IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

Certificateless Public Integrity Checking of Group Shared Data in Cloud Storage

Pranav Pujari[1], Ritesh Pawar[2], Vadnaya Wable[3], Ghanshyam Ramole[4], Narendra Joshi[5]
Students, Department of Cloud Technology and Information Technology[1234]
Guide, Department of Cloud Technology and Information Security[5]
Sandip University, Nashik, India

Abstract: *Cloud storage service supplies people with an efficient method to share data within a group. The cloud server is not trustworthy, so lots of remote data possession checking (RDPC) protocols are proposed and thought to bean effective way to ensure the data integrity. However, mostof RDPC protocols are based on the mechanism of traditional public key infrastructure (PKI), which has obvious security flaw and bears big burden of certificate management. To avoid this shortcoming, identity-based cryptography (IBC) is often chosen to be the basis of RDPC.Unfortunately, IBC has an inherent drawback of key escrow. To solve these problems, we utilize the technique ofcertificateless signature to present a new RDPC protocol for checking the integrity of data shared among a group. Inour scheme, user's private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. To ensure the right public keys are chosen during the data integrity checking, the public key of each user is associated with her unique identity, for example the name or telephone number. Thus, the certificate is not needed and the problem of key escrow is eliminated too. Meanwhile, the data integrity can still be audited by public verifier without downloading the whole data. In addition, our scheme also supports efficient user revocation from the group. The security of our scheme is reduced to the assumptions of computational Diffie- Hellman (CDH) and discrete logarithm (DL). Experiment results exhibit that the new protocol is very efficient and feasible.*

Keywords: Remote data checking, Cloud storage, Certificateless signature, Data shared in group

I. INTRODUCTION

Cloud storage service offers user an efficient way to share data and work as a team. Once someone of the team uploads a file to the server, other members can access and modify the file by Internet. Many real applications such as Dropbox for Business [1] and TortoiseSVN [2] are used in many companies for their staff to work together. The most important problem of such applications is whether the cloud server provider (CSP) can ensure the data to be kept intact [3]. In fact, the CSP is not fully trustworthy and the failure of software or hardware is inevitable in some way, so serious accidents of the data corruption may occur at any time. Therefore, the user needs to audit the CSP to confirm the data on the cloud server is original. To ensure the integrity of stored data, a great number of RDPC schemes are proposed [4-32]. In these schemes, each data block generates an authentication tag which is bound with the block. By checking the correctness of the tags, the verifier can learn the status of the data. However, most of these schemes only focus on checking the integrity for personal data [4-21, 29-32], which is not valid under the situation of data shared in a group. When data is shared among multiple users, some new challenges appear which are not well solved in the RDPC schemes for personal data. For example, block tags may be generated by any group user, and different group user will output different tags even if the block is the same one.

Moreover, when a group user updates a block, it should regenerate the tag again. When auditing the data integrity, all the authentication tags generated individually need to be aggregated and the information of all the generators for these tags will be involved in. It brings great complexity for the checking scheme. Furthermore, the group is dynamic, any group member may initiatively leave or be fired from the group at any time, so the user revocation is also an important problem that must be addressed. More specifically, once a user is revoked, he should not be

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

allowed to access or modify the data and all his public/private keys are invalid. Under this situation, it is impossible to check the correctness of the tags made by revoked user. Thus, all the tags made by revoked user should be renewed by other normal user. The traditional method is to download the blocks signed by revoked user from the CSP, calculate the new tags and upload the new tags to the cloud again. It will increase heavy computation and communication cost for the normal user.

Until now, lots of schemes [22-28] have been presented for the integrity verification of data shared in group. However, most of existing RDPC schemes [22-26, 28] are based on PKI. Although PKI is widely used and occupies an important position in public key cryptography, there are still some security threats in it. For example, the security of PKI is based on the trustworthy of certificate authority (CA), but it is not an easy work to ensure the trustworthiness of CA. Besides, the management of certificate such as distribution, storage, revocation, and verification are also a big burden. To avoid these problems, some ID-based RDPC schemes [27, 28] are proposed. Unfortunately, ID-based RDPC schemes suffer from key escrow problem. Namely, the private key generator (PKG) generates all the private keys for the users. If PKG is untrusted,the scheme is not secure either. Thus, ID-based RDPC schemesmay be restricted to small, closed settings. Compared with PKIand IBC, certificateless cryptography [33] solves the problems of certificate management and key escrow at the same time. Toconstruct certificateless RDPC scheme is a good method for cloud data integrity checking.

