International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC 2014)

Research of Data Possession Provability Proving on Cloud Computing

Du Zhoujie
College of Information Engineering
Shanghai Maritime University, SHMTU
Shanghai, China
duzhoujie@163.com

Bi Kun
College of Information Engineering
Shanghai Maritime University, SHMTU
Shanghai, China
kunbi@shmtu.edu.cn

Han Dezhi
College of Information Engineering
Shanghai Maritime University, SHMTU
Shanghai, China
dezhihan88@sina.com

Shi Lei
College of Information Engineering
Shanghai Maritime University, SHMTU
Shanghai, China
engagesr3_junchoon@163.com

Abstract—With the rapid development of cloud computing, more and more data to be stored in the cloud storage servers. Cloud storage as a new type of storage services, with high scalability, high reliability, low cost, can be accessed anytime and anywhere features, provides a new model for mass data storage management. However, due to data are outsourcing to a cloud services provider, users are actually relinquishing the ultimate control over the fate of their data, so it faces many challenges. Data possession provability allows cloud users to verify whether their data are still integrally, validly and correctly preserved in Cloud Storage system, and whether they can obtain the data at anytime, anywhere. It is a challenging research problem of cloud storage security. This paper concluded data persistence proving model from some aspects such as general encryption scheme to the data, homomorphic encryption scheme, third-party audit (TPA) and so on. This paper discussed and summarized the existing data persistence proving schemes and models, and concluded a general model based on data persistence proving model of TPA (third-party audits).

Keywords-cloud computing;cloud security;data possession provability; third-party audits; homomorphic encryption

I. INTRODUCTION

Cloud computing[1] is a large-capacity information intensive resource pool, set of SOA, Virtualization, Software as a Service(SaaS), Platform as a Service (PaaS), infrastructure as a Service (IaaS), Web Services, grid Computing, distributed Computing, parallel computing, utility computing, and other services or computing in together, and is opening up a new technological revolution in the modern Internet. The development of cloud computing business model that involves servers, networks, storage and other infrastructure, as well as many other areas of middleware, operating systems etc, create a new IT Internet era. Although cloud computing has brought us convenience and benefits, it is also facing some critical problems need to be overcome and bearing the brunt of is security problem. In addition, in 2009,Gartner survey showed that 74% of companies' CTO said they will not use cloud computing recently, the primary reason concerns about the security of data[2] and privacy issues in cloud computing environment. Today, the computing security problem has caused widespread concern [3].

Data possession provability is an important issue in cloud computing security problems. Data possession provability mainly use current user authentication scheme to verify users' data stored on the cloud server are still complete, accurate and secure existence. Currently, there are two kind of verification methods for the data possession provability , one is the mode of cloud tenant - cloud server which the users verify by themselves; In another method is cloud users entrusted authentication authority to a third party to verify . The former validation for small amounts of data has less influence on client, and still can meet the needs of users, but for massive data this validation would take up the client computing and storage resources seriously, resulting in a sharp decline in the performance of the client. The latter put the task entrusted the credibility of the TPA to verify, so clients do not have to take responsibility for the verification users' additional computing and storage overhead task in verification.

This paper focused on data possession provability in cloud computing security issues, then researched or exploration to data possession provability issues. Finally, the paper summarized a general model based on data persistence proving model of TPA.

II. COMPARISON OF PROGRAMS ON DATA POSSESSION PROVABILITY

The traditional method of protecting the integrity of the data is mainly based on the principles of cryptography mechanisms, and makes the original data substituted or transformation of various forms by using the specified encryption algorithm to obtained completely random string sequence. If we want to get the original data information, we only need to use the corresponding decryption algorithm to restore the completely random string sequence.

The existing schemes about data integrity is different in pretreatment process to file, as well as in computing and evidence of verification. Overall indicators to measure the merits of a scheme mainly include: computational overhead, storage and communication cost, whether to support the dynamic operation, recoverability, check number, public verification and so on. The following scheme of [4-16] from above several aspects to compared, as shown in table1.

