Enhancing Data Dynamic Security & Trust for Cloud Computing Storage System

Trupti V. Junghare
M.Tech Student
PG Department of Computer Science and Engineering,
JD College of Engineering & Management
Nagpur University, Maharashtra, India
truptijunghare15@gmail.com

Prof. Mirza M. Baig
Asst. Professor
PG Department of Computer Science and Engineering,
JD College of Engineering & Management
Nagpur University, Maharashtra, India
mmbaig@gdcoe.in

Abstract—Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. We propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the cloud service providers (CSPs) through Storage-as-a-Service (SaaS) and enables indirect mutual trust between owner and CSP. SaaS) is a paid facility that enables organizations to outsource their data to be stored on remote servers and perform full block level dynamic operations and hence reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. The outsorced stored data can be accessed by a group of authorized users by the data owner. The owner has the privilege to grant or revoke access of the stored data in the cloud. 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. It also ensures the newness property to the authorized users for receiving the most recent version of the stored data.

Keywords- **outsourcing data storage, dynamic environment, indirect mutual trust, access control.**

*****

I. Introduction

Cloud computing has received considerable attention from both academia and industry due to a number of important advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, flexibility to scale up and down information technology (IT) capacity, and mobility where customers can access information wherever they are, rather than having to remain at their desks.

SaaS offered by CSPs is an emerging solution to mitigate the burden of large local data storage and reduce the maintenance cost via the concept of outsourcing data storage. The local management unable to access the multiple users to overcome, the CSP often provides better disaster recovery by replacing the data on multiple servers across multiple data centers achieving a higher level of availability. Thus, many authorized users are allowed to access the remotely outsourced stored data from different geographic locations making it more convenient for them. Generally the owner physically outsourced sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. In some practical applications, data confidentiality is not only a privacy concern, but also a juristic issue. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers.

The main objective of this project is constructing a secure data storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. In this work, we propose a scheme that addresses some important issues related to outsourcing the storage of data, namely data dynamic, newness, mutual trust, and access control. One of the core design principles of data outsourcing is to provide dynamic scalability of data for various applications. This means that the remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner. The cloud based storage system allows a data owner to outsource the data to a CSP, and perform full dynamic operations at the block-level such as block modification, insertion, deletion and append. After updating, the 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. The indirect mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme. A mechanism is introduced to determine the dishonest party, i.e., misbehavior from any side is detected and the responsible party is identified. Last but not least, the access control is considered, which allows the data owner to grant or revoke access rights to the outsourced storage data, if and only if the owner don't provide the access to the authorized user no one can access the stored data from CSP.

II. Literature Review

In traditional access control techniques the data exists that is of the data owner and the storage servers is in the same trust domain. But when the data is outsourced to the CSP then the data owner and CSP are in different domain. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote untrusted CSP. The unauthorized users, including the CSP, are unable to access the data since they do not have the decryption key. Through this solution, the data is encrypted under a certain key, which is shared only with the authorized users.

Kallahalla et al. [2] designed a cryptography-based file system called Plutus for secure sharing of data on untrusted servers. Some authorized users of the data have the privilege to read and write, while the others can only read the data. Goh et al. [3] have presented SiRiUS, which is designed to be layered over existing file systems such as NFS (network file system) to provide end-to-end security. To enforce access control in SiRiUS, each data file (d-file) is attached with a metadata file (md-file) that contains an encrypted key block for each authorized user with some access rights (read or write). This technique can prevent and detect malicious actions from the CSP side. Also one thing the CSP needs to be safeguarded from a dishonest owner. Popa et al. [4] have introduced a cryptographic cloud storage system called CloudProof that provides read and write data sharing. CloudProof has been designed to offer security guarantees in the service level agreements of cloud storage systems.

