Strategic Based Encryption for Protecting Storage Data in Cloud Service Provider

[a]G.Sudhakar, [b]M. Swapna
[a]Associate Professor, Dept of CSE, JNTUH, Hyderabad, TS, India
G. SS
[b].Associate Professor, Dept of CSE, Aurora's Scientific Technological & Research Academy, Hyderabad, TS, India.

Abstract

With the recent adoption and diffusion of the data storage in Cloud services or online social networks are generally hosted by third parties where data can be stored and shared. There have been increasing demands and concerns for distributed data security. One of the most changing issues in data storage systems is the enforcement of access polices and the suitable actor. To avoid the unauthorized access, data should be encrypted before outsourcing. Strategy based encryption (PBE), actor based policies can be generated and based on the policies provide the data access permissions. In this system provide the security based on the policies, access data suitable actor give the permission into third party auditor (TPA). A data owner uploads the data with multiple files. Give the data permissions based on the suitable actor access the data in cloud before access the data first must have access strategy and revocation should done with the permission of the data owners. Another major process is the key providing and transporting. Here provide the strategy based encryption technique and manage the suitable actor data. The data stored in the cloud is encrypted using key providing based on the access permission assigned to the data and strategy actor of the owners share the data with highly security and efficient using strategy based encryption technique.

KEYWORDS- Protection Storage, Strategy Based, Encryption, Data Confidentiality.

I. Introduction

Cloud computing is a general term for anything that involves delivering hosted services, scalable services like data sharing, accessing etc., it actor the web and central remote servers to maintain data and applications Cloud computing allows consumers and businesses to use applications without installations. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with web access. Reasoning processing is a new processing paradigm that is built on virtualization, parallel and allocated processing, utility processing and service oriented architecture. In the last several years, cloud processing has emerged as one of the most influential paradigms in the IT industry, Reasoning processing is a concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage space is managed. It focuses on designing cloud storage space for sturdiness, privacy, and functionality.

The cloud storage space program is considered as a large scale allocated storage space program that consists of many independent storage space web servers. Information sturdiness is a major requirement for storage space systems. One way to provide data sturdiness is to replicate a concept such that each storage space server stores a copy of the

concept. It is very robust because the concept can be retrieved as long as one storage space server survives.

Another way is to encode a concept of k signs into a code-word of n signs by erasure coding. To store a concept, each of its code-word signs is stored in a different storage space server. After the concept signs are sent to storage space web servers, each storage space server individually computes a code-word symbol for the received concept signs and stores it. This finishes the development and saving process. The recovery process is the same. The program model that consists of allocated storage space web servers and key web servers. Since saving cryptographic important factors in a single device is risky, a customer distributes his cryptographic key to key web servers that shall perform cryptographic functions on behalf of the customer. The method of threshold proxy re-encryption scheme and integrate it with a protection decentralized code to form a protection allocated storage space program.

The protection scheme supports development operations over encrypted information and sending operations over encrypted and encoded information. The tight integration of development, protection, and sending makes the storage space program efficiently meet the requirements of information sturdiness, data privacy, information sending. The storage space web servers individually perform development and re-encryption and key web servers individually perform partial decryption. The parameters are flexible adjustment between the number of storage space web servers and sturdiness.

II. Problem statement

Storing data in a third party's cloud program causes serious concern on data privacy. To provide strong privacy for information kept in storage space web servers, a customer can encrypt information by a cryptographic method before applying an erasure code method to encode and store information. When he wants to use a concept, he needs to retrieve the codeword signs from storage space web servers, decode them, and then decrypt them by using cryptographic important factors. There are three problems in the above straightforward integration of protection and development. First, the customer has to do most computation and the communication traffic between the customer and storage space web servers is high. Second, the customer has to manage his cryptographic important factors.

If the user's device of saving the important factors is lost or compromised, the protection is broken. Finally, data saving and retrieving, it is hard for storage space web servers to straight support other functions. For example, storage space web servers cannot straight forward a user's information to another one. The owner of information has to retrieve, decode, decrypt and then forward them to another customer. It addresses the problem of sending data to another customer by storage space web servers straight under the command of the information owner as shown in Fig.1. In contrast to traditional solutions, IT services are under proper physical, logical and personnel controls, where Reasoning Computing moves the application software and databases to the large data centers, where the information and services may not be fully trustworthy.

