Protect Cloud Computing's Data Using Fully Homomorphic Encryption

Wu Xu-dong
Key Laboratory of Information Network Security, Ministry of Public Security, People's Republic of China
Shanghai, china
zjusomwu@yahoo.com.cn

Li Xin
The Third Research Institute of Ministry of Public Security
Shanghai, china
ndlixin@sina.com

***Abstract*—With the fast development and wide application of cloud computing,more and more security accident has been appeared.Though some traditional security measure has been applied, the security problem has become the main abstacle to apply cloud computing technology This paper based on the newly developed fully homomorphic encryption then proposed a data security scheme which can operate encryped data directly on cloud server without decrypt while all communication between client and server is encrypted,it can asure data security at the mean time asure the operate efficiency.**

Keywords- fully homomorphic encryption; cloud computing

I. INTRODUCTION

In the past few years,cloud computing has made noticeable progress and it was looked as the revolutional technology in the computing field. Cloud computing can be compared to the supply of electricity and gas, or the provision of telephone, television and postal services. Because it's public service attribute(even for private cloud,it is used by a lot of users),it is suffered from network attack. The main obstacle of cloud computing is it's security as widely regarded,there have many security methods been implied and applied. The cloud computing security research focused on access control[1,2];attribute based encrypt algorithm[3];virtual security technology[4];data protect[5],and so on.

The focus of cloud computing security is the data secury. According the key character of cloud computing,all of the computing service is provide through network,so the main risk is happened when they are tranfered,stored.The easy way is to encrypted data when transfed and stored,but the previous method can't operate encrypted data directed.As in the recent years in the cryptogragh field also made advace ,especially the fully homomorphic encryption.With the newly cryptogragh technology we have the chance to asure cloud computing's data security though maybe it can't applied at once.In this paper we will construct a data secure search scheme based on homomorphic cryptograph.The main advantage of this scheme is that it can directly operate on encypte data.

II. FULLY HOMOMORPHIC CRYPTOGRAPH

Homomorphic cryptograph is first discoved by Rivest,Adleman and Dertouzos, which also called privacy homomorphism was introduce by Rivest, Adleman and Dertouzos [6], shortly after the invention of RSA by Rivest, Adleman and Shamir.The basic concept of homomorphic cryptograph is that we can deal with the cipher text without decrypt the cipher text.For example,the plain text is m ,after encrypt operation E ,we get cipher text e ,through decrypt operation D ,we can get the original plain text.Now we have two operation(function) f and F ,apply f to plain text and apply F to cipher text,we have $F(e) = E(f(m))$,that's mean through F we get the encrypt result of $f(m)$ .The basic RSA is a multiplicatively homomorphic encryption scheme.

After homomorphic encryption is invented,people try to find more homomorphic encrypt scheme.Until recently this field has achieved break forth progress[7].Craig Gentry who was from IBM research center published his research about homomorphic encryption,he used lattice based method successfully constructed a encrypt scheme called fully homomorphic encryption.Fully homomorphic means the encrypt scheme is homomorphic for all operation.His encryption scheme include four algorithm:key generation ,encrypt algorithm,decryp algorithm and the additional evaluate algorithm.

III. CONSTRUCT DATA SECURITY SCHEME USING FULLY HOMOMORPHIC CRYPTOGRAPH

Applying fully homomorphic encryption we can assure data secure for cloud computing.The key concept is that the data is encrypted by homomorphic encryption and stored in cloud server,through this we can get the big benefit:deal with the cipher text directly in server and assure the data's security because anyone else who don't know the key can't decrypt it.We use homomorphic symmetric encryption[8] to construct the data secure scheme.

The symmetric homomorphic encrypt scheme:

Select encrypt parameter: r , p and q , r$\sim 2^n$,p$\sim 2^{n^2}$,q$\sim 2^{n^5}$,and p is prime, p is the secret key.

Encrypt:for plain text m , compute $c = pq + 2r + m$,c is the cipher text.

Decrypt: $m = (c \bmod p) \bmod 2$

Correctness: because pq bigger than $2r + m$, then $(c \bmod p) = 2r + m$,

so $(c \bmod p) \bmod 2 = (2r + m) \bmod 2 = m$

Homomorphic:for two cipher text

$$c_1 = q_1 p + 2r_1 + m_1$$

$$c_2 = q_2 p + 2r_2 + m_2$$

compute:

$$c_1 + c_2 = (q_1 + q_2) p + 2(r_1 + r_2) + m_1 + m_2$$

so if $2(r_1 + r_2) + m_1 + m_2 << p$

then $(c_1 + c_2) \bmod p = 2(r_1 + r_2) + m_1 + m_2$.

so it's add-homomorphism.And

$$c_1 * c_2 = [q_1 * q_2 p + (2r_1 + m_1) + (2r_2 + m_2)]p + 2(2r_1 r_2 + r_1 m_2 + r_2 m_1) + m_1 m_2$$,

so if $2(2r_1 r_2 + r_1 m_2 + r_2 m_1) + m_1 m_2 << p$

then

$$(c_1 * c_2) \bmod p = 2(2r_1 r_2 + r_1 m_2 + r_2 m_1) + m_1 m_2$$,

so it's multiplicatively homomorphism.

