Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage System

POLU. SATHISH
Department of Computer Science & Engineering (M.Tech.)
Sindura College of Engineeringand Technology
Ramagundam,Telangana

B.SUDHAKAR
Asst. Professor,
Department of Computer Science & Engineering
M. Tech.
Sindura College of Engineering and Technology
Ramagundam,Telangana

K.GEETA
Head of the Department of Computer Science & Engineering
M. Tech.
Sindura College of Engineering and Technology
Ramagundam,Telangana

Abstract:
Computing has been widely used for data storage and computational purposes. When we discuss about the cloud storage services, the data must be outsourced, so, there may be serious concerns about the authorization and trust management for the cloud service provider (CSP). These concerns are about confidentiality, integrity, security and access control. In this paper we are going to discuss various models in brief such as Provable data possession (PDP), Proof of irretrievability (POR), HAIL, Attribute Based Encryption Scheme, Plautus, Sirius, Third party auditor (TPA) etc that are introduced for addressing such issues about cloud storage systems. This scheme supports dynamic data and trust in the cloud computing storage systems. The present system is providing a good security mechanism for stored data and proper sharing of keys among authorized users, and data owner for the cryptographic mechanism.

Keywords: *Outsourced data storage, Security, Trusted Auditor, Dynamic Environment*

1. Introduction

Cloud Computing describes a new supplement & delivery model for IT services based on the Internet & it typically involves over- the-Internet provision of dynamically stable & often virtualized resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In this Information age, several organizations posses huge amount of data which needs to be kept secured. These data includes personal information, health information and financial data. Local maintenance of such huge amount of data will be cost effective and problematic. Hence Cloud Service Provider offered Storage as a Service to alleviate the burden of huge local data storage and to reduce the cost by means of outsourcing data storage to the cloud. Since the data owner outsources their sensitive data to the cloud, they want their data to be guaranteed with some security concerns like confidentiality, integrity and proper access control.

In this work, we proposed a technique which addresses some important concerns associated with outsourcing sensitive data to the entrusted remote CSP, namely dynamic data, newness, mutual trust

and access control. The outsourced data can be modified and scaled by the data owner. After doing modification, the authorized users are enabled to get the most recent version of the outsourced data. A technique is required to identify the staleness of the received data. This issue is dangerous for applications in which critical decisions are made based on the received data. Mutual trust between the data owner and CSP is enabled in the proposed scheme. A method is established to resolute dishonest party from any side. Finally, the access control is considered, which allows the data owner to grant or revoke access rights to the outsourced data.

Confidentiality is not only a security concern but also a juristic issue. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote cloud server. For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites.

2. Literature Review

Existing work related to our proposed work can be found in the areas of integrity verification of remotely stored data and file encryption schemes in distributed systems and access control mechanisms over outsourced data. A model for provable data possession (PDP) by Attendees et al. [2] that allows a client that has stored data at an un-trusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server. It reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The response protocol transmits a small, constant amount of data, which reduces network traffic. Thus, the PDP model for remote data checking supports large data sets in Widely-distributed storage system.

Clearway et al [4] present a definitional framework and efficient constructions for dynamic provable data possession (DPDP), which extends the PDP model to support provable updates to stored data. The price of dynamic updates is a performance change from O(1) to O(logn) O(nɛlogn), for a file consisting of n blocks, hale maintaining the same (or better, respectively) probability of misbehavior detection. Carmela et al. [5] designed a model based on MRPDP which uses replication in order to improve data availability and reliability. By storing multiple copies, if some copies are destroyed still the data can be recovered from the remaining copies. But challenges incur relatively more cost in MR-PDP. Dodos et al. [6] presented a model based on POR (Proofs of Irretrievability) in which the client stores a file F on a server and keeps only a short private verification string locally. Later, the client can run an audit protocol to verify the server's data possession, in which the client acts as a verifier and the server proves that it possesses the data. POR is a complementary approach to PDP, and is stronger than PDP in the way that it can be reconstructed from the portions of the data which are reliably stored on the remote server.

3. Proposed Work

In this work, we propose a scheme that addresses important issues related to outsourcing the storage of data, namely dynamic data, newness, mutual trust, and access control. The remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner. After updating, authorized users should receive the latest version of the data (newness property), i.e., a technique is required to detect whether the received data is stale. Mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme.

However the block indices must have the awareness that the CSP has modified the blocks at the requested position. At this end, the proposed scheme uses combined hash values and a small data structure called Block Status Table (BST). The TTP (Trusted Third Party) establishes mutual trust between data owner, CSP and authorized users in an indirect way. To enforce access control the proposed scheme uses three cryptographic functions, namely block wise encryption BckEnc (RC-5), Key Rotation and Lazy Revocation. The BckEnc allows the data owner to encrypt some confidential

information to only authorized users allowing them to access the outsourced data. Lazy revocation enables the revoked users to access the older version of the outsourced data i.e. only the authorized users are allowed to access the most recent version of the outsourced data. Using key rotation authorized users can access both latest version of the data and older version of the data.