TABLE I. COMPARATIVE MEASURE OF SEVERAL SCHEMES ON REFERENCES [4-16]

Schemes	**Computational overhead**	**Storage overhead**	**Communication overhead**	**Dynamic operation**	**Recoverability**	**Public confirmatory**
reference [4]	$\Theta(1)$	$\Theta(n)$	$\Theta(1)$	NO	YES	NO
reference [5]	$\Theta(\log n)$	$\Theta(n)$	$\Theta(1)$	NO	YES	NO
reference [6]	$\Theta(m)$	$\Theta(n)$	$\Theta(1)$	A/D	--	YES
reference [7]	$\Theta(1)$	$\Theta(n)$	$\Theta(1)$	A	NO	NO
reference [8]	$\Theta(1)$	$\Theta(n)$	$\Theta(1)$	A/M/D	NO	NO
reference [9]	$\Theta(\log n)$	$\Theta(n)$	$\Theta(\log n)$	YES	NO	YES
reference[10]	$J\,\Theta(1)$	$J\,\Theta(n)$	$J\,\Theta(1)$	NO	NO	YES
reference[11]	$\Theta(1)$	$\Theta(n)$	$\Theta(1)$	YES	NO	NO
reference[12]	$J\,\Theta(m)$	$J\,\Theta(n)$	$\Theta(1)$	YES	--	YES
reference[13]	$\Theta(m)$	$\Theta(n)$	$\Theta(1)$	YES	NO	NO
reference[14]	$\Theta(\log n)$	$\Theta(n)$	$\Theta(1)$	YES	NO	YES
reference[15]	$\Theta(m)$	$\Theta(n)$	$\Theta(1)$	YES	NO	YES
reference[16]	$\Theta(m)$	$\Theta(n)$	$\Theta(m)$	NO	NO	YES

Note：n represents the number of block file chunked; m is the number of blocks about data owners request authentication data blocks; J is the number of copies under the case of multi-copies; A represents Append, M represents Modify, D represents Delete, I represents Insert.

As we can see from Table 1: the computational costs and communication overhead of POR[4], PDP[7], S-PDP[8], CS-PDP[11] are $\Theta(1)$ of magnitude, and as well as communication overhead of all scheme except D-PDP[9] and MR-PDP[10] are $\Theta(1)$ of magnitude, and the computational costs of HAIL[5], D-PDP[9] and reference[14] are $\Theta(\log n)$ of magnitude; However, because of the MR-PDP[10] need to produce j different copies, the computational costs and communication overhead compare with POR[4], PDP[7], and S-PDP[8] are more than j-1 times, but the same overall on the order of magnitude. Actually in terms of computational costs of servers, the time required from CS-PDP[11] and S-PDP[8] produce evidence is linear positive correlation with the file size. When the file is small, both CS-PDP and S-PDP have not significant difference on running time; When the file increases, the running time of CS-PDP[11] slowly growth, while the running time of S-PDP[8] increased significantly. Therefore, the model of CS-PDP[11] has a great progress than the model of S-PDP[8] on performance improvement. Storage overhead on the server, it is not much difference among the produce new upload file after the file is divided into blocks in all scheme. With the support of data dynamic nature, the program of reference [9, 11-15] is relatively good. But only scheme of POR[4] and HAIL [5] support data recoverability because they added some error correction redundant information in the sub-block data or partitioned data, it can tolerate amount of data corruption in a certain degree. And other solutions that only are able to detect whether the data exists or integrity, if users' data in server is lost or damaged there will be no way to recover the original data.

Generally speaking, there are several main differences between PDP and POR as following: PDP scheme can detect whether the stored data is integrity, but the data recoverability can not be guaranteed; POR scheme can restore the broken storage data. In fact, PDP protocol scheme as long as simply join a Forward-Error-Correcting-Codes (FECCs) can become a POR protocol [17] that supporting data recoverability; Though POR do not support the data dynamic operation, but it is support on data recoverability; However, PDP supports unlimited number of verification under the condition that the various costs or overhead are smaller, and it also supports simple and dynamic data append operation. Both POR and PDP are the most representative scheme. Some other schemes have their own advantages for specific targets, such as S-PDP on the verification overhead, D-PDP in support data dynamic operations, and MR-PDP had a certain technical advantages in terms of supporting multiple copies and so on. In addition, MR-PDP scheme extended single copy under situation of PDP. MR-PDP scheme first encrypt data, then made the encrypted data to exclusive with several different random mask.