II. RELATED WORKS

The first RDPC protocol for remote data checking was proposed by Deswarte et al. [4], in which an RSA-based hash function was utilized to generate the authentication tag of the data. Following it, a great number of provable data possession (PDP) [5] and proof of retrievability (POR) [29] schemes were proposed to solve the issue for data integrity verification. Ateniese et al. [5] first presented PDP model and initially introduced the technique of probabilistic integrity checking for the remote data. However, the first PDP scheme was only suitable for static data. To meet dynamic operations of the data block, Ateniese et al. [6] proposed another scalable and efficient PDP scheme by symmetric encryption, which supported block appending, updating, and deleting. Sebé et al. [7] presented a PDP protocol based on the hard problem of factoring large integers. Erway et al. [8] utilized the authenticated skip list to provide a fully dynamic PDP scheme, which supported data owner to insert, append, modify, and delete data blocks. Based on the technique of random masking and the homomorphic linear authenticator, Wang et al. [9] presented a public verification PDP scheme with property of privacy- preserving. To support the public auditability and data dynamics, Wang et al. [10] utilized Merkle hash tree (MHT) to present a dynamic scheme for cloud data checking. The scheme was fully dynamic and allowed anyone to verify the file integrity with public keys. MHT was also used in schemes [11-12] to implement data dynamic. However, due to the computation complexity of the MHT, this scheme caused heavy computation cost and communication cost. To overcome this shortcoming, Yang and Jia [13] introduced a linear index table to support data dynamic. Yan et al. [14] further optimized the implementation of linear index table and provided an efficient RDPC scheme. Feng et al. [15] presented a public remote integrity checking scheme, which could protect the user identity on file level to reduce the storage and communication cost. Zhu et al. [16] provided a cooperative PDP scheme for the multi-cloud setting, in which the data blocks were stored on different cloud servers. To improve the security, Wang [17] proposed another identity-based PDP scheme for multi-cloud setting without certificate management. Recently, Wang et al.

[18] presented an incentive and unconditionally anonymous identity-based public PDP scheme. To reduce the computation cost of data owner, Wang et al. [19] presented a proxy-oriented PDP scheme which moved the work of tag generation from data owner to proxy. To address the problem of key escrow and certificate management, two PDP scheme based on certificateless [20] and certificate-based cryptography [21] were proposed respectively. All the schemes mentioned above focused on the integrity verification for personal data. In 2012, Wang et al. [22] proposed a protocol for checking the integrity of data shared in a group. They utilized the technique of group signature to generate each authentication tag to preserve the tag generator's privacy. Wang et al. [23] proposed another PDP scheme for group data which supported the group user's joining and leaving. Based on broadcast encryption and group signature techniques, Liu et al. [24] provided a PDP scheme for group data. To improve the efficiency, Wang et al. [25] presented another scheme based on ring signature technique. However, these two

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

schemes did not solve the problem of user revocation. To address this issue, Wang et al. [26] used proxy re-signature technique to propose a new scheme with user revocation. Yu et al. [27] presented a PDP scheme without paring, which also supported dynamic group.

III. LITERATURE REVIEW

1. Public Integrity Checking

Public integrity checking ensures the correctness and integrity of data stored in cloud environments without requiring the data owner to retrieve the entire data set. Key concepts and approaches include:

Provable Data Possession (PDP):

- PDP schemes enable users to verify data integrity without downloading the entire dataset.
- Ateniese et al. (2007) proposed the first PDP scheme, but it was designed for static data and single-user scenarios
- Variants of PDP, such as scalable PDP (SPDP), aim to reduce computational overhead by using homomorphic verifiable tags.

Proof of Retrievability (PoR):

- PoR schemes, like those introduced by Juels and Kaliski (2007), verify both the integrity and retrievability of data.
- These schemes are storage-intensive due to the need for additional metadata.

Auditing Protocols:

- Wang et al. (2010) introduced third-party auditing (TPA) for public integrity verification, allowing independent verification without exposing sensitive data.
- Challenges: Most schemes are limited to static datasets or require significant computational resources.

2. Certificateless Cryptography

- Certificateless cryptography eliminates the need for certificates in traditional PKI and avoids the key escrow problem found in identity-based cryptography (IBC).

Certificateless Public Key Infrastructure (CL-PKI):

- Proposed by Al-Riyami and Paterson (2003), CL-PKI combines the benefits of PKI and IBC while addressing their respective shortcomings.
- In CL-PKI, private keys are derived from a partial private key (from the key generation center) and a user-generated secret, ensuring no single entity holds complete control.

