ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 9, September 2017

Disparate Key Pattern And Data Integrity Checking For Secure Cloud Storage

[1] M.Subhashini, [2] Dr.A.Muthukumaravel, [3] T.Baskar
[1] Research Scholar Department of Computer Science, Bharath University, Chennai.
[2] Head, Department of MCA, Bharath University, Chennai.
[3] Asst. Professor, Dept. of Computer Science, Pachaiyappa's College for men, Kanchipuram.

Abstract: **In this paper we propose an efficient and flexible distributed storage integrity checking mechanism, which uses the token and the cancellation code of the key distinctive pattern homomorphic data. The proposed project allows amendment cloud storage accounts users at a cost of communication and lightweight computing. Customers want to store their data in a public cloud server (PCS) together with the rapid development of cloud computing. The new security issues need to be resolved to help more customers to process their data in the public cloud. When the client is limited to PCS access, delegate their proxy to process the data and load. On the other hand, the remote control data integrity is also an important security issue in the public cloud storage. It makes customers to check whether their outsourced data remains intact without downloading all data. By security problems, we propose a new data proxy form burden-oriented and integrity control of remote data in public key cryptography based on the load identity data driven by proxy based on the identity and integrity checking remote public cloud data (ID-PUIC). The analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, the malicious attack data editing and even collusion server attacks..**

Keywords: Data integrity, distributed key, auditing, data secure, key generation, proxy.

I. INTRODUCTION

Cloud computing is a virtualized resource that we store all our data security measures, so that application software can obtain the full benefits of this without hard drive technology and our local server for data storage. It provides a way to store and share data as a service on the Internet. It allows multiple data exchange capacity. There is an increase in the use of the cloud in various organizations to increase their efforts to share data and reduce maintenance costs. The data exchange is an important function in the cloud storage. Therefore, it is necessary for the exchange of data between users is efficient and safe. It was recognized that data encryption provides a better solution for this problem.

In the public cloud computing, customers store theirdata on remote servers in the public cloud. Since the stored data is beyond the customer's control, it involves security risks in terms of confidentiality, integrity and availability of data and services. Remote Control Data integrity is a primitive that can be used to convince cloud customers that their data will remain intact. On the other hand, the remote data integrity verification protocol must be efficient to make it suitable for terminal devices with limited capacity. Therefore, on the basis of identity-based encryption public and delegation public key cryptography, the ID-PUIC study protocol.

The main contributions are as follows: in the public cloud, this paper focuses on data-oriented identity-based proxyLoad and checking for the remote data. In some special cases, the owner of the data may be limited to access to public cloud server, the data holder will delegate the task of data processing and the load to a third party, for example, the proxy. Using the public key cryptography based on identity, our proposed protocol ID-PUIC is efficient because the certificate is deleted Management. ID-PUIC is a load of proxy-oriented data models and integrity of remote data novelty public cloud. We have a formal system model and security model for ID-PUIC protocol. Then, based on the bilinear pairs, we designed the first specific protocol ID-PUIC. In the random oracle, our ID-PUIC protocol designed is definitely safe. Based on the authorization of the original customer, our protocol can make managing public and private verification check.
PKI protocol remote data integrity check (Public Key Infrastructure) will perform certificate management. When the manager delegates some entities to perform the integrity check of remote data, generate considerable overhead, since the verifier checks the certificate during inspecting the integrity of remote data. In PKI, the considerable overhead come from certified

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 9, September 2017

heavy verification, certificate generation, delivery, withdrawal, renewals, etc. In cloud computing public, the terminal devices may have low computing power, such as mobile phones, iPad etc. Based on public key cryptography can eliminate the complex certificate management. In order to increase the efficiency, the transfer of the proxy on the basis of data based on the identity and integrity of the remote control data is more attractive.

Therefore, it is very necessary to study the PUIC-ID protocol.

Representative network architecture for cloud data storage is illustrated in Fig. 1.