Apply this encrypt scheme,we design the following cloud data secure scheme:

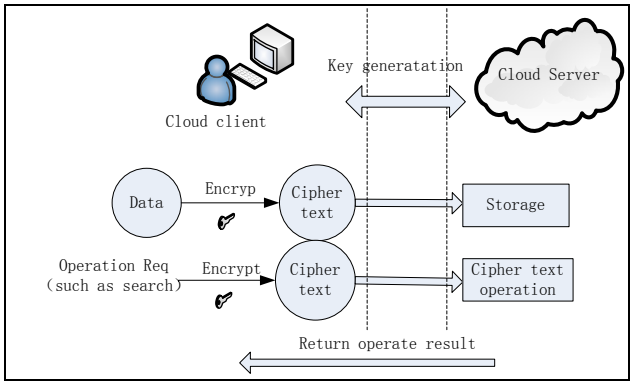

Figure 1 the data security scheme for cloud computing

As the figure 1 show,our scheme uses symmetric homomorphic encrypt to enhance data security.First,the user login and the server assign a key-generation seed to user;then user generate the secret key at client using this seed,so the server don't know the secret key at all.This procedure can be repeated then it enable the user get the same secret key at any time. Secondly the user can use this key to encrypt data which the user want to transmit and save it in the cloud server.While transmitting also other cryptograph technology such as digital signature can applied to assure the integrity and nonrepudiation.At last,the user can send request to cloud server(also encrypted) and the server do the operation even without know the content of the operation.With this scheme,not only the stored data but also the transmitted data is encrypted,so we don't worry about the data is eavesdropped or stolen.It also can provide secure data audit service because the third audit party can deal with the encrypted data directly.And the encryption we use is symmetry so we can compute it with less MIPS which is very important for thin client.The main defect of this scheme is that after encrypt the size of data because very large which will cause heavy burden for network and storage.

IV. CONCLUSION

In this paper we provide a cloud data security scheme based on the newly full homomorphic cryptograph.As the full homomorphic cryptograph can operate cipher text directly we can asure the data security and conviniencely provide cloud service.Though currently full homomorphic encrypt scheme will cause data expansion or need big compute resource,we sure with the development of modern cryptograph[9] and compute industry finally we can achieve applied full homomorphic encryp scheme.

REFERENCES

[1] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. In: Guttan J, ed, Proc. of the 19th IEEE Computer Security Foundations Workshop—CSFW 2006. Venice: IEEE Computer Society Press, 2006. 5−7.

[2] Damiani E, De S, Vimercati C, Foresti S, Jajodia S, Paraboschi S, Samarati P. An experimental evaluation of multi-key strategies for data outsourcing. In: Venter HS, Eloff MM, Labuschagne L, Eloff JHP, Solms RV, eds. New Approaches for Security, Privacy and Trust in Complex Environments, Proc. of the IFIP TC-11 22nd Int'l Information Security Conf. Sandton: Springer-Verlag,2007. 385−396.

[3] [3]Goyal V, Pandey A, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Juels A, Wright RN, Vimercati SDC, eds. Proc. of the 13th ACM Conf. on Computer and Communications Security, CCS 2006. Alexandria: ACM Press, 2006. 89−98.

[4] [4] Bowers KD, Juels A, Oprea A. Proofs of retrievability: Theory and implementation. In: Sion R, ed. Proc. of the 2009 ACM Workshop on Cloud Computing Security, CCSW 2009, Co-Located with the 16th ACM Computer and Communications Security Conf., CCS 2009. New York: Association for Computing Machinery, 2009. 43−54. [doi: 10.1145/1655008.1655015]

[5] [5] Elangop S, Dusseauaetal A. Deploying virtual machines as sandboxes for the grid. In: Karp B, ed. USENIX Association Proc. of the 2nd Workshop on Real, Large Distributed Systems. San Francisco, 2005. 7−12.

[6] [8] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In Foundations of Secure Computation, pp. 169–180, 1978.

[7] [9] Gntry C. Fully homomorphic encryption using ideal lattices. In: Mitzenmacher M, ed. Proc. of the 2009 ACM Int'l Symp. On Theory of Computing. New York: Association for Computing Machinery, 2009. 169−178

[8] [10] Marten van Dijk and Craig Gentry and Shai Halevi and Vinod Vaikuntanathan 。 Fully Homomorphic Encryption over the Integers。Eurocrypt 2010

[9] [11] Nigel Smart and Frederik Vercauteren.Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In PKC 2010,LNCS volume 6056, pages 420-443. Springer, 2010