud cannot be encrypted using this model.
Cloud storeroom can take data separation, encryption, segmentation way to keep privacy; cloud software applications need data separation, the virtual machine separation and operating system loneliness to avoid risks. Privacy of data transmit can be protected by transport layer encryption technology, such as SSL, VPN, etc.

B. PKI applications in the cloud computing

PKI (Public Key Infrastructure) use public key techniques to afford security services including data encryption, digital signatures, classification, as well as the essential key and certificate supervision, and other security services.

Cloud server supply's the user a large distributed data services, with suitable to contact user's data. In order to guarantee superior security, it is requiring providing a large scale authentication and securing transmission design in the cloud.

Some scholars apply PKI system to basic structural design of cloud computing platforms. The key compute is to combine cloud computing proposal services directory and PKI-RA into a single server, intending to defend the CA security, improving the load of CA.

C. Homomorphic encryption

Homomorphic encryption (homomorphism) means for meting out the encrypted data to attain an production, and then decrypt this production, the right results can be attained. With the homomorphic encryption in cloud computing, interpret and operational of information can be isolated, and decrypted information will only be noticeable to the thing that in fact call for interpretation, cloud server calculate encrypted information. Homomorphic encryption operations can be eliminating in much information distribution and encryption and decryption operations.

Homomorphism was proposed by Rivest et al in 1978, it allows through operation of the ciphertext encryption transform, and later improved by Domingo. Homomorphism technology was first used to encrypting statistical data, the homomorphic of algorithm make sure that the user can influence receptive data but do not reveal data. With the expansion of cloud computing, it was suggested in the cloud using homomorphic encryption, some researchers have proposed a real number, integer range homomorphic encryption proposal.

Fully homomorphic encryption be able to practice ciphertext in any computation with high complexity. Using fully homomorphic encryption may defend data privacy of cloud computing user, accumulate and influence 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 PROGRAM FOR DIGITAL ARCHIVES

A. Cloud computing strategy for Digital Library

Firstly, it is need to describe cloud computing manner of library digital resources, a diversity of collections databases and network resources take on cloud computing mode to offer their service, these resources and service are placed in the cloud. The library need not to set the physical tools preservation departments, and can focal point on the library's hub business, keep equipment asset funds also. Whether at anytime, users can access this "library service cloud", librarians can archive data collection with "cloud storage", person who reads can gain entry into library cloud to access digital resources, such as digital journals, books dissertations and so on. Suggested librarian may at any time access cloud services to make available related consulting services.

The entire life cycle of books can also be achieved by cloud management: including publication, distribution, retail, warehousing, archiving, cataloging, 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 this variety of library cloud computing security rule issues, such as authentication, security level, communication encryption, data encryption, data isolation, privacy safety, access control, key distribution strategies. The following selection of its typical application cases are analyzed thoroughly, aiming at its cloud security needs some solutions will be proposed.

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

Conventional communication encryption is to make sure encrypted data 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 needs development.

Research the cloud key allocation system to adjust to library applications, with improved traditional PKI, the PKI-based cloud computing communication and privacy fortification mechanisms for library are introduced:

Certification power center can deal with user information, the user information and location information can be binded to form a confident era virtual identity ID. True identity and login 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 cannot tampering with information packet, in order to respond that the library cloud...
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 cannot 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:

\[ H(x + y) = H(x) + H(y); \]

encryption algorithms:

\[ H(a) = (a + r) \mod (n) = y, \quad n = pq, \]

\[ p \quad \text{and} \quad q \quad \text{are two large prime numbers,} \quad r \quad \text{is a random integer.} \]

Decryption algorithm:

\[ a = D(b) = b \mod (q); \]

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:

\[ H(K1) = (K1 + r \ast q) \mod (n); \]

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

\[ H(K2) = (K2 + r \ast q) \mod (n); \]

Calculating each temporary communication key:

\[ Ke = (H(K1) + H(K2)) \mod (q) = D(H(K1) + H(K2)); \]

Because satisfying homomorphic encryption:

\[ H(K1) + H(K2) = H(K1 + K2); \]

Therefore:

\[ Ke = D(H(K1 + K2)) = K1 + K2; \]

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:

\[ H_{key\ agreement}(K1K2) = H_{key\ agreement}(K1) \quad \text{and} \quad H_{key\ agreement}(K2). \]

IV. OUR APPROACH

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.

As part of the World Wide Web Objects library, we have developed a Cacheable class. The class offers a small set of primitive caching operations which may be performed upon a Cacheable object, i.e., any object derived from the Cacheable class. These operations, in conjunction with appropriate concurrency-control, constitute the basic building blocks used by a client to explicitly specify whichever caching protocol is required. Invoking the basic operations in different sequences provides different protocols. One of these basic operations enables the proxies of Cacheable objects to obtain the state of their remote object. Client operations performed upon the proxy may then occur locally, i.e., the proxy can act as a cache. Another operation enables the proxy to write back the state to the object.

V. CONCLUSION

This paper analyzed the security problems faced by digital archives like 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.
REFERENCES