For verifying data integrity over cloud servers, researchers have proposed provable data possession (PDP) technique to validate the intactness of data stored on remote sites i.e. CSP. A number of PDP protocols have been presented to efficiently validate or maintain the integrity of static data [5]. Another class of PDP schemes was concerned with the dynamic behavior of data over remote servers [8]. This class allows the owner to outsource a data file and perform updating or scaling operations on the outsourced data. A complementary line of research on PDP has focused on multiple data copies stored over different servers. Bowers et.al.[9] presented a PDP construction for multiple copies of dynamic data. This approach is known as Proof of retrievability (POR), it is a stronger than PDP means that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers.

III. RESEARCH METHODOLOGY

A. System Model

The cloud computing storage model in this work proposed that provides solutions to the important issues and concerns related to outsourcing the storage of data, namely dynamic data, newness, mutual trust, and access control.

In figure 1, a data owner that can be an organization generating sensitive data to be stored in the cloud and made available for controlled external use. A CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users.

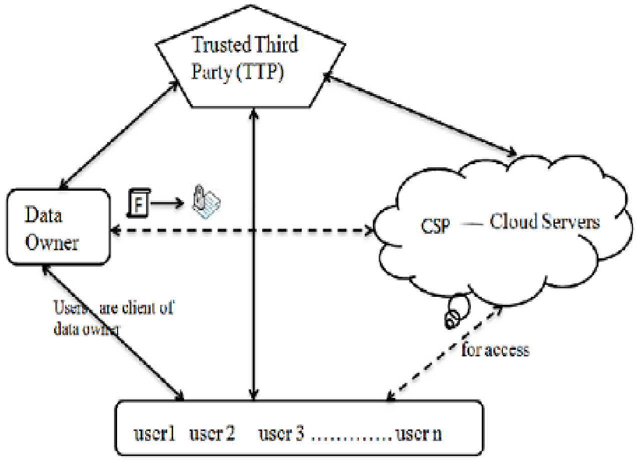
Trusted Third Party (TTP)
Data Owner
F
CSP — Cloud Servers
Users are client of data owner
for access
user1 user2 user 3 ....user n

Figure 1. Cloud computing data storage system model

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.

The authorized users is a set of owner's clients who have the right to access the remote data; and a trusted third party (TTP), an entity who is trusted by all other system components, and has expertise and capabilities to detect and specify dishonest parties. The data owner has a file F consisting of m blocks. For confidentiality, the owner encrypts the data before sending to cloud servers. After outsourcing the data, the owner can interact with the CSP through authorized users to perform block-level operations on the file that is dynamic data property. Data is stored on remote server that is different domain this is only accessed by authorized users. Also the data is updated, scaled and monitored by the owner. After updating, authorized users should receive the latest version of the data that is newness property.

The Mutual trust between the data owner and the CSP is another issue and that is proposed 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.

B. Security Requirments

For Confidentiality, outsourced data must be protected from the TTP, the CSP, and users that are not granted access. Only authorized users are allowed to access the outsourced data. Revoked or granted users can read unmodified data; however, they must not be able to read updated/new blocks. To maintain integrity outsourced data is required to remain intact on cloud servers. The data owner and authorized users must be enabled to recognize data corruption over the CSP side.

To receiving the most recent version of the outsourced data file is an imperative requirement of cloud-based storage systems. There must be a detection mechanism if the CSP ignores any data-update requests issued by the owner. The CSP's defence who safeguarded the CSP against false accusations that may be claimed by dishonest owner/users and such a malicious behavior is required to be revealed. Combining the confidentiality, integrity, newness, access control, and CSP's defence properties in the proposed scheme enables the mutual trust between the data owner and the CSP. Thus, the owner can benefit from the wide range of facilities offered by the CSP, and at the same time, the CSP can mitigate.

C. Trusted Third Party

The data owner, the authorized users, and the CSP trust the TTP. However, the data owner and the authorized users have mutual distrust relations with the CSP shown in figure.1. 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.

