ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

PUBLIC-PRESERVING PUBLIC AUDITING FOR SHARE CLOUD DATA WITH SECURE GROUP MANAGEMENT

[1] Mr.B.N.S.GUPTA, [2] KANDRIKA SIVAKALYAN

[1](Associate Professor), MCA, S.V.K.P & Dr K.S. Raju Arts & Science College(A) Penugonda, W.G.District,Andhra Pradesh, bnsgupta@gmail.com

[2]PG, scholar, S.V.K.P & Dr K.S. Raju Arts & Science College(A) Penugonda, W.G.District, Andhra Pradesh, kskalyan00@gmail.com

ABSTRACT

With cloud storage services, users can store their data in the cloud and efficiently access the data at any time and any location.

However, when data are stored in the cloud, there is a risk of data loss because users lose direct control over their data. To solve this problem, many cloud storage auditing techniques have been studied.

In 2019, Tian *et al.* proposed a public auditing scheme for shared data that supports data privacy, identity traceability, and group dynamics.

In this paper, we point out that their scheme is insecure against tag forgery or proof forgery attacks, which means that, even if the cloud server has deleted some outsourced data, it can still generate valid proof that the server had accurately stored the data.

We then propose a newscheme that provides the same functionalities and is secure against the above attacks. Moreover, we compare the results with other schemes in terms of computation and communication costs

1.INTRODUCTION

Cloud storage provides users with significant storage capacity and advantages such as a cost reduction, scalability, and convenient access to the stored data. Therefore, cloud storage that is managed and maintained by professional cloud service providers (CSPs) is widely used by many enterprises and personal clients . Once the data are stored in cloud storage, the

clients lose direct control over the stored _les. Despite this, the CSPs must ensure that the client data are placed in cloud storage without any modification or substitution. The simplest way to achieve this is by checking the integrity of the stored data after downloading. When the capacity of the stored data is large, it is quite inefficient, and thus many methods for verifying the integrity of the data stored in the cloud without a full download have been proposed [2]_[34].

These techniques are called cloud storage auditing and can be classified into private auditing and public auditing according to the subject of the integrity verification. In private auditing, verification is achieved by users who have ownership of the stored data. Public auditing is conducted by a third-party auditor (TPA) on behalf of the users to reduce their burden, and thus public auditing schemes are more widely employed for cloud storage auditing.

Public auditing schemes provide various properties depending on the environment, such as privacy preservation [5]_[9], data dynamics [10]_[13], and shared data [14]_[33]. Privacy-preserving auditing is used to conduct an integrity verification while protecting data information from the TPA, and dynamic data auditing is where legitimate users are free to add, delete, or change the stored data.

Shared data auditing means freely sharing data within a legitimate user group. In this case, a legitimate user group should be defined, and user addition and revocation should be carefully considered. Recently, schemes that satisfy identity traceability, a concept that can trace the abnormal behavior of legitimate users in shared data auditing, have also been proposed.

Tian et al. [25] proposed a scheme that supports privacy preservation, data dynamics, and identity traceability in shared data auditing.

For efficient user enrollment and revocation, the authors adopted the lazy revocation technique. Moreover, to secure the design against collusion attacks between the revoked user and server, they apply a technique in which the group manager manages messages

and tag blocks generated by the revoked user to the scheme. Because the lazy-revocation technique is applied to the scheme, even if a user is revoked, no additional operation occurs until additional changes are made to the block.

In this paper, we show that Tian et al.'s scheme [25] is insecure against two types of attacks, a tag forgery and a proof forgery, and proposed a new scheme that provides the same functionality and is secure against the above attacks.

