# Study of Data Security Based On Cloud Computing

Honghua Wang
Huaiyin Institute of Technology
the Department of Computer Sicence and Engineering ,Huaiyin Institute of Technology
Huaian 223003,Jiangsu ,China
email :whhly35@163.com

*Abstract*—**This paper analysis the core problem of cloud computing: data secure problem, using the newly development of cryprology: fully homomorphism encrytion(FHE) to protect cloud computing data. Put forward data secure scheme based on the character that FHE can operate encrypted data. This scheme not only protect the data, but also can assure the efficency of the application.**

***Keywords-cloud computing; fully homomorphism encryption; data security***

## I. INTRODUCTION

Cloud computing has achieved great progress in recent years, and has a tendency to continue to develop. As an emerging technologies, cloud computing security issues have not yet been fully studied, did not offer a complete solution at present, security issues related to cloud computing focused on access control, using attribute-based encryption algorithms, virtual security technology, such as data protection, integrated studies, core of the recognized most of them data security issues.

This article seeks to analyse this issue combined with recent advances in cryptography, technical programme addressing the issues.

### *A. Introduction to cloud computing*

First proposed the concept of "cloud computing" (Cloud Computing) is put forward in August 9, 2006, by Google CEO Eric Schmidt (Eric Schmidt) in the search engine assembly (SES San Jose 2006). Here refer to Wikipedia's definition, that is, cloud computing (Cloud Computing), including the main meaning: it is a calculation based on the Internet, in this way, the hardware and software resources that are shared and information can be provided to computers and other devices. Cloud computing describes a new IT services based on the Internet increased, use and delivery models, usually involves providing dynamic easy to expand through the Internet and often virtualized resources. Cloud computing can be considered to include the following levels of service: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). Cloud computing services usually provide common access online business application through the browser, software and data that can be stored in the data center. At present, many companies have launched the practical or commercial cloud services, such as Amazon (Amazon) launched the Elastic Compute Cloud (Elastic Compute Cloud; EC2) service, Googl.

Using cloud computing to shore up its search service, Microsoft also attached great importance to the cloud, Live services framework and the company on cloud computing due to cloud computing cost advantage, has a good development momentum, with application looks promising.

### *B. cloud computing data security issues*

Be seen from the above, cloud computing is one of the key characteristics of its services are provided through a network. All user data is stored in the cloud, and evaluates the results back to the client over the network. As a new service delivery model, the security threats facing is unprecedented, both the theoretical and the practical. Since cloud computing is a distributed, and in order to improve the efficiency of resource use, possible sharing of computing or storage resources among users, if security isolation between users is not enough attacks or malicious users to take advantage of technology, will result in threats to data security, stolen, tampered with or deleted. Therefore, guarantee the security of the cloud data and stand-alone modes have different characteristics, using only traditional methods of protection is difficult to guarantee the security of user data. In fact, has a number of cloud computing security problems occur, such as in March 2009, Google leaking out the large number of users files event occurs. In October 2009, the Microsoft cloud computing user data loss due to server failures, and so on.

Summed up, data security risks of the major cloud computing services have the following several aspects:

*1) Data transmission security*

Normally, the enterprise data center to save a large number of enterprises and private data, these data are often represents the core competitiveness of enterprises, such as the enterprise customer information, financial information, the key business process and so on.In cloud computing model, enterprise data through the network to the cloud computing services processing, faced several problems: one is how to ensure the enterprise data in network transmission process strictly encryption, guarantees the data even if the theft can not restore; the two is how to ensure the cloud service providers in the receive data when the enterprise confidential data leak out; three is in the cloud computing services department store, how to ensure access to the user through the strict certification authority and legitimate access to the data, at the same time to ensure that the enterprise at any time all can secure access to their own data.

Published by Atlantis Press, Paris, France.

