A cloud computing security solution based on fully homomorphic encryption

Feng Zhao *, Chao Li *, Chun Feng Liu *
*GUODIANTONG CORPORATION,
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE
Ages Wealth World, No.1Hangfeng Road, Fengtai District, Beijing, 100070, China
feng_zhao@sgcc.com.cn, lichao3@sgepri.sgcc.com.cn, liuchunfeng@sgepri.sgcc.com.cn

Abstract— **With the rapid development of Cloud computing, more and more users deposit their data and application on the cloud. But the development of Cloud computing is hindered by many Cloud security problem. Cloud computing has many characteristics, e.g. multi-user, virtualization, scalability and so on. Because of these new characteristics, traditional security technologies can't make Cloud computing fully safe. Therefore, Cloud computing security becomes the current research focus and is also this paper's research direction[1].**

In order to solve the problem of data security in cloud computing system， by introducing fully homomorphism encryption algorithm in the cloud computing data security，a new kind of data security solution to the insecurity of the cloud computing is proposed and the scenarios of this application is hereafter constructed. This new security solution is fully fit for the processing and retrieval of the encrypted data， and effectively leading to the broad applicable prospect，the security of data transmission and the storage of the cloud computing[2].

Key words— **Distributed implementation、Cloud service、Cloud security、Fully homomorphic encryption;**

I. INTRODUCTION

Cloud computing is an innovative service mode. It enables users to get almost unlimited computing power and abundant a variety of information services from internet. They are distributed computing, parallel computing and grid computational evolution. This kind of new pattern refers the integration and expansion to the IT infrastructure, through the network to the required resources (hardware, platform, software), virtual integration into a reliable and high performance computing platform. In cloud computing, all users 'data are stored in the cloud resources Nodes. The results distribute to the user through the network when the user needed.

Although cloud computing has become a mature service model, and have large commercial, cloud computing is still facing many problems. In 2009, the well-known research institutions IDC release an IT report that cloud computing service is facing three major challenges: safety, stability and performance issue. Including the security problem concerns the most. The results are shown in Figure 1. A real cloud computing security incidents have profound reveals the urgency of cloud security issues, such as the 2009 Microsoft SIDEKICK service was interrupted for a week, a large number of users can not access to their email and other personal data. More seriously, due to the technical personnel not to make backups of their data, resulting in Microsoft cannot recover data. Although the cloud storage service can realize multi copy of fault tolerance and backup automatically, it is also can not do guarantee 100% security. In 2009, Google expose to the risk of mixed date by unauthorized accessing in cloud platform and unauthorized sharing user's spreadsheets date and document date. [3]

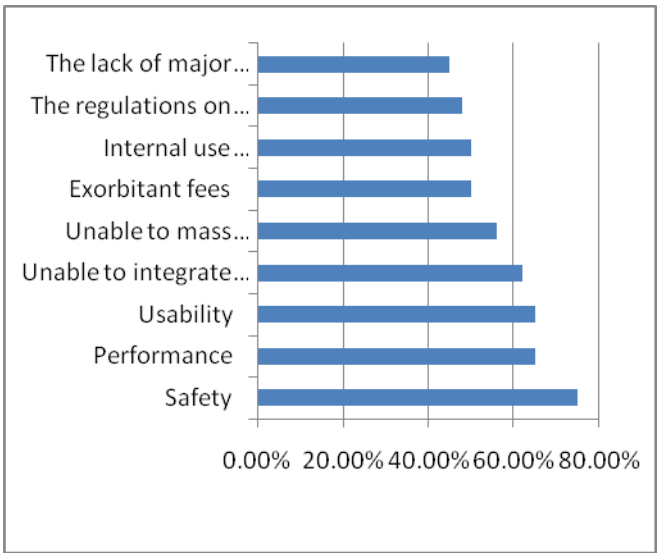

Figure1. In 2008 survey the IDC cloud computing faced problems

Three security requirements are often considered: confidentiality, integrity, and availability for most Internet service providers and cloud users. In the order of SaaS, PaaS, and IaaS, the providers gradually release the responsibility of security control to the cloud users. In summary, the SaaS modelrelies on the cloud provider to perform all security functions. At the other extreme, the IaaS modelwants the users to assume almost all security functions, but to leave availability in the hands of the providers. The PaaS model relies on the provider to maintain data integrity and

availability, but burdens the user with confidentiality and privacy control.

II. FULLY HOMOMORPHIC ENCRYPTION

A. *Principle of fully homomorphic encryption*

Craig Gentry construct homomorphism encryption scheme including 4 methods. They are the key generation algorithm, encryption algorithm, decryption algorithm and additional Evaluation algorithm.

