Data sharing by conditioning privacy on cloud data

E.Aruna Assistant Professor in Department of Information Technology in Teegala Krisha Reddy Engineering college.Telangana
G.Vani UG Scholar in Department of Information Technology in Teegala Krisha Reddy Engineering college.Telangana
V.Naga Lakshmi UG Scholar in Department of Information Technology in Teegala Krisha Reddy Engineering college.
B.Rakesh UG Scholar in Department of Information Technology in Teegala Krisha Reddy Engineering college.

Abstract: Today, cloud storage becomes one of the critical services, because users can easily modify and share data with others in cloud. However, the integrity of shared cloud data is vul- nerable to inevitable hardware faults, software failures or human errors. To ensure the integrity of the shared data, some schemes have been designed to allow public verifiers (i.e., third party auditors) to efficiently audit data integrity without retrieving the entire users' data from cloud. Unfortunately, public auditing on the integrity of shared data may reveal data owners' sensitive information to the third party auditor. In this paper, we propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least t group managers to recover a trace key cooperatively, which eliminates the abuse of single-authority power and provides non- frameability. Moreover, our scheme ensures that group users can trace data changes through designated binary tree; and can recover the latest correct data block when the current data block is damaged. In addition, the formal security analysis and experimental results indicate that our scheme is provably secure and efficient.

Index Terms—Data Integrity; Homomorphic Verifiable; Non- frameability; Provable Security..

I. INTRODUCTION

Cloud data sharing increasing number of applications of shared data, such as iCloud, Google Docs, and so on, users can upload their data to a cloud and share it with other peers as a group. Unfortunately, since cloud servers are vulnerable to inevitable hardware faults, software failures or human errors, data stored in the cloud may be spoiled or lost. In the worst cases, a cloud owner may even conceal data error accidents in order to preserve its reputation or avoid profit losses . In addition, users who lose direct control over their data are not sure whether their cloud-stored data is intact or not. Therefore, integrity verification for the shared data in the cloud is an important, yet timely issue for a large number of cloud users.

In particular, in order to reduce the burden on users, a trusted third-party auditor (TPA) is engaged to conduct the verification, which is called public auditing . However, the TPA may have unnecessary access to private information dur- ing the auditing process . Therefore, researchers proposed some new schemes to protect privacy, including data privacy , and identity privacy . To be specific, the TPA cannot learn each block that is signed by a particular user in the group by constructing homomorphic authenticable ring signatures
or computing tags based on common group private key . However, since both methods concern about conditional privacy, the real identity of the signer can no longer be traced. A later development is the homomorphic authenticable group signature scheme based on group signatures], which is designed to protect privacy.
On one hand, the identity of each signer is anonymous; and on the other hand, the group manager can trace a signer's real identity after a dispute. Unfortunately, in all existing public auditing schemes, the tracing process is accomplished by a single entity. As a result, that entity has the privilege of tracing, which may lead to abuse of single-authority power. Therefore, an innocent user may be framed or a malicious user may be harbored.

Meanwhile, to support data dynamics, the data structure based on index hash table or Merkle Hash Tree (MHT) has been utilized efficiently. However, this kind of data structure merely records the newest data block with the corresponding signature, which prevents users from tracing the changes of the data blocks. When the current data has been corrupted, users cannot recover the old data from the records. Therefore, the problem of data traceability and recoverability also should be considered.

Moreover, a necessary authentication process is missing between the auditor and the cloud in most existing public auditing schemes, hence anyone can challenge the cloud for the auditing proofs. This problem will trigger network conges- tion and unnecessary waste of cloud resources. Although Liu *et al*. Resources designed such that each signed an authorized public auditing scheme to solve the problem, it is only suitable for a single client, and cannot be applied to group-shared data. Since the malicious or pretended auditors/users might constantly request cloud access for the auditing proof by utilizing TPA, unauthorized auditing is another important issue that should be addressed in integrity verification for shared cloud data.

In this paper, we propose a new privacy-aware public auditing mechanism, called *NPP*, for the shared cloud data with multiple group managers. Our contributions can be sum- marized as follows.

1) We establish a model for data (in a group) shared with multiple group managers, and propose a new privacy-preservation public auditing scheme for multiple group man- agers in shared cloud storage. Our proposed scheme can not only provide multi-levels privacy-preservation abilities (including identity privacy, traceability and non-frameability), but also can well support group user revocation.

2) We design a data structure based on a binary tree for clouds to record all the changes of data blocks. Group users can trace the data changes through the binary tree and recover the latest correct data block when the current data block is damaged.

3) We utilize an authorized authenticate process to verify TPA's challenge messages. Therefore, only the TPA who has been authorized by the group users can pass the authentication and then challenge the cloud, which protects clouds from malicious challenges.

4) Our formal security analysis and experimental results

show that *NPP* is provably secure and efficient.