In this scheme, a tag forgery is possible by exploiting the vulnerability in which the tag is created in a malleable way, and a proof forgery is possible by exploiting the secret value being exposed to the server when additional changes to the block occur after the user is revoked. In general, the contributions of this study can be summarized as follows

1. We show that Tian et al.'s scheme [25] is insecure against two types of attacks: tag and proof forgeries. In tag forgery, we show that an attacker can create a valid tag for the modified message without knowing any secret values. In the proof forgery, we show that an attacker can create a valid proof for the given challenged message even if some _les stored on the cloud have been deleted.

2. We design a new public auditing scheme that is secure against the above attacks and has the same functionalities, such as privacy preservation, data dynamics, data sharing, and identity traceability. We changed the tag generation method to eliminate the malleable property and the data proof generation method to enhance the privacy preservation. We also changed the lazy revocation process to protect the secret information from the CSP and proposed an active revocation process to flexibly apply the various environments.

3. We formally prove the security of the proposed scheme. According to the theorems, the attacker cannot generate a valid tag and proof without knowing the

secret values or the original messages, respectively. We also provide comparison results with other schemes

in terms of the computation and communication costs.

The rest of this paper is organized as follows. In Section II, we introduce the background, and in Section III, we review Tian et al.'s scheme [25].We present our detailed scheme for public auditing in Section IV, and provide the security and efficiency of our scheme in Section V. Finally, we conclude this paper in Section VI.

2.LITERATURE SURVEY

The advent of cloud computing has revolutionized data storage and sharing, offering unprecedented flexibility and scalability. However, this paradigm shift also introduces significant security and privacy challenges, particularly when sensitive data is shared among a group of users.

Public-preserving public auditing has emerged as a crucial solution, allowing data owners to ensure the integrity of their data while enabling third-party auditors to verify data correctness without compromising privacy.

Secure group management further complicates this scenario, necessitating robust mechanisms to handle dynamic membership changes, access control, and group key management.

This literature survey explores the intersection of public-preserving public auditing and secure group management, reviewing key methodologies, cryptographic techniques, and system architectures proposed in recent research.

The survey aims to provide a comprehensive overview of existing solutions, identify current gaps, and suggest potential directions for future work in enhancing security and privacy in shared cloud environments.

3. EXISTING SYSTEM

Ateniese *et al.* [2] first introduced a provable data possession scheme called PDP and provided two provably secure PDP schemes using RSA-based homomorphic authenticators. This supports public verification with lower communication and computation costs.

At the same time, Juels *et al.* [3] first proposed the concept and a formal security model of proof of retrievability (POR) and a sentinel-based POR scheme with certain properties. Later, Shacham *et al.* [4] improved the POR scheme and proposed a new public auditing scheme that was built from the BLS signature [36] and is secure in the random oracle model. In recent years, many studies have been conducted on cloud storage auditing, supporting various functionalities such as data privacy preservation, data dynamics, and shared data.

Erway *et al.* [10] first proposed the PDP scheme using a rank-based authenticated skip list to support data dynamics. However, the scheme suffers from high computational and communication costs, and to address this concern, Wang *et al.* [11] proposed a new auditing scheme employing the Merkle Hash Tree (MHT), which is much simpler.

Although Wang *et al.* [5] proposed a privacy-preserving public auditing scheme, their approach requires heavy communication and computation costs in the audit and data update process. Zhu *et al.* [12] also proposed a new scheme using another authenticated data structure, called an index hash table (IHT), to support data dynamics. Although this scheme succeeded in reducing the communication and computation costs, it did not resolve the inefficient problem of lookup and updating operations. Shen *et al.* [13] proposed a new efficient scheme with a doubly linked information table and location array. Tian *et al.* [25] recently proposed a more efficient scheme using a dynamic hash table (DHT), which has been proven to be more effective than IHT for data updating [12]. In terms of data privacy, Wang *et al.* [5] first proposed a privacy-preserving public auditing scheme to protect data privacy through random masking, and many schemes for predicting data privacy have been studied [6]_[9].