#### *2) Data storage security*

The enterprise data storage is a very important link, which includes a data storage location, data are isolated from each other, data disaster recovery.In cloud computing model, cloud computing service provider in a highly integrated high capacity storage space, open up a portion of the storage space available to the enterprise.But the customer is not aware of their data to be placed on which server, even don't know this server is placed in the country; cloud computing service providers in the storage resource country whether there is information security issues, can ensure enterprise data will not be disclosed; at the same time, in the data storage resource sharing environment, even if the encryption mode, cloud computing service provider is able to guarantee the data between the finite isolation; in addition, even if the enterprise users to understand the data stored in the server's location, they must also require service providers to make a promise to the hosting, data backup, to prevent the occurrence of major accidents, enterprise user data could not be restored.

#### *3) Data auditing security*

The practical work, in order to guarantee the accuracy of the data and effectiveness tend to attract third-party certification body carries on the data trial in cloud computing environment, cloud computing service provider must ensure that no other enterprise data calculated risks at the same time, and provide the necessary information support.in order to assist the third party data generation the safety and accuracy of the audit, enterprises realize the compliance requirements; In addition, the enterprise to cloud computing services of the sustainable development in the authentication process, how to ensure that cloud computing services can provide effective data, and does not damage the interests of other existing customers. In the implementation of the audit process, also should guarantee the audit institution does not leak related enterprise's sensitive number.

## II. Brief introduction of Fully homomorphic encryption

Fully homomorphic encryption was proposed based on homomorphic encryption. Homomorphic encryption (Homomorphie Cryptograph) by Rivest et al to put forward 1978, also known as a homomorphism (Private Homomorphic).Remember the encryption operation for E, specifically m P, encryption, decryption operations for D, namely e=E (m), m=D (E).Known plaintext operation in F, according to E can be used to construct F, such that F (E) =E (f (m)), then E is a f for the homomorphic encryption algorithm that is to say, can not know clearly the situation on the ciphertext, direct action, like to express operation, and then encrypts the results obtained as two homomorphic encryption includes two basic types: take the homomorphism and homomorphism, additive homomorphic encryption algorithm respectively, the multiplication and addition with homomorphic properties. For example, the original RSA algorithm is a homomorphism.

In 2009, the field has made breakthrough progress. IBM's Craig Gentry (Craig Gentry) was published an Article, published a new found on cryptography .He is based on the ideal lattice (Ideal Lattice) method to construct a species known as the "homomorphism" (Full homomorphic) encryption scheme. It is called the homomorphism, ibecause the programs for all of the algorithms are homomorphism.He constructed homomorphic public key encryption scheme includes four algorithms, namely the key generation algorithm, encryption, decryption algorithm and additional evaluation algorithm.

## III. Ease of Use Fully homomorphic encryption data security solution

Use of fully homomorphic encryption to encrypt the data, the data security of cloud computing can be ensured. After the data encryption stored in the clouds, the security of the data is improved, even if the data is stolen, no corresponding key can not be reversed, and the key that only the user knows, the clouds do not know the secret. At the same time, because of the characteristics of cloud homomorphic encryption, the encryption operation, thus avoiding the traditional encryption data processing efficiency problem for ordinary encryption scheme for its operation, will be encrypted data transmission, encryption decryption operation after the return to the clouds. In order to reduce the amount of calculation, the author uses Gentry proposed symmetry fully homomorphic encryption algorithm, put forward below the data security solutions.

### *A. Symmetric homomorphism encryption algorithm profile*

Encryption algorithm:

Encryption parameters: Q and R, P key: odd

Encryption: the plain (bit) m, calculation:c=pq+2r+m, namely for the corresponding ciphertext

Decryption: m= (c mod p) mod 2

Correctness verification: because the Pq is larger than 2r+m, then (c mod p) =2r+m, so ((c mod p) mod 2= (2r+m) mod 2=m.

The following test homogeneity, with addition and multiplication as the example:

A two ciphertext c1 = q2P+2r2+m2, =q1P+2r1+m1,c1+ c2= (q1+ Q2) P+2 (r1+r2) + m1+m2, so, only need to meet the conditions of 2 (r1+r2) + m1+ M2 far less than P, (c1+ C2) mod p =2 (r1+r2) + m1+m2 is the encryption meet additive homomorphic conditions.