Fully homomorphic encryption includes two basic homomorphism types. They are the multiply homomorphic encryption algorithm and additively homomorphic encryption algorithm .The multiplication and addition with Homomorphic properties. Homomorphic encryption algorithm supports only addition homomorphism and multiplication homomorphism before 2009[4]. Fully homomorphic encryption is to find an encryption algorithm, which can be any number of addition algorithm and multiplication algorithm in the encrypted data. For simply, this paper uses a symmetrical fully encryption homomorphic algorithm proposed by Craig Gentry [5].

1) Encryption algorithm: The encryption parameters p, q and r, where p is a positive odd number, q is a large positive integer, p and q determined in the key generation phase, p is an encryption key, and r is a random number encrypted when selected.

For the text m, calculation

$$c = m + 2r + pq$$

Then you can get the ciphertext.

2) Decipherment algorithm:

To plaintext

$$m = \left(c \bmod p\right) \bmod 2$$

Because the p×q is much less than $2r + m$,then

$$\left(c \bmod p\right) \bmod 2 =$$

$$\left(2r + m\right) \bmod 2 = \text{m}$$

B. *Homomorphism Verification*

1) The homomorphism additive property verification:

Suppose there are two groups of the plaintext m_1 and m_2. To encrypt them become the ciphertext.

$$c_1 = m_1 + 2r_1 + pq_1$$

$$c_2 = m_2 + 2r_2 + pq_2$$

To plaintext

$$m_3 = m_1 + m_2$$

Due to

$$c_3 = c_1 + c_2 =$$

$$\left(m_1 + m_2\right) + 2\left(r_1 + r_2\right) + p\left(q_1 + q_2\right)$$

As long as the $\left(m_1 + m_2\right) + 2\left(r_1 + r_2\right)$ is much less than[6] p , then

$$c_3 = \left(c_1 + c_2\right) \bmod p = \left(m_1 + m_2\right) + 2\left(r_1 + r_2\right)$$

This algorithm satisfies the additive homomorphic conditions

2）The homomorphic multiplicative property verification

To plaintext

$$m_4 = m_1 \times m_2$$

Due to

$$c_4 = c_1 \times c_2 =$$

$$\left(m_1 + 2r_1 + pq_1\right) \times \left(m_2 + 2r_2 + pq_2\right) =$$

$$m_1 m_2 + 2\left(2r_1 r_2 + r_1 m_2 + r_2 m_1\right) +$$

$$p[pq_1 q_2 + q_2\left(m_1 + 2r_1\right) + q_1\left(m_2 + 2r_2\right)]$$

As long as the $m_1 m_2 + 2\left(2r_1 r_2 + r_1 m_2 + r_2 m_1\right)$ is much less than p , then

$$c_4 = \left(c_1 \times c_2\right) \bmod p = m_1 m_2 + 2\left(2r_1 r_2 + r_1 m_2 + r_2 m_1\right)$$

This algorithm satisfies the multiplicative homomorphic conditions[7].

III. SECURITY ARCHITECTURE AND APPLICATION SCENE

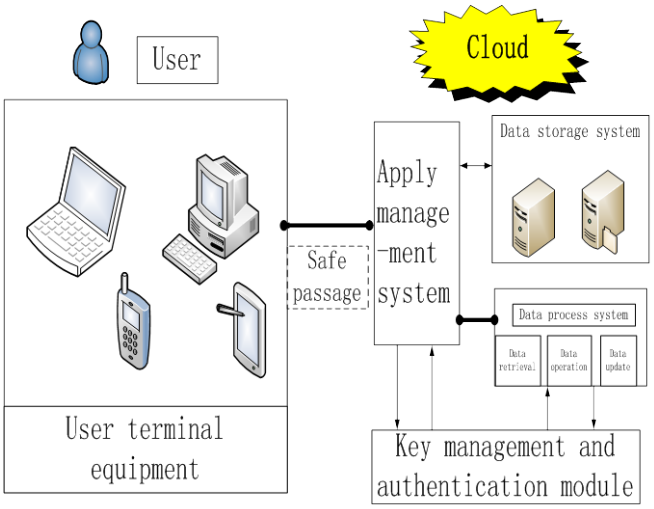

Figure2. Safety program structure diagram

1) Privacy Protection: User transmit and save their data to the cloud by encrypted. Both ensure the security of data in the process of transmission, and ensure safe storage of data. Although the cloud computing service providers handle, they can't easily obtain the information of plaintext[8].

2) Data Processing: Fully homomorphic encryption mechanism enables users or the trusted third party process ciphertext data directly , instead of the original data. Users can obtain arithmetic results to decrypt to get good data. For example, in the medical information system[9], electronic medical records are in the ciphertext is stored in the cloud server. When the health department deal with potential safety problems , they must know some areas of certain disease

location and age distribution. They can give encrypted electronic medical record data to the professional data processing services. Then they can get the correct data after decryption[10].