Wang *et al.* [14] proposed an efficient public auditing scheme called Knox for shared data. The scheme supports hiding the identity of individual users based on a group signature, but does

not support a user revocation. In Oruta [15], a ring signature is used to hide the identity of individual users; however,the scheme also has a problem in that all user keys and block tags must be regenerated to provide a user revocation.

Wang *et al.* [16] also proposed a scheme that can achieve a user revocation using a proxy re-signature. The scheme utilizes a proxy for a resigning used to update the tag generated by the revoked user; however, it is vulnerable to collusion attacks between an invalid user and the cloud server.

In addition, Jiang *et al.* [17] proposed a new public auditing scheme that combines a vector commitment [37] and a verifier-local-revocation group signature [38]. During the revocation phase, the computational costs are relatively high because it is necessary to first find the tags generated by the revoked user and regenerate them. Yu *et al.* [18], [19] also proposed a new scheme using polynomial authentication tags and proxy re-signatures. Although this scheme can reduce the communication overhead during verification, it can suffer from a collusion attack because the revoked user still has a valid private key and might collude with the CSP

4. PROPOSED SYSTEM.

1. We show that Tian *et al.*'s scheme [25] is insecure against two types of attacks: tag and proof forgeries. In tag forgery, we show that an attacker can create a valid tag for the modified message without knowing any secret values. In the proof forgery, we show that an attacker can create a valid proof for the given challenged message even if some files stored on the cloud have been deleted.

2. We design a new public auditing scheme that is secure against the above attacks and has the same functionalities, such as privacy preservation, data dynamics, data sharing, and identity traceability. We changed the tag generation method to eliminate the malleable property and the data proof generation method to enhance the privacy preservation. We also changed the lazy revocation process to protect the secret information from the CSP and proposed an active revocation process

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

to flexibly apply the various environments.

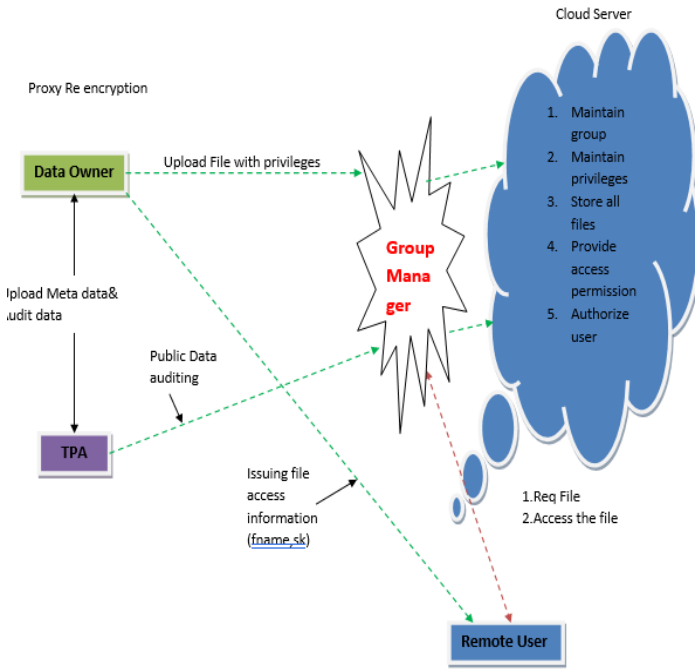
3. We formally prove the security of the proposed scheme. According to the theorems, the attacker cannot generate a valid tag and proof without knowing the secret values or the original messages, respectively. We also provide comparison results with other schemes in terms of the computation and communication costs.

Advantages

- In the proposed system, to manage the data blocks handled by revoked users, we use an extended dynamic hash table (EDHT).

In the proposed system, the modification record table (MRT) is a table in which the group manager records operations for each block to provide identity traceability and is a two-dimensional data structure

5. SYSTEM ARCHITECTURE



6. MODULES

Modules Involved in Privacy-Preserving Public Auditing for Shared Cloud Data With Secure Group Management

To implement the system for privacy-preserving public auditing of shared cloud data with secure group management, the following modules are essential:

1. User Management Module

1.1 **User Registration**

- Handles user sign-up, email verification, and role assignment.