III. EXISTING METHOD OF DATA POSSESSION PROVABILITY

A. *The programs of generally encryption mechanism*

The traditional methods of data encryption were mainly included symmetric encryption scheme and asymmetric encryption scheme.

Symmetric encryption: symmetric encryption, is an encryption technology that use the same key, often called "Session Key", to encrypt data and decrypt data, and it is used widely now. For example, DES encryption standard adopted by the U.S. Government is a typical symmetric encryption method, and its length of Session Key is 56 Bits. There are some common symmetric encryption algorithms as follows: DES encryption algorithm is a fast encryption algorithm which is useful to encrypt large amounts of data; Triple DES (3DES) encryption algorithm based on the DES algorithm can enhance security by use three different keys to encrypt a data block three times; RC2 and RC4 Symmetric algorithm is faster than DES encryption algorithm when encrypt large amounts of data with a variable-length key; International Data Encryption Algorithm (IDES) provide very strong security by using 128-bit keys; An implementation of advanced encryption standard (AES) based on Rigndael algorithm; User-oriented independently verified method of POR[18]; It is typical representative based on symmetric encryption scheme to ensure data possession that recoverable proof system POR[5] based on sentry was put forwarded by RSA company's Juels and EMC company's Kaliski and as well as the HAIL scheme in table1 all based on symmetric cryptography.

Asymmetric encryption: Encryption and decryption use different keys. There are two keys called the "public key" and "private key". Both of them must be used together, otherwise they can't open the encrypted files. Common asymmetric encryption schemes are introduced as follows: PDP, S-PDP, D-PDP, MR-PDP and so on are typically schemes based on an asymmetric encryption algorithm and the advantages and disadvantages of each scheme listed in detail in Table1. In addition, RSA asymmetric encryption algorithm invented by RSA company is a public key algorithm that support variable-length keys, and the length of file block encrypted is also variable; Digital Signature Algorithm (DSA) based on Digital Signature Standard (DSS); ECC (Elliptic Curves Cryptography) also belong to public key algorithm. It is known from the analysis of some experts or scholars to study in the ECC encryption algorithm that several parameters variable T = (p, a, b, G, n, h) often used in describes an elliptic curve encryption principle in cryptography. p, a and b are used to determine an elliptic curve, G as a base point, n is the order of G, h is represents m% n (m is the number of all points on the elliptic curve). However, the select values of these parameters directly affect to encryption security (value of p, for example, the bigger the security, but the computing speed will be slower, etc.).

B. *Scheme of homomorphic encryption mechanism*

Homomorphic encryption has always been an important topic in the field of cryptography and people only to find some part of the implement method of this operation in the past. Homomorphic encryption is a form of encryption, which allows people to make specific algebraic manipulations for cipher file and obtain a result which is still encrypted. In fact, it is the same to encrypt result that with the same algebraic manipulations on plaintext. In other words, through this technology people can obtain correct results from retrieved information and comparative analysis in the encrypted data, and in the whole process the data not need to be decrypted. Its significance is that really and fundamentally solving the private problem about entrusting data and operations to a third party, for example, the various kinds of cloud computing application and so on. Homomorphic Encryption (HE) was proposed originally in 1978 by Rivest etc. and it is a encrypt conversion technology that allow users operate the cipher files directly. And a new feasible method about "full homomorphic encryption" was proposed in a mathematical perspective in a paper[19] written in 2009 by IBM's Craig Gentry, which can do any data operations on encrypted data as on the plaintext. Its significance is that really and fundamentally solving the private problem about entrusting data and operations to a third party.

Many scholars dedicated to researching homomorphic encryption method to solve the problem of data security in the cloud. Fujian Normal University, CHEN Lan-xiang, etc. used homomorphic hash technology to achieved data possession provability[20]. The user only saves a key (K) which is 520byte and less traffic in verify process can greatly reduce the bandwidth requirements in this scheme, thus it can improve the efficiency of data possession provability. Homomorphic hash not only provide data possession provability but also provide data integrity protection; Within the cycle of data life, the user can verified data possession unlimited times, but further research need to be done on other aspects of performance exploration. Reference[21] put forward a new full homomorphic encryption mechanism based on integer, it only using addition, multiplication and modular arithmetic instead of the ideal lattice based on polynomial ring to improve the method of original ideal lattice, which can reduce the complexity and improve computational efficiency. In addition, the model of PDP used HVTs (Homomorphic Verifiable Tags) as testing meta-information or metadata. HTVs have unforgeability, homogeneity, and don't need to verify original data block. Its verification process depends on the model of challenge-response, too. Through verifying the pseudo random sampling in storage file data block, it can give a high probability of security. Here is a comparison of several aspects about the performance of the data possession provability based on homomorphic scheme, as shown in Table 2.