Applications in Cloud Security:

- Certificateless encryption and signature schemes are widely used in secure data sharing and communication.
- Works by Sun et al. (2014) and Zhang et al. (2016) highlighted certificateless encryption schemes tailored for cloud storage.

Limitations in Existing Certificateless Approaches:

- High computational overhead for large datasets.
- Lack of support for dynamic group membership and real-time data updates.

3. Dynamic Group Data Sharing

Dynamic group sharing introduces unique challenges in managing group membership and ensuring data integrity for all members.

Group-Based Key Management:

- Key management schemes, like those proposed by Wang et al. (2015), focus on efficient revocation and rekeying for group members.
- Limitations: Certificate-based approaches complicate the process due to frequent updates in keys and certificates.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

Efficient User Revocation:

- Yang et al. (2013) proposed schemes for revoking users without re-encrypting the entire dataset.
- Certificateless approaches, however, remain underexplored in dynamic groups.

Access Control and Integrity:

- Proxy re-encryption schemes have been studied for managing access control in shared data scenarios (Chu et al., 2014).
- Integration with public integrity checking remains a challenge, especially in certificateless environments.

IV. PROPOSED SCHEME

System Model:

- **Entities**: Data Owner (DO), Group Members, Cloud Service Provider (CSP), Third-Party Auditor (TPA).
- **Processes**: Data generation, storage, integrity checking, user revocation, and public auditing.

Threat Model:

- Assumptions about adversaries (e.g., malicious CSP, revoked users).
- Security goals, including integrity, confidentiality, and resistance to collusion attacks.

Key Features:

- **Certificateless Integrity Verification**: Eliminates the need for certificates, reducing management complexity.
- **Dynamic Group Membership**: Supports efficient addition and revocation of users without affecting existing members.
- **Public Auditing**: A third-party auditor can verify data integrity without accessing the actual data.
- **Privacy Preservation**: Ensures the confidentiality of user data during auditing.

Techniques:

- Use of bilinear pairings and elliptic curve cryptography (ECC) for lightweight computation.
- Aggregate signatures for efficient integrity verification.
- Key distribution mechanisms that avoid key escrow

V. SYSTEM MODEL

This image (Fig.01) represents the conceptual architecture of a **Certificateless Public Integrity Checking System for Group Shared Data in Cloud Storage**. Below is a detailed explanation of the entities and processes depicted in the diagram:

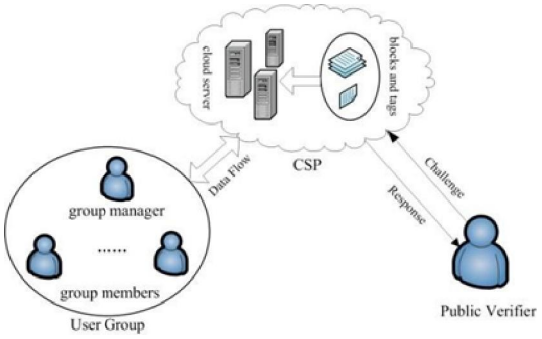

Fig.01

Entities in the Diagram: -

User Group:

Group Manager:

- Responsible for managing the group and coordinating access to shared data.
- Performs tasks such as adding or revoking group members, generating group keys, and delegating specific operations to members.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

- Often acts as the data owner who uploads the data to the cloud server.

Group Members:

- Members who have authorized access to shared data in the group.
- They can perform operations like downloading, verifying integrity, or appending new data to the shared dataset.

Cloud Service Provider (CSP):

- A third-party entity that provides storage and computational resources for hosting the group's shared data.
- Stores the data as **blocks and tags**, where:
  - **Blocks**: The actual data chunks stored in the cloud.
  - **Tags**: Metadata or cryptographic verification tokens used for integrity checking.
- CSP is assumed to be semi-trusted, meaning it may behave honestly but could also maliciously tamper with or delete data to save storage space

Public Verifier:

- An external entity (e.g., Third-Party Auditor or TPA) that verifies the integrity of the group-shared data stored in the cloud.
- The verifier operates without requiring access to the actual data, ensuring privacy and confidentiality.
- The verifier issues a **challenge** to the CSP and validates the **response** received, confirming the correctness of the stored data.

Processes Illustrated

Data Flow:

- The **Group Manager** uploads data to the CSP after preprocessing it into data blocks and generating tags for each block.
- Group members can access or verify the shared data through the CSP.