1.2 **User Authentication**

- Manages user login, multi-factor authentication, and session management.

1.3 **Role-Based Access Control (RBAC)**

- Controls access permissions based on user roles (e.g., User, Administrator, Auditor).

2. Data Management Module

2.1 **Data Upload and Encryption**

- Provides interfaces for users to upload data.
- Encrypts data before storage using secure encryption algorithms (e.g., AES-256).

2.2 **Data Access and Decryption**

- Manages decryption keys and provides data access to authorized users.

2.3 **Metadata Management**

- Stores metadata for each encrypted file to facilitate auditing and access management.

3. Auditing Module

3.1 **Audit Request Handling**

- Allows TPAs and users to request audits of specific data sets.

3.2 **Proof of Integrity Generation**

- Generates cryptographic proofs (e.g., using homomorphic encryption or zero-knowledge proofs) to verify data integrity without exposing data content.

3.3 **Audit Verification**

- Verifies the cryptographic proofs and confirms the integrity of the data.

3.4 **Audit Log Management**

- Maintains logs of all audit activities, ensuring logs are tamper-evident and accessible only to authorized personnel.

4. Group Management Module

4.1 **Group Creation and Administration**

ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024

- Enables administrators to create and manage groups of users, assigning permissions and roles.

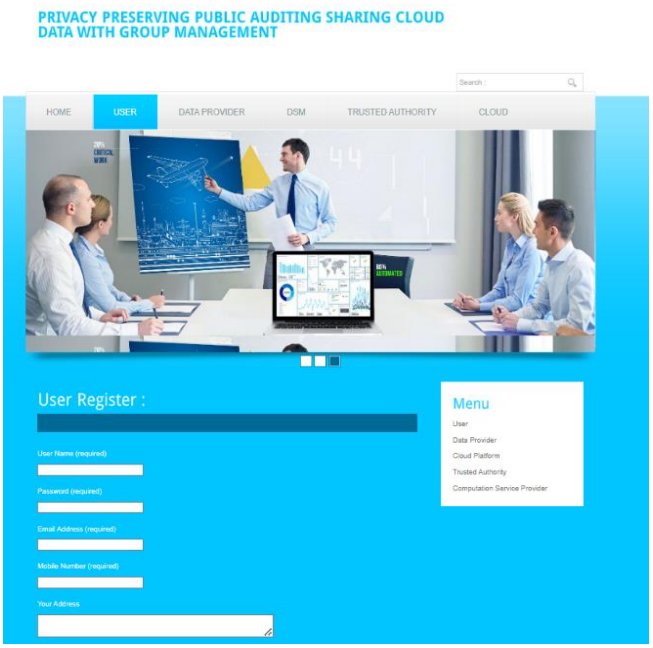
4.2 **User Addition and Removal**

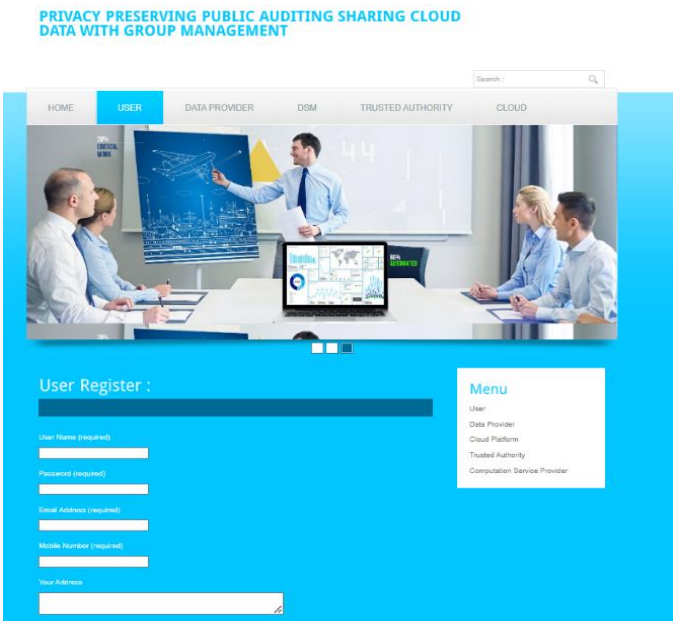
- Securely adds or removes users from groups, ensuring data integrity and confidentiality.