TABLE II. COMPARISON OF THE DATA POSSESSION PROVABILITY BASED ON HOMOMORPHIC SCHEME

Schemes	R[17]	R[6]	R[22]	R[23]
A	Yes	Yes	No	Yes
B	Insert	Yes	No	Yes
C	No	No	--	Yes
D	O(1)	0(m log n)	0(log n)	O(m)
E	O(m)	0(m log n)	0(m log n)	O(m)
F	O(1)	O(1)	O(1)	O(1)
G	O(1)	O(1)	O(1)	O(1)

Note : R represents Reference; A is representative of the public verifiability; B is representative of the dynamic nature of the data; C is representative of privacy protection; D is representative of communication overhead; E is representative of the server computational overhead; F is representative of the verifier computational overhead; G is representative of the user storage overhead; n is the number of blocks of the file; m is the number of blocks of the file to be random.

Except for the scheme listed in table 2, there are some other models of data possession provability based on homomorphic hash such as HH-PDP, V-HH-PDP and so on. But the model of HH-PDP is different from the scheme of PDP based on HTVs on file representation type; V-HH-PDP is a variant scheme obtained by simplifying and selecting some parameters of HH-PDP. Communication cost of V-HH-PDP is little and its computational efficiency is high.

Most of conventional homomorphic encryption schemes are based on public key cryptography. Although data security and data integrity has been secured, necessary computational overhead is very large especially when dealing with the case of large amount of data. There are many problems such as the restriction of the number of verification data possession, poor support of recoverability of data and low efficiency, which will also be the focus of our further research and exploration.

IV. VERIFICATION OF THIRD-PARTY AUDIT

Faced with lack of computing resources, cumbersome task, a huge amount of data and key management problems continuous bursting, the data possession provability based on cloud tenants - server model can't meet the needs of users. Thus, some experts and scholars turned eye to meet the demand of user based on the third party audits (TPA), and user replaced by a trusted third party verify data is or not exist true and completed, so reduce the burden of the client.

The third party audit (TPA) support public audit, dynamic updates and security audit features etc. For previous tenant cloud -- server model[24], this paper proposed a general data possession provability model based on third party audits, as shown in Fig .1.

Known from Fig .1, the model involves the cloud tenant (Client), cloud service provider (CSP) and third party auditor (TPA) three roles, the function of each role as follows:

1) Cloud tenant or client: Data file owner. Large amounts of original data stored in the cloud storage server by CSP provided. To confirm the integrity of the data in the cloud server, users authorize TPA checkout data integrity periodically during the lifetime of the file.

2) Cloud Service Provider (CSP): Provide cloud storage services and large amounts of data file sent by the client stored in cloud servers. It was defined as unreliable objects, but also is the object of data integrity provability challenges.

3) Third party audit (TPA): Entrusted by user and access to cloud storage server periodically verify the integrity of the data. Taking into account the aspect of data privacy protection, TPA can't access to the data directly or obtain data from the validation process.

From above Fig .1, the process of data possession provability model based on TPA is as follows:

Step ① : User submitted the original data to preprocessing module before the user data is stored.

Step ② :The part of the dashed box in Fig .1, Firstly user pre-processing original data at a certain (the data block, encryption of data , and metadata information extracted etc, there are a variety of operation methods), then obtained persistent data used to store and metadata after pretreatment used to verify data possession provability.

