International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 4, May-June 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

CSP Dynamic Data & TTP Indirect Approach

Mr. Jaydeep Pawar (ME CSE), **Prof. Sarika Bodke** (Head)

Department of Computer Engineering, PVPIT College of Engineering, Pune, Maharashtra, India

ABSTRACT

In today's digital era, the amount of sensitive data produced by many organizations is outpacing their storage ability. The management of such huge amount of data is quite expensive due to the requirements of high storage capacity and qualified personnel. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. On the other hand, the CSP needs a protection from any false accusation that may be claimed by the owner to get illegal compensations. In this paper, we propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: First one, it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append. Second one, it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data. Next one, it enables indirect mutual trust between the owner and the CSP. Last one, it allows the owner to grant or revoke access to the outsourced data. We discuss the security issues of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

KEYWORDS: *Cloud computing, Data security, Data outsourcing, Cloud service provider, Mutual trust*

How to cite this paper: Mr. Jaydeep Pawar | Prof. Sarika Bodke "CSP Dynamic Data & TTP Indirect Approach" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-4, June 2022, pp.683-687, URL: www.ijtsrd.com/papers/ijtsrd50080.pdf

IJTSRD50080

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. Cloud computing is a distributed computational model over a large pool of shared-virtualized computing resources (e.g., storage, processing power, memory, applications, service and network bandwidth).Cloud service Provider(CSPs) offer different classes of services Storage-as-a-Service (SaaS), Application-as-a-Service, and Platform-asa-Service that allow organizations to concentrate on their core business and leave the IT operations to experts.

In the current era of digital world, different organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. 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. Through outsourcing data storage scenario, data owners delegate the storage and management of their data to a CSP in exchange for pre-specified fees metered in GB/ month. Such outsourcing of data storage enables owners to store more data on remote servers than on

private computer systems. Moreover, the CSP often provides better disaster recovery by replicating 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 stored data from different geographic locations making it more convenient for them. Since the owner physically releases 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. For example, in e-Health applications inside the USA the usage and exposure of protected health information should meet the policies admitted by Health Insurance Portability and Accountability Act (HIPAA), and thus keeping the data private on the remote storage servers is not just an option, but a demand. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. For supportive data integrity over cloud servers, researchers have projected demonstrable data possession technique to validate the intactness of information hold on remote locales.

In this work, a service that locations vital issues identified with outsourcing the storage of data, access control, newness namely dynamic data and mutual trust The remotely keep data will be not solely accessed by authorized users, however additionally updated and scaled by the owner.

Our contributions can be summarized in two main points.

1. The design and implementation of a cloud-based storage scheme that has the following features:

A. It allows a data owner to outsource the data to a remote CSP, and perform full dynamic operations at the block-level, i.e., it supports operations such as block modification, insertion, deletion, and append

B. It ensures the newness property, i.e., the authorized users receive the most recent version of the data

C. It establishes indirect mutual trust between the data owner and the CSP since each party resides in a different trust domain

D. It enforces the access control for the outsourced data

2. We discuss the security features of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

After data change, authorized users should receive the most recent version of the data (newness property), i.e., a method is needed to observe whether or not the received data is stale. Mutual trust between the data owner and therefore the CSP is another imperative issue, which is addressed within the projected scheme. A mechanism is introduced to work out the dishonest party, i.e., misbehavior from any aspect is detected and therefore the responsible.

II. RELATED WORK

Existing research close to our work can be found in the areas of integrity verification of outsourced data, Cryptographic file systems in distributed networks, and access control of outsourced data. Based on proxy re-encryption have introduced a secure distributed storage protocol. In their protocol, a data owner encrypts the blocks with symmetric data keys, which are encrypted using a master public key. The data owner keeps a master private key to decrypt the symmetric data keys. Using the master private key and the authorized user's public key, the owner generates proxy re-encryption keys. A semi-trusted server then uses the proxy re encryption keys to translate a cipher text into a form that can be decrypted by a specific granted user, and thus enforces access control for the data..

Aameek Singh describe "SHAROES" it is a platform for data sharing in the storage-as-a-service model. SHAROES uses novel cryptographic access control primitives (CAPs) to support rich data sharing semantics without trusting the SSP for enforcement of security policies. He showed how SHAROES is able to support an expressive access control model, which in conjunction with its in-band key management technology provides seamless transition ability from local storage to the outsourced model with minimal user involvement. [1]

Giuseppe Ateniese introduced a model for provable data possession, in which it is desirable to minimize the file block accesses, the computation on the server, and the client-server communication. They incur a low (or even constant) overhead at the server and require a small, constant amount of communication per challenge.[2]

Francesc Sebe provide first practical protocol for remote file integrity checking allowing an infinite number of verifications presented. An ordering or a structure between the set of files should be defined, so that the set of files can be regarded as a super file. Once the super file is defined, its integrity can be checked using his protocol without any modification.[3]

III. PROPOSED SYSTEM

The cloud computing storage model during this work consists of four main parts a data owner that may be a corporation generating sensitive data to be keep within the cloud and made out there for controlled external use.