The third party auditor is to verify the data stored on remote servers, and give incentives to providers for improving their services. The proposed scheme in this work uses the TTP in a slightly different fashion. The auditing process of the data received from the CSP is done by the authorized users, and we choice to the TTP only to determine disputes that may arise regarding data integrity or newness. Reducing the storage overhead on the CSP side is efficiently a key feature to lower the fees paid by the customers. Moreover, decreasing the overall computation cost in the system is another important aspect. For achieving these goals, a small part of the owner's work is delegated to the TTP that is the nothing but the direct trust between Owner and TTP.

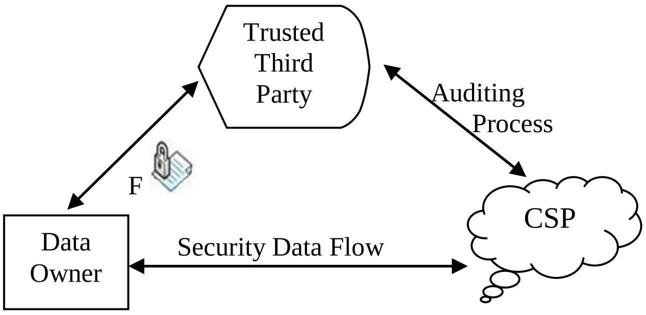

Figure 2. TTP model for data storage

The data owner sends the encrypted data to the CSP through TTP and wise versa. For auditing process the authorized users send the request for hash value of the receiving data unless & untill this means integrity.The TTP maintain the BST record due to this owner knows about the dynamic operations which will perform on stored data.Indirectly the data owner & CSP makes the secured flow of data this is new aspects of our work. The TTP is an independent entity, and thus has no reason to join together with any party in the system. However, any possible leakage of data towards the TTP must be prevented to keep the outsourced data private. The TTP and the CSP are always online, while the owner is intermittently online. The authorized users are able to access the data file from the CSP even when the owner is offline.

IV. SYSTEM PRELIMINARIES

The proposed scheme supported some procedural steps to provide all the techniques which are beneficial to the data owner to outsource their sensitive data to the CSP. The whole system accesses the setup & files preparation process, also make dynamic operations on the outsourced data. The most important step is data access & cheating detection. The setup is done only once during the life time of the data storage system has two parts one is on owner side and another is done on TTP side. The dynamic operations are performed at the block level where request come from owner side to the authorized users. The BST and hash value will be used before and after the operations are performed and the all record will be maintained by TTP to the BST table.

A. Owner Role

An owner browses the file from the local storage and generate master key (MK). The data file F will be encrypted into the F' by using the RC-5 block encryption algorithm with variable block and key sizes. The proposed scheme used RC-5 algorithm for encryption because in that there is very difficult to break the encrypt key if the attacker does not know the sizes when attempting to decrypt captured data. The master key will be generated by the combination of the user id and identifier.

The encrypted secret key is the same as the MK for optimizing the database. Also owner generates the Block status table (BST) to check the data integrity also performing block level dynamic operations. Finally owner sends {F', MK, BST} to the TTP and delete the data files from the local storage.

B. TTP Role

To resolve disputes that may arise regarding data integrity or newness, the TTP computes hash values FH_{TTP} for the encrypted file F' and TH_{TTP} for the BST. The TTP keep only FH_{TTP} and TH_{TTP} on its local storage. Finally send encrypted data file F' to the CSP and delete from the TTP local storage. The BST is used by the authorized users to reconstruct and access the outsourced data file.

The proposed scheme in this work assumes that the data owner is intermittently online and the authorized users are enabled to access the data file even when the owner is offline. Moreover, the BST is used during each block level dynamic operation such as block modification, insertion, deletion and append on the outsourced data file, where one table entry is modified/inserted/deleted with each dynamic change on the block level. For each operation request by owner the request generates to the TTP and CSP. The TTP computes the hash value of old block with the new one. 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 on the outsourced file. To avoid such communication and computation overheads, the owner keeps a local copy of the BST.