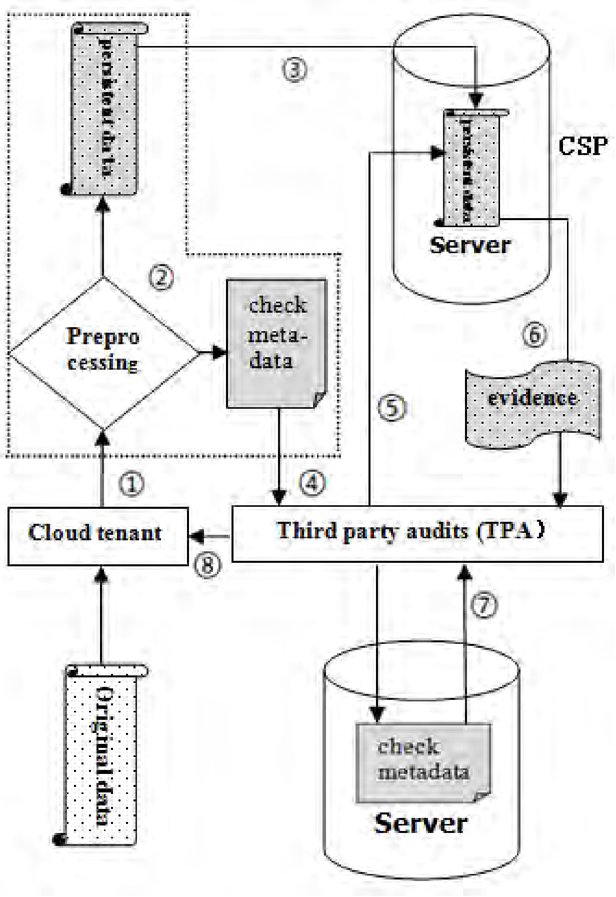

Figure 1. Data possession provability model based on TPA (third-party audits).

Step ③and step ④ warehousing the processed data respectively, in other word, persistent data into the database of CSP provided to be persistent stored and validation metadata stored in the database provided by TPA which used for verification of data possession.

Step ⑤: TPA sent out a challenge to CSP, which apply to verify the integrity and possession of the data in storage.

Step ⑥: CSP received challenge of TPA and deal with the persistent data in storage for specific processing to extract evidence about persistent data integrity existed in storage server, which sent the evidence to TPA in the form of response.

Step ⑦: TPA received evidence come from CSP and removed metadata of persistent data integrity from the database of TPA to verify data possession and compare evidence of CSP provided is consistent.

Step ⑧: Send the comparison result of the previous step to the cloud tenant or client.

Compared with the traditional model about the mode of client/server, the model of this paper alleviate the burden on the user, which take the validation of all the work about data possession provability should had done by user to the TPA to complete, especially when the data stored in storage is larger , the more obvious advantages. While TPA send a challenge to CSP, also just send a small challenge of information. However, CSP using its powerful computing ability to generate evidence of persistent data integrity exists about users to stored in storage as response to TPA when CSP receiving TPA challenge. Compared the produce evidence of CSP to TPA and send the results of verification back to the user. TPA workload moderate in the whole process and not access to the user's original information, so that data security is guaranteed and also the data possession provability has been verified. Therefore, considering from the viewpoint of safety, this model is particularly suited to data storage and verification of data possession provability in the cloud computing.

V. THE MODEL AND PROCESS OF THIRD PARTY CERTIFICATION

The model of data possession provability based on third-party audits can effectively prove the existence and integrity of the data in storage, a trusted third party is essential. How can make the third party becomes a trusted to user? It is do a series of certification about third party to above model of data possession provability, user can be accessed to the corresponding data in server which only in a certain order certification passed the certification of all, or denied access as long as there is one authentication failure. By the above model of data possession provability based on third-party audit simplified out the model of verification about third-party certification as shown in Fig .2.

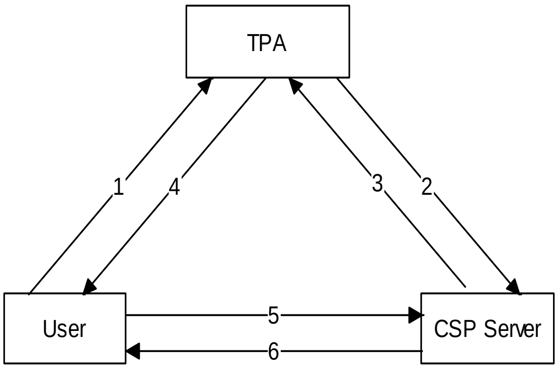

Figure 2. Model of calibration based on third party certification .

1). The user sent their own authentication information to the TPA, which will do a authentication for user identity.

2). TPA asked for authentication information request to the CSP about user access to server of CSP provided.