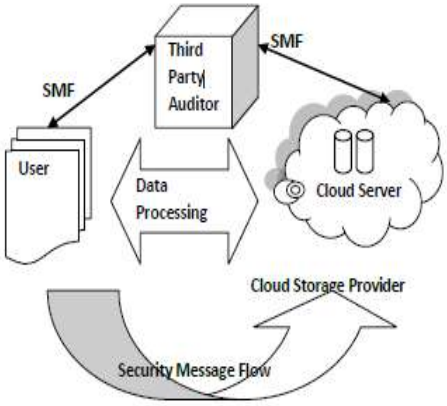


Fig 1: Cloud Data Storage architecture

Three different network entities can be identified as follows:
• Client: Entity, which has large data files to be stored in the cloud and is based on the cloud for the maintenance of data and the calculation can be both for individual consumers or organizations.
• Cloud Storage Server (CSS): An entity that is managed by the Cloud Service Provider (CSP), has an important Storage Resource Computing to maintain customer data.
• Third Party Auditor (TPA): An entity that has experience and capabilities that customers do not have, is trusted to assess the risk and expose the cloud storage services on behalf of customers on request.

Important security problem.Since the data of mass customers are beyond their control, customer data can be corrupted by malicious server cloud, intentionally or not.
To address the new security problem, some efficient models are presented. In 2007, Athenian et al. It proposed the paradigm demonstrable possession of the data (PDP). In the PDP, the tester can check the integrity of remote data without retrieving or download the full data. PDP is a probabilistic test inspecting the integrity of remote data by sampling random blocks of a public cloud server, which drastically reduces the cost of I / O Tester can perform the data integrity checking, keeping a small distance metadata.

A company may grant proxy access to a portion of confidential data. The difficult question is how to share encrypted data. Of course, users can download the storage of encrypted data, decrypt and send others to share, but lose the value of cloud storage. Users should be able to delegate access rights to share with others so they can access this data directly from the server data.
However, finding a safe and effective way to share the partial data storage in the cloud is not trivial. Because of the different data protection mechanisms to escape the possibility of privacy encrypt all data with their own keys before boarding.

Therefore, the best solution to the above problem is that the owner encrypts files with various public keys, but it sends a unique decryption key (distinctive pattern) to delegate only. Since the decryption key must be sent through a secure channel and kept secret. There are proposals for additional levels of security to protect you from misuse of the data by the cloud providers.

Allow customers to realize the full potential of cloud vendor is perfectly creating a platform for managing trusted cloud, governed and secured between the supplier and the consumer cloud services. The main advantage of using the third mayor in this scenario is its ability to integrate more than one provider.

Unlike most previous work to ensure the integrity of remote data, the new system supports safe and efficient operations in dynamic data blocks, including: update, delete and add. A full analysis of safety and performance shows that the proposed scheme is highly efficient and resistant against Byzantine failure, the malicious attack data editing and even collusion server attacks. The easiest and most obvious way to support these operations is that the user to download all data from the cloud server and recalculate full parity blocks and verification witnesses. You can always ask the servers that send blocks of the rows specified in the challenge and regenerate the correct blocks to correct the deletion. We believe that the data storage Security of Cloud Computing, an area full of challenges and of fundamental importance, is still in its infancy now, and have not yet been identified many research problems.

We can construct a scheme to achieve both publicverifiability and storage correctness assurance of dynamic data.

I. THE PROPOSED MODEL

ORIGINAL CLIENT:

The original customer is an entity that will act as a load of mass data on the server's public cloud (PCS) by the delegate proxy, and the main purpose is to verify the integrity of massive data will be through remote control. For the upload and download of data client must follow the following process steps:

The customer can view the files in the cloud and also for download.

The client must upload the files with certain attributes required by the encryption key.

Then the customer must make the request to the TPA and proxy to accept the request to download and ask for the secret key that will be given by the TPA.