C. CSP Role

The CSP stores a copy of the BST along with the outsourced data file. Also when dishonest CSP tampered some data on stored data file then CSP side generates the new hash value. When an authorized user requests to access the data, the CSP responds by sending both the BST and the encrypted file F'. At auditing process request from TTP the CSP send the computed hash value to the TTP for checking the loss of integrity. If the both TTP and CSP side hash value are same means there is no loss of integrity, if change that means some data will be tampered.

D. User requst to access the file

The user requests file from the TTP and CSP. User gets {F', BST} from CSP and combined hash FH_{TTP} from TTP. The authorized users have the decrypt key, by using key user can decrypt the encrypted file F' into the original file F. This means that the authorized user verifies the signature and access the data.

V. RESULT ANALYSIS

We experimentally evaluate the computation overhead the proposed scheme brings to a cloud storage system that has been dealing with data with only confidentiality requirement. To evaluate the computation overhead on the owner side due to dynamic operations, we perform 100 different block operations. For different number of system users, figure 3 shows the owner's average computation overhead per operation. The access control of the proposed scheme depends on the square root of the total number of system users. Figure3 shows that for a large organization with 100,000 users, performing dynamic operations and enforce access control for outsourced data as in practical (0.62 seconds).

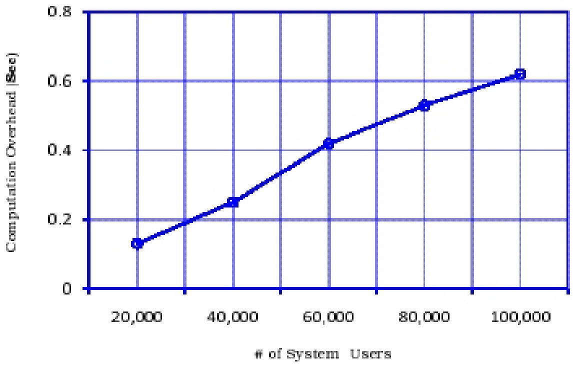

Figure 3. Due to dynamic operations. Owner's average computation overhead

To examine the computation time, we access the file after running 100 different block level operations. As a reply to the data access request, the CSP compute two signatures: σF and σT. Thus, the computation overhead on the CSP side due to data access is about 10.75 seconds and can be easily hidden in the transmission time of the data (1GB file and 2MB table). To identify the dishonest party in the system in case of disputes, the TTP verifies two signatures (σF and σT), computes combined hashes for the data (file and table), and compare the computes hashes with the authentic values (TH_{TTP} and FH_{TTP}). Thus, the computation overhead on the TTP side is about 10.77 seconds. Through our experiments, we use only one desktop computer to simulate the TTP and complete its work. In practice, the TTP may choose to divide the work among a few devices or use a single device with a multi-core processor which is becoming prevalent these days, and thus the computation time on the TTP side is significantly reduced in many applications.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 598–609.

[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST 03 Conference on File and Storage Technologies. USENIX, 2003.

[3] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proceedings of the Network and Distributed System Security Symposium, NDSS. The Internet Society, 2003.

[4] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage SLAs with cloudproof," in Proceedings of the 2011 USENIX conference on USENIX annual technical conference, ser. USENIXATC'11. USENIX Association, 2011.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in SecureComm '08: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York, NY, USA, 2008, pp. 1–10.

[6] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in CCS '09: Proceedings of the 16th ACM Conference on Computer and Communications Security, New York, NY, USA, 2009, pp. 213–222.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS'09: Proceedings of the 14th European Conference on Research in Computer Security, Berlin, Heidelberg, 2009, pp. 355–370.

[8] A. F. Barsoum and M. A. Hasan, "On verifying dynamic multiple data copies over cloud servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011, http://eprint.iacr.org/.

[9] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[10] 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.