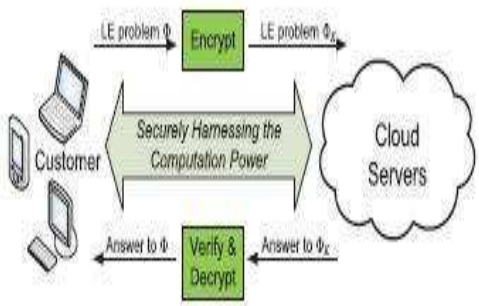

Fig 1.Aritecture of Protection Strategy Based Encryption.

This unique attribute, however, poses many new protection challenges which have not been well understood. The customer doesn't have the privacy for preserving the information and the protection risks towards the correctness of the information in cloud which may not be possible. From the perspective of information protection, which has always been an important aspect of quality of service, Reasoning Computing inevitably poses new challenging protection threats for number of reasons. The traditional cryptographic primitives for the purpose of details security protection cannot be directly implemented due to the users' loss control of details under Reasoning Processing. Therefore, confirmation of correct details storage space in the cloud must be performed without precise details of the whole details. Considering various kinds of details for each user saved in the cloud and the demand of long lasting ongoing guarantee of their details safety, the problem of confirming correctness of details storage space in the cloud becomes even more challenging. And the Reasoning Processing is not just a third celebration details factory. The details saved in the cloud may be frequently modified by the users, including placement, removal, modification, appending, reordering, etc. To make sure storage space correctness under powerful details upgrade is hence best.

III. Third Party Auditing

In this audit stage, the auditor continuously checks the saved details using a challenge-response method. Each examine determines the data's reliability immediately before the examiner. We will also show how to handle the protection details and security key, one after the other. During audit, the primary risk which may occur in the storage space support is that it lost some part of the details which can be protection and security important factors added with some harmful details and can deceive the auditor into knowing that it has both. It may deceive the auditor in two primary ways (1) by adjusting the current and cached past difficulties the auditor provides or (2) by mixing these difficulties and produced principles from the details or the security key, such that the protection details and security key cannot be entirely retrieved from the produced principles. Thus, for both the protection details and security key, we need to confirm two qualities to make sure details integrity:

- **Completeness:** After getting details, if the support
- offers all the pieces of the protection details and security key, the auditor allows the reactions.
- **Soundness:** After getting the details, if the supportis missing any bit in the protection details or security key, the auditor allows with minimal probability.
- The primary risk from the auditor is that it may obtain important info from

the audit process that could bargain the comfort assures provided by the support. For example, even a few pieces from a file containing health background could reveal whether a customer has a disease. To make sure comfort, we depend on different requirements for the protection details and the security key. For the details, we depend on (1) the strength of the security plan and (2) the zero-knowledge property of the method for encryption-key audits. Thus, we must confirm the encryption-key audits with the support that can be efficiently simulate such that the auditor's connections is indistinguishable from one with a true support.

A. Encrypted Data Verification

We use a simple challenge-response method to examine the protection details as described in method.

A chooses any Rj ,Hj from L and L = L\ {(Rj , Hj)}.

A! S: Rj.
S computes Hs = HMAC (Rj, EK (M)).
S -> A: Hs.
A checks Hs = Hj else declares S lost data.

B. Security Key Verification

To determine if the encryption key is unchanged, we have several options. One option is to evolve current recognition techniques to confirm the support has K without exposing K. For example, method uses the Schnorr recognition plan to show that the support still has K.

Schnorr's plan is complete and sound. For soundness, the support can deceive the auditor into recognizing with probability < 1/2t. But, this method is only provably zero-knowledge if the auditor genuinely follows the method.

A selects a unique β s.t. 1 < β < q and determines gβ.
A ->S :Va = gβ.
S determines Ws = (Va)K = gβK .
S ->A : W .

A determines Wa = (gK)β

A assessments Wa = Ws else states S lost key.

IV. Modules

A. System Model

User: customers, who have information to be saved in
the reasoning and rely on the reasoning for information calculations, involve both individual customers and
companies.

Cloud Service Provider (CSP): a CSP, who has significant resources and skills in building and handling allocated reasoning storage space web servers, functions and functions live Cloud Processing systems.

Third Celebration Auditor (TPA): an optionally available TPA, who has skills and abilities that customers may not have, is reliable to evaluate and reveal risk of reasoning storage space services on part of the customers upon demand.

B. Cloud Functions

Upgrade Operation: In reasoning information storage space, sometimes the customer may need to alter some information block(s) saved in the reasoning, we relate this function as information update. In other words, for all the rarely used wedding party, the customer needs to remove every incident of the old information prevent and substitute it with the new one.