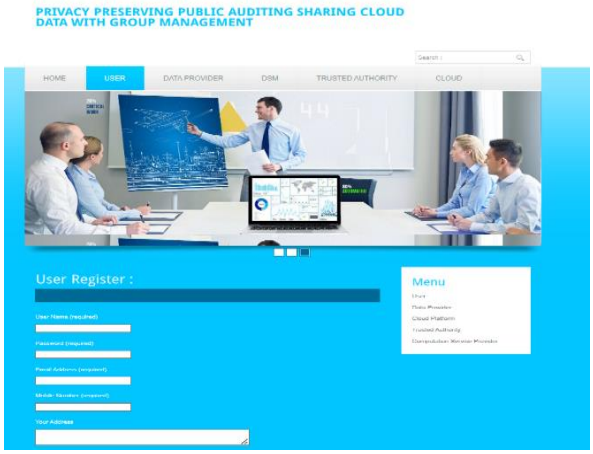
4.3 **Group Key Management**

- Manages cryptographic keys for each group, including key generation, distribution, and revocation.

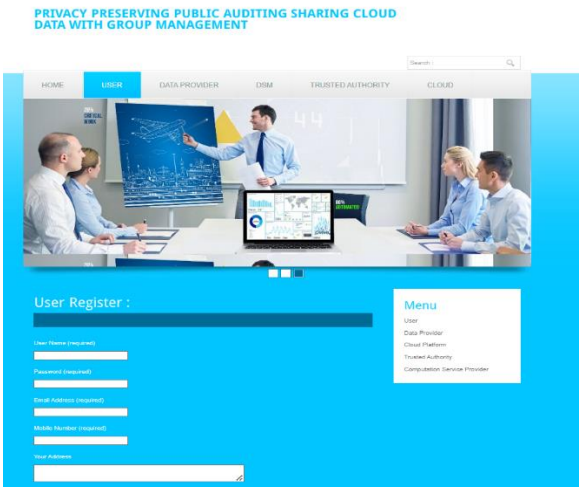
7. SCREENS







ISSN2321-2152
www.ijmece .com
Vol 12, Issue 2, 2024



8. CONCLUSION

Cloud storage auditing is an extremely important technique for resolving the problem of ensuring the integrity of stored data in cloud storage. Because the need for the concept is shared, many schemes providing different functions and security levels have been proposed. In 2019, Tian *et al.* [25] proposed a scheme that supports data privacy, identity traceability, and group dynamics and claimed that their scheme is secure against collusion attacks between the CSPs and revoked users. In this paper, we showed in their scheme that a tag can be forged from a valid message and tag pair without knowing any secret values. We also showed that a proof can be forged by a collusion attack, even if some challenged messages have been deleted. We then proposed a new scheme that is secure against the above attacks while providing the same functionality as their approach. We also provided formal security proofs and an analysis of the computation costs ofboth schemes.