After receiving the secret key the client can be downloaded.

PUBLIC CLOUD SERVER:

PCS is an entity that is managed by the cloud service provider. PCS is the important resource of cloud storage and computing to keep the data of mass customers.PCS can see all the customer details and upload a file that is useful for the customer and make the storage of files uploaded by the client.

PROXY

Proxy is an entity, which is authorized to process the Original Client's data and upload them, is selected and authorized by Original Client. When Proxy satisfies the warrant mω which is signed and issued by Original Client, it can process and upload the original client's data; otherwise, it cannot perform the procedure.Simply say means: without the Knowledge of Proxy's authentication and verification and acceptance of proxy client cannot download the file which is uploaded by the Client.

KGC

KGC (Key Generation Center): an entity, when receiving an identity, it generates the private key which corresponds to the received identity.Generated Secret key is send to the client who is make the request for the secret key via mail id which is given by the Client.

II. MATH

A key aggregate encryption scheme consists of five algorithms in polynomial time as follows. The owner sets the public system parameter data via the installer and generates a pair of public / master key secret3 through keygen. Messages can be encrypted using encryption by anyone even decide what kind of cipher text is associated with the plaintext message to be encrypted. The owner of the data can use the master secret to generate a decryption key added to a collection of encrypted text extracted classes. Finally, any user with a key can decrypt added more and ciphertext as ciphertext class is contained in the aggregate through key Decrypt4.

• Setup(1λ, n): Executed by the holder of the information to set up an account in an untrusted server. When you enter a backup file the level of 1λ parameter and the number of classes n ciphertext (that is, the class index must be an integer

defined by 1 en), outputs the public system parameter parameter, which is omitted from the entrance of the other algorithms for brevity .

• KeyGen : Performed by the data owner to randomly generate a pair of public / master-secret key (pk, MSK).

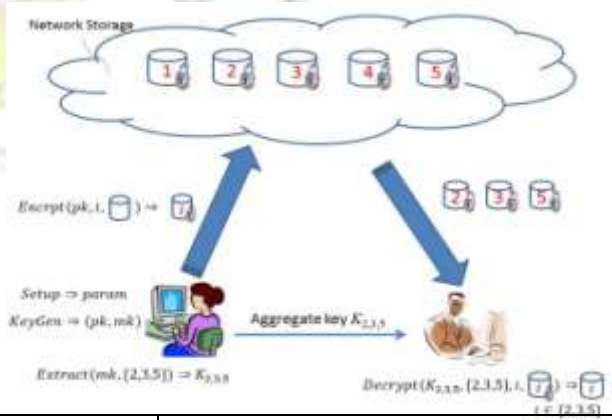
• Encrypt(pk, i,m):Performed by anyone who wishes to encrypt data. Introducing a public key pk, an index i indicates the class encrypted text and a message m, emits a ciphertext C.

• Extract(msk, S): Performed by the data owner to delegate the power to decipher a certain set of classes encrypted text to a delegate. Inserting the key MSK mastersecret S and a set of indices for the different classes, it gives the aggregate for the set of S designated KS keys.

• Decrypt(KS, S, i, C): It performed by a delegate who received an inert KS key extraction generated. In KS input, the set S, an index i indicates the ciphertext to the ciphertext C to class C belongs, and,
ISSUES the M decoding result if i ∈ S. There are two functional requirements:

• In fairness Any integer and λ n, Any Together S ⊆ {1, ⋯, n}, Any index i ∈ S and EVERY Message m,
Pr [Decrypt (KS, S, I, C) = m: param ← Configuración (1λ, n), (PK, MSK) ← KeyGen (), C ← Encrypt (pk, i, m)
KS ← Extract (MSK, S)] = 1.

Compactness For any integers λ, n, any set S, any index i ∈ S and any message m; param ← Setup(1λ, n), (pk, msk) ← KeyGen(), KS ←Extract(msk, S) and C ← Encrypt(pk, i,m); |KS| and |C| only depend on the security parameter λ but independent of the number of classes n.