Remove Operation: Sometimes, after being saved in the reasoning, certain information prevents may need to be removed. The delete function we are considering is a general one, in which customer changes the information prevent with zero or some unique arranged information icon. From this perspective, the delete function is actually a unique case of the information update function, where the original information prevents can be changed with 0's or some pre-specified unique prevents.

Add Operation: In some cases, the customer may want to enhance his saved information by adding prevents at the end of the computer file, which we relate as information append. We anticipate that the most Frequent append function in reasoning information storage space is large append, in which the customer needs to publish a huge variety of prevents (not a single block) at one time.

C. Computation Outsourcing Security

Another fundamental service enabled within the cloud paradigm is computation outsourcing. By outsourcing workloads to the cloud, users' computational power is no longer limited by their resource-constrained devices. Instead, they can enjoy the cloud's literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays locally. However, current outsourcing practice operates in plaintext — that is, it reveals both data and computation results to the commercial public cloud. This can raise big security concerns, especially when the outsourced computation workloads contain sensitive information, such as a business's financial records, proprietary research data, or even personally identifiable health information.

Furthermore, the cloud's operational details aren't transparent enough to users. Consequently, various motivations can cause the cloud to behave unfaithfully and return incorrect results. These range from possible software bugs, hardware failures, or even outsider attacks to cloud servers deliberately being— lazy‖ to save computational costs. Thus, we're in great need of protection computation outsourcing mechanisms to both protect sensitive workload information and ensure that the computation results returned from the cloud are correct. This task is difficult, however, due to several challenges that the mechanism design must meet simultaneously. First, such a mechanism must be practically feasible in terms of computational complexity.

Otherwise, either the user's cost can become prohibitively huge, or the cloud might not be able to complete the outsourced computations in a reasonable amount of time.

Second, it must provide sound security guarantees without restricting system assumptions. Namely, it should strike a good balance between security guarantees and practical performance. Third, this mechanism must enable substantial computational savings at the user side compared to the amount of effort required to solve a problem locally. Otherwise, users have no reason to outsource computation to the cloud. A recent breakthrough in fully homomorphic encryption (FHE) has shown the general results of protection computation outsourcing to be viable in theory. But applying this general mechanism to everyday computing tasks is still far from practical due to

FHE operations' extremely high complexity, which can't yet be handled in practice. On a different front, researchers are working on mechanisms for specific computation outsourcing problems, such as linear programming via problemtransformation,7 genomic computation via specialized computationpartition,8 and efficient verification of large-scale biometric computations, all of which should provide much more practical efficiency than the more general solutions currently available.

V. Conclusion

In this paper, we believe that data storage security in Cloud Computing is an emerging computing paradigm, allows users to share resources and information from a pool of distributed computing as a service over Internet. Cloud storage is much more beneficial and advantageous than the earlier traditional storage systems especially in scalability, cost reduction, portability and functionality requirements. Cloud Computing is an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. System uses encryption/decryption keys.

VI. References

[1] P. Mell and T. Grance, ―The NISTDefinition of Cloud Computing, ‖USNat'l Inst. of Science andTechnology,2011; http://csrc.nist.gov/publications/nistpubs/ 800-145/SP800-145.pdf.

[2] Security Guidance for Critical Areasof Focus in Cloud Computing,‖ Cloud Security Alliance, Dec. 2009; https:// cloud securityalliance.org/csaguide.pdf.

[3] T. Ristenpart et al., ―Hey, You, Get Offof My Cloud!Exploring Information Leakage in Third-Party Compute Clouds,‖Proc. 16th ACM Conf. Computer and Communications Security (CCS 09), ACMPress, 2009, pp. 199–212.

[4] C. Wang et al., ―Privacy-Preserving Public Auditing forStorage Securityin Cloud Computing,‖ Proc. 30th IEEEInt'lConf. Computer Communications(INFOCOM 10), IEEE Press, 2010,pp. 525–533.M. Bellare, R. Canetti, and H. Krawczyk, ―Keying hash functions for message authentication,‖ in Proc. of Crypto'96, volume 1109 of LNCS. Springer-Verlag, 1996, pp. 1–15.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, ―Above the clouds: A berkeley view of cloud computing,‖ University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, ―Achieving potection, scalable, and fine-

grained access control in cloud computing,‖
[7] in Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010.
[8] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, ―Dynamic provable data possession,‖ in Proc. of CCS'09,2009, pp. 213–222.
[9] R.C.Merkle, ―Protocols for public key cryptosystems,‖ in Proc. of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.