3). CSP sent own certificate to TPA, so that TPA made a certification for CSP.

4). TPA will be sent certified results to the user, which decided whether the user can continue or not the following certification.

5). The user will be sent application requests certificate to the CSP Server and requesting certification.

6). CSP sent the authentication result back to the user, which to decide whether allow users request access or not.

In the model of authentication as shown in Fig .2, we can first do a judge for user and determine whether the user is first put forward access request or not, if the access request is proposed by a new user, and not retrieved his any previous authentication information, we should make a series of certification for him. Only after passed all authentication users can obtain the corresponding access rights. If the user had passed the relevant certification at previously, just to authenticate the user's request of application, passed authentication and request of user is accepted. It can increase the efficiency of the model of certification that do a judgment before the user first authenticated, we can improve the certification efficiency of this model in this way. The specific certification process is shown in Fig .3.

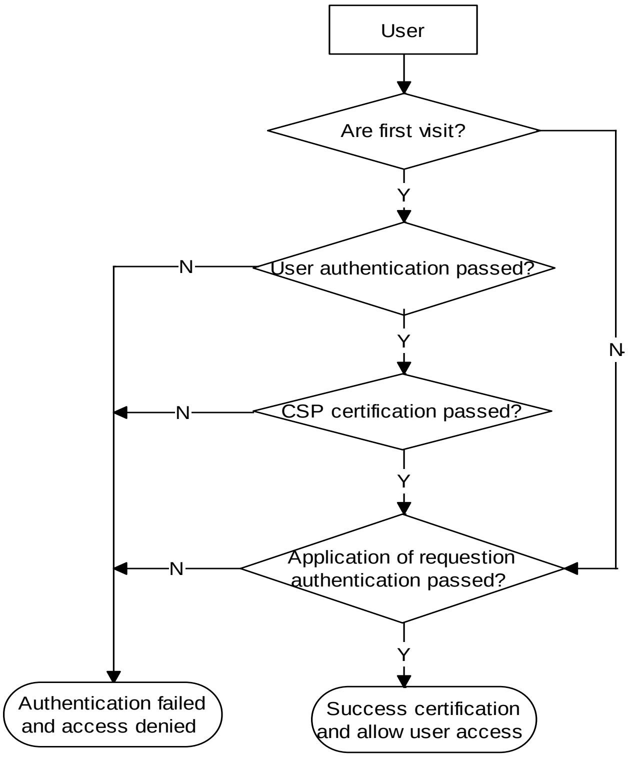
User
Are first visit?
Y
N
User authentication passed?
Y
N
N
CSP certification passed?
Y
N
Application of requestion authentication passed?
N
Y
Authentication failed and access denied
Success certification and allow user access

Figure 3. The process of certification .

VI. CONCLUSIONS

The development of cloud computing has been overwhelming and the needs of user are constantly changing. Data security issues become increasingly prominent, which is a bottleneck problem in the history of cloud computing on the development road. The scheme of data possession provability under the mode of cloud Tenant--server, the users have a certain control over the data, but the data integrity check must be done by users themselves and increasing the burden of users and the experience user is worse especially when the number of data is very large. However, it is reduce the burden of user apparently under the basis of the third party audit (TPA) mode, but the user give the rights of control to TPA and lost control to data, but introduce TPA at the same time, as well as increases the risk of other aspects. There is still no a scheme can be fully efficiently applied to verify the integrity of data that the main problems in computational overhead expenses, data transmission, data dynamic (update operation is supported or not), finite verification, publicly verifiable, privacy protection and many other aspects. Although there are many schemes which can meet several conditions of, still can’t solve above of all the defects mentioned. For example, the schemes based on RSA have very big advantage in unlimited verification and integration of verify metadata, but there is a big problem in the computational overhead expenses. The current schemes can’t be a better balance between client and authenticator, if one of the parties to keep the cost at a low level, the other party would need to pay the higher cost. How to enable client and authenticator both achieve excellent at the same time, which will also become the focus of our research and exploration.

ACKNOWLEDGMENTS

This work was partly supported by National Natural Science Foundation of China (No. 61373028 and No. 61070154); Innovation Program of Shanghai Municipal Education Commission (12ZZ153); Science & Technology Program of Shanghai Maritime University (20130471).