Challenge-Response Protocol:

- The **Public Verifier** initiates an integrity-checking process by sending a **challenge** to the CSP.
- The CSP computes a **response** based on the requested data blocks and their corresponding tags.
- The verifier validates this response using cryptographic operations to ensure data integrity.

Block and Tag Structure:

- Data is divided into smaller blocks for storage efficiency and ease of verification.
- Each block is associated with a unique tag generated using cryptographic algorithms (e.g., hash functions, signatures).
- Tags play a critical role in enabling the verifier to check data integrity without accessing the raw data.

Dynamic Group Management:

The group manager ensures secure and seamless integration of dynamic operations, such as:

- **Adding Members**: Newly added members receive the necessary keys or credentials to access data.
- **Revoking Members**: Revoked members lose access to the data without re-encrypting the entire dataset.
- **Data Updates**: Data modifications or additions are reflected in the CSP, with new tags generated for updated blocks.

VI. PERFORMANCE EVALUATION

Performance evaluation is a critical component to validate the practicality and efficiency of the proposed certificateless public integrity-checking scheme for group-shared data in cloud storage. The evaluation typically involves three aspects: security analysis, computational efficiency, and communication overhead. Here is a detailed explanation:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

1. Security Analysis

The scheme's robustness against various attack scenarios is assessed through formal security proofs and simulation. Key security properties such as data confidentiality, integrity, and resistance to attacks (e.g., collusion, forgery, and replay attacks) are analysed. For example:

- **Data Integrity**: Verifying that the scheme can detect unauthorized modifications to the shared data.
- **Resistance to Collusion**: Ensuring that a group of malicious users or a compromised cloud service provider cannot forge valid proofs.
- **Key Escrow Prevention**: Demonstrating that the certificateless nature prevents a single authority (such as the PKG) from compromising user security.

2. Computational Efficiency

The computational cost of the scheme is evaluated by measuring the time required for key operations, including:

- **Key Generation**: Both partial key generation by the PKG and the user's private key computation are benchmarked to ensure efficiency.
- **Proof Generation and Verification**: The scheme's efficiency in generating and verifying integrity proofs is compared to existing methods. For example, using lightweight cryptographic techniques like bilinear pairings or aggregate signatures minimizes computational overhead.
- **Data Updates**: The time complexity for adding, modifying, or deleting data blocks is analysed, particularly for dynamic group environments where frequent updates occur.

3. Communication Overhead

The scheme's communication cost is assessed based on the size of the integrity proof and the data transmitted between the user, cloud service provider (CSP), and third-party auditor (TPA). Efficient aggregation techniques are often employed to minimize the bandwidth usage, even for large datasets and frequent verification requests. Comparative analysis with other schemes demonstrates the proposed method's advantage in maintaining low communication overhead.

VII. CONCLUSION

In this paper, we present a novel RDPC scheme for dataoutsourced on cloud server. Our scheme devotes to solve the integrity checking for the group data which is shared among many clients of a team. We utilize the idea of certificatelesssignature to generate all the block tags. Because each user of agroup has both partial key and secret value, the problem of key escrow is eliminated in our scheme and the certificate management in PKI does not exist. Besides, our scheme supports public verification, efficient user revocation and multiuser data modification. We give the detailed description ofthe system model and security model of our scheme. At last, based on the CDH and DL assumption, we prove the security ofour scheme. The experiment results show that our scheme hasgood efficiency

REFERENCES

[1] Dropbox for Business. [Online]. Available: https://www.dropbox.com/ business, accessed Sep. 16, 2016.
[2] TortoiseSVN. [Online]. Available: https://tortoisesvn.net/, accessed Sep. 16, 2016.
[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comp. Syst., vol. 25, no. 6, pp. 599 – 616, 2009.
[4] Y. Deswarte, J. J. Quisquater, and A. Saïdane, "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS'03), pp. 1-11.
[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ''Provable Data Possession at Untrusted Stores,'' in Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS'07), pp. 598-609.
[6] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, ''Scalable and Efficient Provable Data Possession,'' in Proc. 4th Int'l Conf. Security and Privacy in Commun. Netw. (SecureComm'08), pp. 1-10.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 5, November 2024

[7] F. Sebé, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.
[8] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession,'' in Proc. 16th ACM Conf. on Comput. and Commun. Security (CCS'09), pp. 213-222.
[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ''Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847-859, May, 2011.
[10] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013