C1*c2= [q1*q2 + (2r1+m1) + (2r2+m2)]p+2 (2 r1*r2+ r1*m2 + R2 *m1 + m1*m2) therefore, just meet 2 (2 r1*r2+ r1*m2 + R2 *m1) + m1*m2 far less than P, there is (c1*c2) modp=2 (2 r1*r2+ r1*m2 + R2 *m1 + m1*m2) that the encryption to meet by homomorphic conditions.

### *B. Implementing Scheme*

Specific steps and programs are as follows:

*1)* the user access the clouds, generating a key.Users of its public key encryption the denseKey and the encrypted data stored in the cloud.

*2)* the user uses the key to encrypt the data, and uploads the encrypted data to the clouds.And storage.

*3)* the user needs to access data, using the key data to be operated on, such as the query operation.At this point, the client sends the encrypted requests to the cloud, the

Published by Atlantis Press, Paris, France.

cloud encrypted data with the implementation of the corresponding operation, and return results to the client.

Using The encryption scheme, structure data secure cloud computing solutions, the solution used in the client hardware (such as a smart card) to generate a key, and the key and the hardware (i.e., with a pair of public and private keys) binding, thereby indirectly realize the user and the key bindings. Customers using the public key encryption key and stored in the cloud. Thus, only the user can decrypt the key, ensure customer data security. The client uses this key will be encrypted data transmission to the cloud storage. At the same time, by using digital signature technique, can guarantee the data integrity and non-repudiation. Similarly, the client need cloud data related services (such as search), but also related to the content encryption to send the clouds; using homomorphic encryption features, by the cloud on the ciphertext direct implementation of related operations, and then the result back to the terminal user. Such, Whether in the transmission channel or on a storage medium, transmission or operation is plusDensity data, even if the theft, also cannot get from raw data or other usefulInformation. In addition, the encryption algorithm of symmetric encryption algorithm, a relatively small amount of calculation, Easy to implement, can effectively reduce the client's burden, can adapt to various cloud terminal Environmental science. The disadvantage of data is the main volume will become larger, increasing the network transmission and storage overhead.

## IV. CONCLUSION

The recent advances in the application of cryptography to cloud, a design can ensure the security of user data, but also can avoid the disadvantages of the traditional encryption scheme of the new cloud computing data security solutions, for the protection of cloud computing security made beneficial exploration.

The scheme can be applied in cloud computing in many aspects, for example, the ciphertext ciphertext retrievalAuditing etc.. At present, although at present as a result of fully homomorphic encryption calculation complexity, data volume increase is too much wait for a reason, fully homomorphic encryption scheme also failed to cast a person to utility, but along with the development of cryptography, believe that in the near future will occur can be practical, can ensure the safety of the homomorphism algorithm for cloud.

## REFERENCES

[1] Gntry C. Fully homomorphic encryption using ideal lattices[M]. 1n:Mitzenmacher M, ed. Proc. of the 2()09 ACM Int'  1 Symp. On Theoryof Computing. New York: Association for Computing Machinery, 2009.169-178.

[2] Goyal V, Pandey A, Sahai A, Waters B. Attribute-Based encryption for tine-grained access control of encrypted data[M}. In: Duels A, Wright RN, Vimercati SDC, eds. Proc. of the 13th ACM Couf. on Computer and Conmmnications Security, C:CS 21)06. Alexandria: ACM Press, 2006.

[3] Marten van Dijk and Craig Gentry and Shai Halevi and Vinod Vaikuntanathan. Fully Homomorphic Encryption over the Integers[D]Eurocrypt, 2010

[4] Nigel Smart and Frederik Vercauteten.Fully HomomorphicEncryption with Relatively Small Key and Ciphertext Saes[M]一 In PKC2l)1(I,LNCS volume 6056, Springer, 2010.420-443.

Published by Atlantis Press, Paris, France.