Recently, to solve the problem of collusion attacks, Yuan *et al.* designed polynomial-based authentication tags, allowing aggregation of tags for different data blocks data. Their scheme allows secure delegation of user revocation operations to the cloud, permitting the cloud itself to conduct revocation without the participation of revoked users. Unfortunately, their scheme is also vulnerable to resist collusion attacks. If a revoked user colludes with the cloud, the cloud server can update the data as many times as the revoked user requests until it finally returns a legal data centers. Another attempt to solve the issue is the combination of vector commitments and group signatures with verifier-local revocation data. However, the computation cost of user revocation grows with the number of revoked users.

II. OBJECTIVE

To achieve integrity checking of the shared data in the cloud, *NPP* is expected to the following design objectives: **1) Public auditing:** Besides the group users, the TPA can also correctly check the integrity of the shared data in the cloud without retrieving entire users' data from cloud. **2) Authorized auditing:** Only the TPA that has been authorized by the group users can challenge the cloud. **3) Identity privacy:** During the process of auditing, the TPA cannot learn the identity of the group user from the signatures of the data blocks. **4) Traceability:** Under certain conditions, the group managers can reveal the signer's identity from the signatures and decide which group user has modified the data block. **5) Non-frameability:** Group managers can guarantee the fairness of the tracing process, i.e., innocent group user won't be framed and the misbehaved user won't be harbored by the group managers. **6) Support data traceability and recoverability:** Group users can easily trace the data changes and recover the latest correct data once current data is damaged. **7) Support group dynamics:** Group dynamics include two aspects. One is that GMs can easily join or leave the group, the other is that new users can be easily added into the group and misbehaved users can be efficiently excluded from the group.

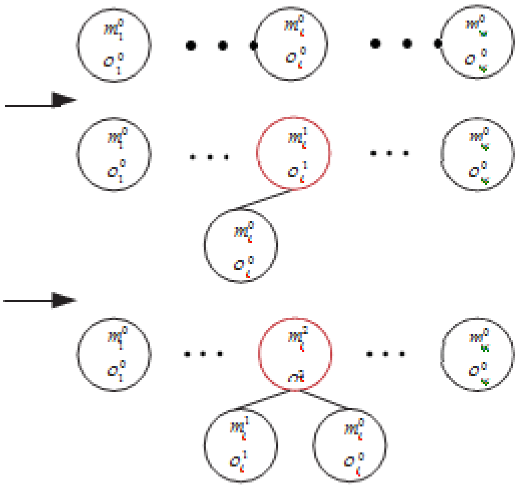


Figure:updation of records with scheme function.

With the *Authorize* algorithm, the group authorizes TPA to generate authorized auditing challenges, and then the valid TPA can check the integrity of the shared data on behalf of the group user. Once the cloud receives a challenge from TPA, the cloud verifies whether the challenge has been authorized and decides whether to generate the audit proof . TPA checks the correctness of the proof . Finally, in the at least many set centres work together to trace the real identity of the signer. When the damaged has been found, group users can recover the right data by the records. As the group users can verify the older blocks one by one until discover the latest correct block. the verification, then the latest right block has been found. Otherwise, the group users continue verifying the signatures one by one according to the order of traversal tree with the help of TPA until the latest right block is discovered. The verification algorithm can be found in the next section.

III. IMPLEMENTATION

. To protect data privacy, the data can be encrypted by the means of symmetrical encryption technology and attribute-based encryption technology before shared data is outsourced to the cloud

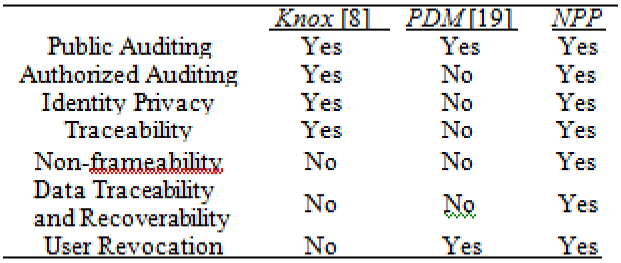
Messages autherisation to the cloud, and then the cloud generates a auditing proof message if the TPA is authorized. As following steps:

i. The TPA challenges the cloud as follows:

- Randomly choose a subset data from the setoff resources, where each data contains authorization.
- Generate random numbers for all set of data request where data is subset of main center.
- Send an auditing challenge message the cloud by generating private and public key of the cloud, the cloud can decrypt *ID by* private key to get *ID*.

ii. The cloud checks whether the TPA has been authorized as follows:

- Compute *ID* by decrypting *ID* with its private key *subset of data centers.*



	Knox [8]	*PDM* [19]	*NPP*
Public Auditing	Yes	Yes	Yes
Authorized Auditing	Yes	No	Yes
Identity Privacy	Yes	No	Yes
Traceability	Yes	No	Yes
Non-frameability	No	No	Yes
Data Traceability and Recoverability	No	No	Yes
User Revocation	No	Yes	Yes

Figure:comparisons of computations

Decrypt actual message to the cloud, and then the cloud generates a auditing proof message if the TPA is authorized. Computing public key to get access to data. the identity privacy of the group users. Moreover, unlike

the existing schemes, the proposed *NPP* requires at least *t* group managers to work together to trace the identity of the misbehaving user. Therefore, it eliminates the abuse of single- authority power and ensures non-frameability. Exceptionally, group users can trace the data changes through the designed binary tree and recover the latest correct data block when the current data block is damaged. In addition, the analysis and the experimental results show that *NPP* is provably secure and efficient.