It includes file splitting process, which means storing of data into multiple servers. We propose the system with the data stored in the cloud may not only accessed but also be frequently updated by the users. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. 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. 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 owner to grant or revoke access rights to the outsourced data.

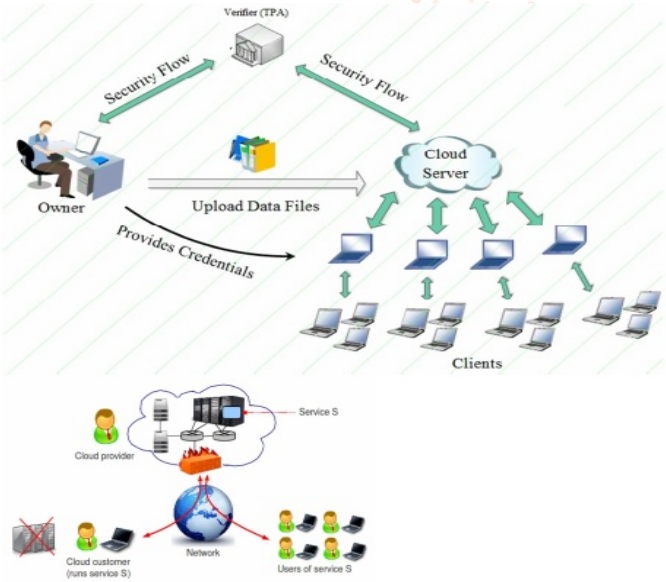

Fig 1. System Architecture

Fig. 1 shows the relations between completely different system parts are denoted by double-sided arrows, where dotted and solid arrows represent trust and distrust relations, severally. as an example, the data owner, the authorized users, and also the CSP trust the TTP. On the opposite hand, the data owner and also the authorized users have mutual distrust relations with the CSP. Thus, the TTP is used to modify indirect mutual trust between these 3 components. There's a right away trust relation between the data owner and also the authorized users.

In this work, the auditing method of the data received fromthe CSP is completed by authorized users and we resort to the TTP only to resolve disputes that may arise relating to data integrity or age. Reducing the storage overhead on the CSP aspect is economically a key feature to lower the fees paid by the purchasers. Moreover,decreasing the computation value within the system is another crucial side. To realize these goals, a small a part of the owner's work is delegated to the TTP.

The owner encrypts before sending data to cloud servers. When data outsourcing, the owner will act with the CSP toperform block level operations on the file which included data. Additionally, the owner enforces access control by granting access rights to the outsourced data. To access the data, the authorized user sends a data access request to the CSP and receives the data file in an encrypted kind which will be decrypted using a secret key generated by the authorized user.

A. Security Requirements

- Confidentiality: outsourced data must be protected from the TTP, the CSP and users that don't seem to be granted access.
- Integrity: Outsourced data is needed to stay intact on cloud servers. The data owner and authorized users should be enabled to acknowledge data corruption over the CSP aspect.
- Newness: Receiving the foremost recent version of the outsourced data file is an essential demand of cloud- based storage systems. There should be an identification system if the CSP disregards any data overhaul demands issued by the owner.
- Access control: Only authorized users are allowed to access the outsourced data. Revoked users will read unmodified data; however, they need to not be able to read updated/new blocks.
- Defense: The CSP should be safeguarded against false accusations which will be claimed by dishonest owner/users and such a malicious conduct is required to be uncovered.

IV. SYSTEM PRELIMINARIES

1. Lazy Revocation:

The proposed scheme in this work allows the data owner to revoke the right of some users for accessing the outsourced data. In lazy revocation, it is acceptable for revoked users to read (decrypt) unmodified data blocks.

2. Key Rotation:

Key rotation is a technique in which a sequence of keys can be generated from an initial key and a master secret key. The sequence of keys has two main properties: (i) only the owner of the master secret key is able to generate the next key in the sequence from the current key, and (ii) any authorized user knowing a key in the sequence is able to generate all previous versions of that key. In other words, given the i-th key Ki in the sequence, it is computationally infeasible to compute keys Kl for l > i without having the master secret key, but it is easy to compute keys Kj for j < i. Whenever a user's access is revoked, the data owner generates a new key in the sequence (rotating forward). Let ctr indicate the index/version number of the current key in the keys sequence. The owner generates the next key by exponentiating Kctr with the master secret key d: Kctr+1 = Kdctr mod N. Authorized users can recursively generate older versions of the current key by exponentiating with the public key component e: Kctr-1 = Kectr mod N (rotating backward). The RSA encryption is used as a pseudorandom number generator; it is unlikely that repeated encryption results in cycling, for otherwise, it can be used to factor the RSA modulus N.