3.1 An overview of Mutual Trust Model

The Mutual trust between the data owner and the CSP is another issue and that is addressed in this scheme. A mechanism is introduced to determine the dishonest party, from any side is detected and the responsible party is identified. Access control is also provided by the model which allows the owner to grant access or to revoke access rights to the outsourced data. Cloud storage model considered in our proposed work has four main components as depicted in Fig.1.

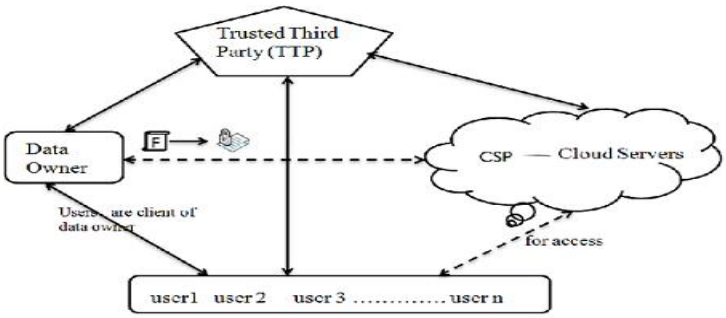

Figure 1 : Mutual trust model for cloud computing storage

1. A data owner can be an organization, which generates sensitive data that is to be outsourced to the cloud and made available for only authorized users.
2. A Trusted Third Party Auditor (TTPA) who is trusted by all other components and has the capability to detect the dishonest party.

The relations between different system components are represented by double-sided arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the data owner, the authorized users, and the CSP trust the TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to enable indirect mutual trust between these three components. There is a direct trust relation between the data owner and the authorized users.

1. Owner Role: Generate master key MK & browse the file to be uploaded on server. Encrypt the File F into F' by using the RC-5 algorithm.. Generate BST to check the data integrity & finally owner sends {MK, F', BST} to TTP & deletes the file from local. Also generate the hash value by using the SHA-512 algorithm for maintain integrity.
2. TTP Role: Computes combined hash values for the encrypted file F' and the BST.
3. User request to access file: When User requesting file from TTP & CSP then gets {F' BST} and combined hash from TTP. The outsource data to a remote CSP perform full dynamic operations at the block-level such as block modification, insertion, deletion, and append. Each and every operation request by owner, the same request generates to the TTP & CSP. TTP recomposes the hash value of old block with the new one. Last but not list, a security analysis, computational & storage cost calculation.

3.2 Digital Certificates and Hashing

The digital signature scheme using self-certified public keys. It has provided the message recovery property. This scheme only allows a specified receiver to verify and recover the message with authenticated encryption. For transmission of large message or blocks, while providing the linkages among signature blocks, this scheme is suitable. [9] It described browser security in the Cloud

computing context. It described the threat of flooding attacks on Cloud systems. Cloud Computing security concerns and analysis on their potential impact and relevance to real-world scenarios.

3.3 Outsourcing, updating and accessing

The data owner has a file F, which is divided into m blocks and is to be outsourced to CSP, who will provide paid storage space to the data owner. Before outsourcing the file to the cloud server, to achieve confidentiality the owner encrypts the file blocks. After doing so, the owner can interact with the CSP to do full block-level dynamic operations on the file. These block-level operations include insert, delete, append, and modify certain blocks of the outsourced file. For time being, we have considered only insert and delete operations in our work. An authorized user receives the encrypted file, by sending the data access request to the CSP. The encrypted file can be decrypted using a decrypt key which can be generated by the authorized user.

The access of the authorized users' has already been done by the data owner; hence we haven't considered this in our work. And also all authorized users have the same access privilege over the outsourced data. The TTPA and the CSP are always online, while the data owner can be online or offline. Even though the owner is in offline, the authorized users can access the outsourced data from the CSP. There is no need to data owner is in online but the accessing authorized user is must is in online for accessing the required data.

4. Cloud Computing Components

4.1 Trusted Third Party Auditor

There is also solution provided by introducing trusted third party auditor (TTPA), into the cloud system. That is on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The TTPA replaces the involvement of client through the auditing of whether his data stored in the cloud is indeed intact, which can be commercially important Cloud Computing. The data operations such as block modification, insertion and deletion, is also a significant. The public verifiability and dynamic data operations are provided in this model of TTPA The proof of retrievability model is modified by manipulating the classic Merle Hash Tree (MHT) construction for block tag authentication. The Extensive security and performance is proposed in TPA model and provably secure

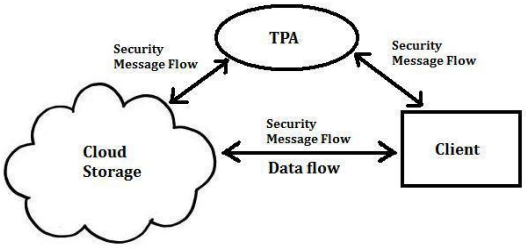

Figure 2 : Trusted Third party auditor model for data storage in cloud

4.2 Block Status Table

The block status table is a small data structure used to access and restructure the received file blocks. The BST is implemented as a linked list to simplify the insertion and deletion of table entries. The BST is used by authorized users to reconstruct and access the outsourced data file. The proposed scheme assumes that the owner is intermittently online and the users are enabled to access the data even when the owner is offline. To this end, the CSP stores a copy of the BST along with the outsourced data file. When a user requests to access the data, the CSP responds by sending both the BST and the encrypted file F.