Moreover, by implementing the postorder traversal to the additional binary tree and revealing the real identities from the signatures, GMs can trace each user data access.

IV.CONCLUSION

In this paper, we propose a novel multi-level privacy preserving public auditing scheme for cloud data sharing with multiple managers. During the process of auditing, the TPA cannot obtain the identities of the signers, which ensures the identity privacy of the group users. Moreover, unlike the existing schemes, the proposed *NPP* requires at least *t* group managers to work together to trace the identity of the misbehaving user. Therefore, it eliminates the abuse of single- authority power and ensures non-frameability. Exceptionally, group users can trace the data changes through the designed binary tree and recover the latest correct data block when the current data block is damaged. In addition, the analysis and the experimental results show that *NPP* is provably secure and efficient.

REFERENCES

[1] K.Yang, X.Jia, K.Ren, B.Zhang and R.Xie,”DAC-MACS: Effective data access control for multi authority cloud storage systems,”IEEE transactions on information Forensics & Security, vol. 7, 2012

[2]Ming Li,Shucheng Yu,Yao Zheng,Kui Ren,Wenjing Lou, “Scalable and secure sharing of personal heath records in cloud computing using attribute based encryption,”IEEE transactions on parallel and distributed systems, vol 24, 2013

[3]Elli Androulaki,Claudio Soriente,Luka malisa & Srdjan Capkun, ”Enforcing location and time based access controlon cloud stored data,IEEE 34 th international conference on Distributed computing systems,2014.

[4]Baishuang Hu, Qin Liu,Xuhui Liu,Tao Peng,Guojun Wang & Jie wu, ”DABKS:Dynamic attributebased Keyword search in cloud computing”,IEEE communication and information systems security symposium,2017

[5]Quin Liu, Guojun Wang, & Jie wu,”Clock based proxy Re-encryption scheme in unreliable cloud,”IEEE 41st international conference on parallel processing workshops, 2012

[6]Kan Yang, he Liu, Xiao Hua jia, “Time domain attribute based access control for cloud based video content sharing: A cryptographic approach, IEEE transaction on Multimedia, vol 18, 2016

[7]Kui Ren, Cong Wang & Quian Wang, “Security Challenges for the Public Cloud, IEEE Computer Society, Jan2012

[8]Cong Wang, Quian Wang & Kui Ren, ”Privacy preserving public auditing for data Storage Security in cloud Computing”,IEEE communication society,2010.

[9]J.Bethencourt,A Sahai andb.Waters “cipher text Policy Attribute based encryption,” In proceeding of the 28thIEEE symposium on security and privacy,IEEE 2007.

[10]R.L Rivest, A.Shamir and D.a Wagner,”Time lock puzzles and timed release Crypto,”Massachusets Institute of Technology, 1996

[11]Gartner Inc: Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: . Accessed: 15-Jul-2011 http://www.gartner.com/it/page.jsp?id=1454221 Online. Available: . Accessed: 15-Jul-2011

[12] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.Google Scholar

[13] Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN’10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.View ArticleGoogle Scholar

[14] Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011. Available:

[15] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.Google Scholar

[16] Giuseppe Pirr´o, Paolo Trunfio ,Domenico Talia, Paolo Missier andCarole Goble, 2010, “ERGOT: A Semantic-based System for Service Discovery in Distributed Infrastructures,” 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

[17]VijaykumarJavaraiah Brocade Advanced Networks and Telecommunication Systems (ANTS), 2011, “Backup for Cloud and Disaster Recovery for Consumers and SMBs,” IEEE 5th International Conference, 2011.

[18]Lili Sun, Jianwei An, Yang Yang, Ming Zeng, 2011, “Recovery Strategies for Service Composition in Dynamic Network,”
International Conference on Cloud and Service Computing.

[19]Xi Zhou, Junshuai Shi, YingxiaoXu, Yinsheng Li and Weiwei Sun, 2008, "A backup restoration algorithm of service composition in MANETs," Communication Technology ICCT 11th IEEE International Conference, pp. 588-591.

[20]Ms..KrutiSharma,ProfK.R.Singh, 2012, “Online data Backup And Disaster Recovery techniques in cloud computing:A review”, JEIT, Vol.2, Issue 5.

[21]Y.Ueno, N.Miyaho, and S.Suzuki, , 2009, “Disaster Recovery Mechanism using Widely Distributed Networking and Secure Metadata Handling Technology”, Proceedings of the 4th edition of the UPGRADE-CN workshop, pp. 45-48.