3. Broadcast Encryption:

Broadcast encryption (bENC) allows a broadcaster to encrypt a message for an arbitrary subset of a group of users. The users in the subset are only allowed to decrypt the message. However, even if all users outside the subset collude they cannot access the encrypted message Such systems have the collusion resistance property, and are used in many practical applications including TV subscription services and DVD content protection.

4. Block Status Table:

The block status table (BST) is a small dynamic data structure used to reconstruct and access file blocks outsourced to the CSP. The BST consists of three columns: serial number (SN), block number (BN), and key version (KV). SN is an indexing to the file blocks. It indicates the physical position of each block in the data file. BN is a counter used to make a logical numbering/indexing to the file blocks.

V. EXPERIMENTAL EVALUATION

In this section we experimentally evaluate the computation overhead the proposed scheme brings to a cloud storage system that has been dealing with static data with only confidentiality requirement. The experiments are conducted using .NET on a system with an Intel(R) Xeon (R) 2-GHz processor and 3GB RAM running Windows XP. Algorithms (hashing, broadcast encryption, digital signatures, etc.) are implemented using MIRACL library version 5.5.4. For a 128-bit security level, bENC uses an elliptic curve with a 256-bit group order. In the experiments, we utilize SHA-256, 256-bit BLS signature, and Barreto-Naehrig (BN) [50] curve defined over prime field GF(p) with p = 256 bits and embedding degree = 12 (the BN curve with these parameters is provided by the MIRACL library). To evaluate the computation overhead on the owner side due to dynamic operations, we perform 100 different block operations from which 50% are executed following revocations (this percent is higher than an average value in practical applications). Scalability (i.e., how the system performs when more users are added) is an important feature of cloud storage systems. The access control of the proposed scheme depends on the square root of the total number of system users. To identify the dishonest party in the system in case of disputes, the TTP verifies two signatures (F and T), computes combined hashes for the data (file and table), and compare the computes hashes with the authentic values (THTTP and FHTTP). 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 accomplish its work. In practice, the TTP may choose to split 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.

VI. CONCLUSIONS

Outsourcing data to remote servers has become a growing trend for many organizations to alleviate the burden of local data storage and maintenance. In this work we have studied different aspects of outsourcing data storage: block-level data dynamic, newness, mutual trust, and access control. We have proposed a cloud-based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity/newness, a TTP is able to determine the dishonest party. The data owner enforces access control for the outsourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, –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.

[2] Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.- J. Quisquater, ―Efficient remote data possession checking in critical information infrastructures,‖ *IEEE Trans. on Knowl. And Data Eng.*, vol. 20, no. 8, 2008.

[3] Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, ―Scalable and efficient provable data possession,‖ in *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks*, 2008, pp. 1–10.

[4] Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, ―Dynamic provable data possession,‖ in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009, pp. 213–222.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, ―Enabling public verifiability and data dynamics for storage security in cloud computing,‖ in *Proceedings of the 14th European Conference on Research in Computer Security*, 2009, pp. 355–370.

[6] Barsoum and M. A. Hasan, ―Provable possession and replication of data over cloud servers,‖ Centre For Applied Cryptographic Research, Report 2010/32, 2010, http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-32.pdf.

[7] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ―MR-PDP: multiple- replica provable data possession,‖ in *28th IEEE ICDCS*, 2008, pp. 411– 420.

[8] 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 *Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*, 2009.

[11] Juels and B. S. Kaliski, ―PORs: Proofs of Retrievability for large files,‖ in *CCS'07: Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 584–597.

[12] Shacham and B. Waters, ―Compact proofs of retrievability,‖ in *ASIACRYPT '08*, 2008, pp. 90–107.

[13] 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: File and Storage Technologies*, 2003.

[14] 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*, 2003.

[15] Ateniese, K. Fu, M. Green, and S. Hohenberger, ―Improved proxy re- encryption schemes with applications to secure distributed storage,‖ in *NDSS*, 2005.

[16] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, ―Over-encryption: Management of access control evolution on outsourced data,‖ in *Proceedings of the 33rd International Conference on Very Large Data Bases*. ACM, 2007, pp. 123–134.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control of encrypted data,‖ in *CCS '06*, 2006, pp. 89–98.

[18] S. Yu, C. Wang, K. Ren, and W. Lou, ―Achieving secure, scalable, and fine-grained data access control in cloud computing,‖ in *INFOCOM'10*, 2010, pp. 534–542.

[19] 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*, 2011.

[20] K. E. Fu, ―Group sharing and random access in cryptographic storage file systems, ‖ Master's thesis, MIT, Tech. Rep., 1999.