REFERENCES

[1] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security [J].Journal of Software, 2011,22(1) : 71-83.(in Chinese)

[2] YU Neng-hai, HAO Zhuo, XU Jia-jia, ZHANG Wei-ming, ZHANG Chi. Review of Cloud Computing Security [J].ACTA ELECTRONICA SINICA, 2013,41(2):371-379.

[3] 2011RSA International Forum on Information Security Conference, 2011.11.2.

[4] ARI J, BURTON K. PORs: proofs of retrievability for large files [A].14th ACM Conference on Computer and Communications Security[C]. Alexandria, VA, USA, 2007.584-597.

[5] BOWERS K D, JUELS A, OPREA A. HAIL: A high-availability and integrity layer for cloud storage [A].16th ACM Conference on Computer and Communications Security[C]. 2009. 187-198.

[6] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores. Proc of CCS'07. New York: ACM, 2007:598-609

[7] ATENIESE G, BURNS R, CURTMOLA R. Remote data checking using provable data possession[J]. ACM Transactions on Information and System Security, 2011, 14(1): 12-34.

[8] ATENIESE G, PIETRO R D, MANCINI L V. Scalable and efficient provable data procession [A].4th International Conference on Security and Privacy in Communication Networks[C]. Istanbul, Turkey, 2008.1-10.

[9] CHRIS E, ALPTEKIN K, PAPAMANTHOU C. Dynamic provable data procession [M]. ePrint Archieve, 2009.

[10] CURTMOLA R, KHAN O, BURNS R. MR-PDP: Multiple replica provable data possession [A].28th IEEE International Conference on Distributed Computing Systems[C]. Beijing, China, 2008.411-420.

[11] LIU Hua-nan,WANG Shi-qing. Design and Analysis of Provable Data Possession Model in Cloud Storage [J].Computer Applications and Software, 2012, 29(10):222-226.

[12] RONG Li, LI Lei, LI Chao-ling. Extensible provable data possession scheme with data dynamics [J]. Application Research of Computers, 2013, 30(7):2132-2135.

[13] LIU Fei-fei,GU Da-wu,Lu Hai-ning. An improved dynamic provable data possession model[C]//Proc of IEEE International Conference on Cloud Computing and Intelligences Systems．2011 : 290—295.

[14] WANG Qian, WANG Cong, REN Kui, et a1.Enabling public auditability and data dynamics for storage security in cloud computing[J].IEEE Trans on Parallel and Distributed Systems,2011,22(5):847—859.

[15] HAO Zhuo,ZHONG Sheng,YU Neng- hai. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability[J].IEEE Trans off Knowledge and Data Engineering.2011.23(9): 1432-1437.

[16] WANG Cong,WANG Qian,REN Kui, et al. Privacy-preserving public auditing for data storage security in cloud computing[C]//Proc of IEEEINFOCOM. 2010:1-9.

[17] Ateniese G, Burns R, Curtmola R, et al. Remote data checking using provable data possession. ACM Trans. Inf. Syst. Secur, 2011, 14(1):1-34

[18] Gentry 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.

[19] GENTRY C. Fully homomorphic encryption using ideal lattices [A].Proceedings of the 41st Annual ACM Symposium on Theory of Computing [C]. New York,2009.169-178.

[20] CHEN Lan-xiang. A Homomorphic Hashing Based Provable Data Possession [J]. Journal of Electronics & Information Technology, 2011, 33(9):2199-2204.

[21] Marten van Dijk, Craig Gentry, Shai Halevi, et al. Fully Homomorphic Encryption over the Integers[C]//Proc of Cryptology-CRYPTO, 11. [S. l.]: Springer-Verlag, 2011: 24-43.

[22] K. Zeng. Publicly Verifiable Remote Data Integrity Information and communications Security, vol. 5308,L. Chen, et al., Eds., ed: Springer Berlin /Heidelberg, 2008: pp. 419-434.

[23] Dodis Y, Vadhan S, Wichs D. Proofs of retrievability via hardness amplification.In TCC’09. San Francisco, CA, USA, 2009: 109-127.

[24] FU Wei,YE Qing,CHEN Ze-mao,WU Xiao-ping. Survey of data possession provability proving on cloud storage[J]. Journal on Communications,2012,33(Z2):201-206.