	Decryption keysize	Ciphertextsize		Encryption type
Key assignment schemes most likely non-constant constant symmetric or public-key for a predefined hierarchy	most likely non-constant constant symmetric or public-key for a predefined hierarchy ((depends on the hierarchy)		Constant	Symmetric or public key
Symmetric-key encryption with Compact Key	Contant	Constant		Public key
IBE with Compact Key	constant	Non-constant		Symmetric key
Attribute-Base d	Non constant	Constant		Symmetric key

Encryption (e.g., [10])			
KAC	constant	Constant	Symmetric key

- Cloud storage at a cost of communication and lightweight computing.
- The proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append.
- The private cloud gets the proxy-key and the authorization of the original client through the interaction between the original client and its private cloud.
- To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users

III. . CONCLUSION

Overall we produce andisparatekey pattern Cryptosystem which produces effective constant size private key by means of derivations of different cipher text classes.Proposed approach proves more secureand efficient cryptographic scheme in which we have an effective derivation of secret key generation and key management for the outsourced Cloud data.The private cloud gets the proxy-key and the authorization of the original client through the interaction between the original client and its private cloud.To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users.

REFERENCES

[1] Z. Fu, X. Sun, Q. Liu, L. Zhou, And J. Shu, “Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search Over Encrypted Cloud Data Supporting Parallel Computing,” Ieice Trans. Commun., Vol. E98-B, No. 1, Pp. 190–200, 2015.

[2] Y. Ren, J. Shen, J. Wang, J. Han, And S. Lee, “Mutual Verifiable Provable Data Auditing In Public Cloud Storage,” J. Internet Technol., Vol. 16, No. 2, Pp. 317–323, 2015.

[3] M. Mambo, K. Usuda, And E. Okamoto, “Proxy Signatures For Delegating Signing Operation,” In Proc. Ccs, 1996, Pp. 48–57.

[4] E.-J. Yoon, Y. Choi, And C. Kim, “New Id-Based Proxy Signature Scheme With Message Recovery,” In Grid And Pervasive Computing (Lecture Notes In Computer Science), Vol. 7861. Berlin, Germany: Springer- Verlag, 2013, Pp. 945–951.

[5] B.-C. Chen And H.-T.Yeh, “Secure Proxy Signature Schemes From The Weil Pairing,” J. Supercomput., Vol. 65, No.2, Pp. 496–506, 2013.

[6] X. Liu, J. Ma, J. Xiong, T. Zhang, And Q. Li, “Personal Health Records Integrity Verification Using Attribute Based Proxy Signature In Cloud Computing,” In Internet And Distributed Computing Systems (Lecture Notes In Computer Science), Vol. 8223. Berlin, Germany: Springer-Verlag, 2013, Pp. 238–251.

[7] H. Guo, Z. Zhang, And J. Zhang, “Proxy Re-Encryption With Unforgeable Re-Encryption Keys,” In Cryptology And Network Security (Lecture Notes In Computer Science), Vol. 8813. Berlin, Germany: Springer-Verlag, 2014, Pp. 20–33.

[8] E. Kirshanova, “Proxy Re-Encryption From Lattices,” In Public-Key Cryptography (Lecture Notes In Computer Science), Vol. 8383. Berlin, Germany: Springer-Verlag, 2014, Pp. 77–94.

[9] P. Xu, H. Chen, D. Zou, And H. Jin, “Fine-Grained And Heterogeneous Proxy Re-Encryption For Secure Cloud Storage,” Chin. Sci. Bull., Vol. 59, No. 32, Pp. 4201–4209, 2014.

[10] S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, And K. Matsuura, “Re-Encryption Verifiability: How To Detect Malicious Activities Of A Proxy In Proxy Re-Encryption,” In Proc. Ct-Rsa Conf., Vol. 9048. 2015, Pp. 410–428.