Moreover, the BST is used during each dynamic operation on the outsourced data file, where one

table entry is modified/inserted/deleted with each dynamic change on the block level. If the BST is stored only on the CSP side, it needs to be retrieved and validated each time the data owner wants to issue a dynamic request.

4.3 Access control mechanism

The three cryptographic techniques Lazy Revocation, Key Rotation and Block level Encryption which are discussed below are combined to enforce access control over outsourced data.

4.3.1. Lazy Revocation

The data owner in our proposed work is allowed to revoke access right of some users from accessing the outsourced data at any time. The revoked users are allowed to access unmodified blocks in Lazy Revocation. However, modified or new blocks must not be accessed by such revoked users. This is equivalent to accessing the file blocks from caches. The idea behind this scheme is, modified or new blocks following revocation are encrypted under new key. Thus each data block may have more than one key. Lazy Revocation trades re-encryption cost.

4.3.2 Key Rotation

In this technique [11], a sequence of keys can be generated from an initial key and a master secret key. The sequence of keys has two main characteristics.

1. The next key in the sequence can only be generated by the owner of the master secret key.
2. The authorized users knowing the key in the sequence can able to generate previous keys in the sequence. i.e. given the key in the sequence, the authorized users can compute the previous keys in the sequence

5. Implementation & Performance Analysis

Our implementation consists of four modules: owner module, CSP module, TTP module and user module. To implement this encryption algorithm we use an elliptic curve with a 256 bit group order. And we have used RC-5, SHA-256 for hashing, and digital signature algorithms. We evaluate the performance of the proposed scheme by analyzing storage, communication and computation overhead. The data file we have used for our experiments is of size 10GB with block size of 100MB.

5.1 Storage overhead

This is the additional storage space required to store necessary information other than the outsourced file F. An entry of BST at the owner side is of 8bytes, and the no of entries will be equal to number of blocks q of the file F. Likewise, at the CSP side the additional storage of BST requires 8q bytes, where q is the number of blocks. Each may require 800 MB storage.

Table 1: Storage Overhead

Data Owner	**Authorized Users**	**CSP**	**TTP**
8q	-	8q	-

5.2 Computation overhead

The computation cost for encrypting the data before outsourcing, and the dynamic operations require hash function, encryption, Burden and it may require FR forward rotation if there is a revocation.

Table 2: Computational Overhead

Component	TTP	Users	CSP
Computational Overhead	0.04 ms / 3.59 s	0.55 s	6.04 s

The storage overhead is ≈ 0.4% of the outsourced data size, the communication overhead due to block-level dynamic changes on the data is ≈ 1% of the block size, and the communication overhead due to retrieving the data is ≈ 0.2% of the outsourced data size. For a large organization with 105 users, performing dynamic operations and enforcing access control add about 63 milliseconds of overhead. Therefore, important features of outsourcing data storage can be supported without excessive overheads in storage, communication, and computation.

6. Conclusion

There is outsourcing of data over the cloud service provider. Thus there are serious concerns about the cloud storage systems, so there are various schemes have been introduced. These models are about trust and security for the cloud storage systems.

In this scheme, the owner is capable of archiving and accessing the data stored by the CSP and updating and scaling this data on the remote servers. This scheme enables newness of data. The trusted third party has been introduced in this model which determines whether the storage is honest or not. It detects the party. Also the access control is provided by data owner. They provided the three techniques for cryptography i.e. broadcast encryption, lazy revocation, and key rotation. We have also investigated the overheads added by our scheme when incorporated into a cloud storage model for static data with only confidentiality requirement. The experimental results show that the proposed scheme is a robust model in terms of security.

References

1. NIST SP 800-145, “A NIST definition of cloud computing”, http://csrc.nist.gov/publications/drafts/800-145/Draft- SP- 800-145_cloud-definition.pdf
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song,
3. “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07, 2007, pp. 598–609.
4. Sehgal NK, et al.: Information Security and Cloud Computing, Iete Technical Review, Vol. 28, Issue 4, Jul-Aug 2011..
5. C. Erway, A. Kupc¸ U, C. Papamanthou, and Tamassia, “Dynamic provable data possession,” in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.
6. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: multiple replica provable data possession,” in 28th IEEE ICDCS, 2008, pp. 411–420.
7. Y. Dodis, S. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC ’09: Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 109–127.