Future enhancements of privacy-preserving public auditing for shared cloud data with secure group management could encompass several advanced features and improvements:

9. REFERENCE

1] (Apr. 2021). Cloud Storage-Global Market Trajectory and Analyt-
ics. [Online]. Available: https://www.researchandmarkets.com/reports/

5140992/cloud-storage-global-market-trajectory-and[2] 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. Comput. Commun. Secur. (CCS), 2007, pp. 598_609.
[3] A. Juels and B. S. Kaliski, ``PORs: Proofs of retrievability for large _les,"
in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007,
pp. 584_597.
[4] H. Shacham and B. Waters, ``Compact proofs of retrievability," in Proc.
Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer,
2008, pp. 90_107.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, ``Privacy-preserving public
auditing for data storage security in cloud computing," in Proc. IEEE
INFOCOM, Mar. 2010, pp. 1_9.
[6] Z. Hao, S. Zhong, and N. Yu, ``A privacy-preserving remote data integrity
checking protocol with data dynamics and public veri_ability," IEEE
Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432_1437, Sep. 2011.
[7] K. Yang and X. Jia, ``An ef_cient and secure dynamic auditing protocol
for data storage in cloud computing," IEEE Trans. Parallel Distrib. Syst.,
vol. 24, no. 9, pp. 1717_1726, Sep. 2013.
[8] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ``Privacypreserving
public auditing for secure cloud storage," IEEE Trans. Comput.,
vol. 62, no. 2, pp. 362_375, Feb. 2013.
[9] K. He, C. Huang, K. Yang, and J. Shi, ``Identity-preserving public auditing
for shared cloud data," in Proc. IEEE 23rd Int. Symp. Quality Service
(IWQoS), Jun. 2015, pp. 159_164.
[10] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ``Dynamic provable
data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur.
(CCS), New York, NY, USA, 2009, pp. 213_222.
[11] 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.

[12] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, ``Dynamic audit services for outsourced storages in clouds," IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227_238, Apr./Jun. 2013.

[13] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ``An ef_cient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402_2415, Oct. 2017.

[14] B. Wang, B. Li, and H. Li, ``Knox: Privacy-preserving auditing for shared data with large groups in the cloud," in Proc. 10th Interfaces Conf. Appl. Crypto. Netw. Secur., 2012, pp. 507_525.

[15] B. Wang, B. Li, and H. Li, ``Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43_56, Jan./Mar. 2014.

[16] B. Wang, B. Li, and H. Li, ``Panda: Public auditing for shared data with ef_cient user revocation in the cloud," IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92_106, Jan./Feb. 2015.

[17] T. Jiang, X. Chen, and J. Ma, ``Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Trans. Comput., vol. 65, no. 8, pp. 2363_2373, Aug. 2016.

[18] J. Yuan and S. Yu, ``Ef_cient public integrity checking for cloud data sharing with multi-user modi_cation," in Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM), Apr. 2014, pp. 2121_2129.

[19] J. Yuan and S. Yu, ``Public integrity auditing for dynamic data sharing with multiuser modi_cation," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717_1726, Aug. 2015.

[20] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ``Enabling public auditing for shared data in cloud storage supporting identity privacy and

traceability," *J. Syst. Softw.*, vol. 113, pp. 130_139, Mar. 2016.

[21] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, ``NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," *IEEE Trans. Big Data*, vol. 8, no. 1, pp. 14_24, Feb. 2022, doi: 10.1109/TBDATA.2017.2701347.

[22] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ``Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331_346, Feb. 2018.

[23] Y. Zhang, C. Chen, D. Zheng, R. Guo, and S. Xu, ``Shared dynamic data audit supporting anonymous user revocation in cloud storage," IEEE Access, vol. 7, pp. 113832_113843, 2019.

[24] G. Wu, Y. Mu, W. Susilo, F. Guo, and F. Zhang, ``Threshold privacypreserving cloud auditing with multiple uploaders," Int. J. Inf. Secur., vol. 18, no. 3, pp. 321_331, Jun. 2019.

[25] H. Tian, F. Nan, H. Jiang, C.-C. Chang, J. Ning, and Y. Huang, ``Public auditing for shared cloud data with ef_cient and secure group management," Inf. Sci., vol. 472, pp. 107_125, Jan. 2019.