3) The Ciphertext Retrieval: Fully homomorphic encryption technology based on ciphertext retrieval method can search directly on the ciphertext data. It is not only ensure query privacy and improve the efficiency of retrieval, the retrieval data can be added and multiply without changing the corresponding plaintext[11].

Three generations of network defense technologies have appeared in the past. In the first generation, tools were designed to prevent or avoid intrusions. These tools usually manifested themselves as access control policies or tokens, cryptographic systems, and so forth. However, an intruder could always penetrate a secure system because there is always a weak link in the security provisioning process. The second generation detected intrusions in a timely manner to exercise remedial actions. These techniques included firewalls, intrusion detection systems (IDSes), PKI services, reputation systems, and so on. The third generation provides more intelligent responses to intrusions.

IV. CONCLUSIONS

Security problem is a big problem for the development of cloud computing, encryption is a central technology to ensure the cloud computing data security[12].

Security infrastructure is required to safeguard web and cloud services. At the user level, one needs to perform trust negotiation and reputation aggregation over all users. At the application end, we need to establish security precautions in worm containment and intrusion detection against virus, worm, and distributed DoS (DDoS) attacks. We also need to deploy mechanisms to prevent online piracy and copyright violations of digital content. We will study reputation systems for protecting cloud systems and data centers. Security responsibilities are divided between cloud providers and users differently for the three cloud service models. The providers are totally responsible for platform availability. The IaaS users are more responsible for the confidentiality issue. The IaaS providers are more responsible for data integrity. In PaaS and SaaS services, providers and users are equally responsible for preserving data integrity and confidentiality.

Based on the cloud data security problem faced, this article introduced the homomorphic encryption mechanism, proposes a cloud computing data security scheme. The scheme ensures the transmission data between the cloud and the user safety. And in the cloud storage their data is still safe. It is convenient for users and the third party agency to search date to dispose. At present, fully homomorphic encryption scheme has high computation problem needs further study[13].

V. REFERENCE DOCUMENTATION

[1] *Rivest R, Adleman L, Dertouzos M. On data banks and privacy homomorphisms [M].NewYork: Academic Press,1978:169—180.*

[2] *Jay Heiser，Mark Nicolett. Assessing the Security Risksof Cloud Computing[EBOL]. (2008—6—3)[2012—12—28]. www.gartner.com／id=685308.*

[3] *Gentry C. Fully homomorphic encryption using ideallattices[M]. New York：Association for Computing Machinery，2009：169—178.*

[4] *BEDRA A. Getting started with Google App engine and clojure[J]. IEEE Internet Computing, 2010, 14(4): 85-88.*

[5] *GENS F. IT cloud services user survey, pt.2: top benefits & challenges[EB/OL]. http://blogs.idc.com/ie/?p=210, 2012-12-01.*

[6] *Wikipedia.2009 Sidekick data loss [EB/OL]. http://en.wikipedia.org/wiki/2009_Sidekick_data_loss, 2012-12-0*

[7] *SONEHARA N, ECHIZEN I, WOHLGEMUTH S. Isolation in cloud computing and Privacy-Enhancing technologies[J]. Business & Information Systems Engineering, 2011, 3(3), 155-162.*

[8] *TALBOT D. Security in the ether[J]. Technology Review, 2010, 113(1), 36-42.*

[9] *ZISSIS D, LEKKAS D. Addressing cloud computing security issues[J]. Future Generation Computer Systems, 2012, 28(3): 583-592.*

[10] *KLEMS M, COBEN R, KAPLAN J, etal. Twenty-one experts define cloud computing [EB/OL]. http://cloudcomputing.sys-con.com/node/612375/print, 2012-12-05.*

[11] *FOSTER I, ZHAO Yong, RAICU I, etal. Cloud computing and grid computing 360-degree compared[C]. Grid Computing Environments Workshop, 2008. GCE '08, 2008: 1-10.*

[12] *VAQUERO L M, RODERO-MERINO L, CACERES J, etal. A break in the clouds: towards a cloud definition[J]. ACM SIGCOMM Computer Communication Review, 2009, 39(1): 50-55.*

[13] *Wikipedia. Cloud computing[EB/OL]. http://en.wikipedia.org/wiki/Cloud_Computing, 2012-12-05.*

First A. Author:

Feng Zhao was born in HeBei province, China, October, 14th, 1980. He was graduated from Beijing University of Posts and Telecommunications, master, majoring in automation .and now he is a PHD student in China Elect ric Power Research Institute., majoring in Electrical Engineering and Autom ation.

Second A. Author

Li Chao was born in Hubei province, China, November, 13th, 1988. He was graduated from Kunming Universiy of Science and Technology, master, majoring in Signal and information processing.

Third A. Author

Liu chun feng was born in LiaoNing province, China, July, 31th, 1981. He was graduated from Beijing University of Posts and Telecommunications, master's degree, His major is electronic and communication engineering。In 10 years, He mainly engaged in research of electric power information.