Group User Revocation and Integrity Auditing of Shared Data in Cloud Environment

K. SURESH BABU
PG Scholar
Dept of CSE
Krishna Chaitanya Institute of Technology & Sciences
Markapur, Prakasam Dist, AP, India.

J. MAHALAKSHMI
Associate Professor
Dept of CSE
Krishna Chaitanya Institute of Technology & Sciences
Markapur, Prakasam Dist, AP, India

Abstract: **The advent of the cloud computing makes storage outsourcing becomes a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some researches consider the problem of secure and efficient public data integrity auditing for shared dynamic data. In this paper, signifies that the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. Analysis shows a concrete scheme based on the scheme definition. The scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, count ability and traceability of secure group user revocation.**

Keywords: **Public Integrity Auditing, Dynamic Data, Victor Commitment, Group Signature, Cloud Computing.**

I. INTRODUCTION

The development of cloud computing motivates enterprises and organizations to outsource their data to third-party cloud service providers (CSPs), which will improve the storage limitation of resource con-strain local devices. Recently, some commercial cloud storage services, such as the simple storage service (S3) [1] on-line data backup services of Amazon and some practical cloud based software Google Drive [2], Dropbox [3], Mozy [4], Bitcasa [5], and Memopal [6], have been built for cloud application. Since the cloud servers may return an invalid result in some cases, such as server hardware/software failure, hu-man maintenance and malicious attack [7], new forms of assurance of data integrity and accessibility are required to protect the security and privacy of cloud user's data.

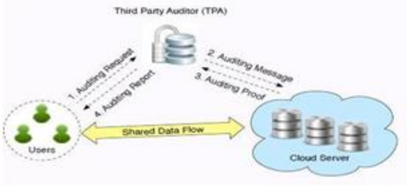
To overcome the above critical security challenge of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme [8] are far from practical application.

For providing the integrity and availability of re-mote cloud store, some solutions [10], [11] and their variants [12], [13], [14], [15], [16], [17], [18] have been proposed. In these solutions, when a scheme supports data modification, we call it *dynamic* scheme, otherwise *static* one (or limited dynamic scheme, if a scheme could only efficiently support some specified operation, such as append). A scheme is *publicly verifiable* means that the data integrity check can be performed not only by data owners, but also by any third-party auditor. Recently, the development of cloud computing boosted some applications [19], [20], [21], where the cloud service is used as a collaboration platform. In these software development environments, multiple users in a group need to share the source code, and they need to access, modify, compile and run the shared source code at any time and place. The new cooperation network model in cloud makes the re-mote data auditing schemes become infeasible, where only the data owner can update its data. To support multiple user data operation, Wang et al. [22] proposed data integrity based on ring signature. In the scheme, the user revocation problem is not considered and the auditing cost is linear to the group size and data size. To further enhance the previous scheme and support group user revocation, Wang et al. [23] designed a scheme based on proxy re-signatures.

II. EXISTING MECHANISM

In particular, this paper exploits the concept of group signature which computes the verification information required for integrity auditing of shared data. With this mechanism, the signer identity of each block in shared data remains private from a third party auditor (TPA) which can publicly verify shared data integrity without accessing entire data. In extend this mechanism support batch auditing. This paper represent first attempt towards designing effective public auditing of shared data in the cloud storage by preserving privacy.

The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices.



But this paper only shows that how to audit shared data integrity in a cloud with **static** group. It means groups of users already defined in cloud before shared data and membership of user is not changed during data sharing. The original user is responsible for deciding who is able to share its data before uploading data to the cloud. Another interesting problem is how to audit the integrity of shared data in the cloud with **dynamic** groups a new user can be added into the group and an existing group member can be revoked during data sharing while still preserving identity privacy. This will leave to future work.

III. PROPOSED SYSTEM

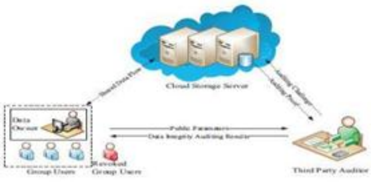
In this paper, we study the problem of constructing public authentication inspection for shared dynamic data with group user revocation. The paper contributions are:

1) For cipher text database, we explore on the secure and efficient shared data integrate auditing for multi-user operation.

2) We intend an efficient data auditing scheme along with new features such as traceability and countability by incorporating the vector commitment primitives, asymmetric group key agreement and group signature.

3) The analysis results show that the scheme is secure and efficient as we provide the security and efficiency analysis proposed scheme which will result in back-up and data storage in cloud.

4) The authorized duplicate check in the hybrid cloud architecture is supported by several deduplication constructions and this authorized duplicate check scheme comparatively incurs minimum overhead than normal operations.



The cloud storage model

IV. FORMULATION OF RESEARCH PROBLEM

Cloud Storage Model

In the cloud storage model as shown in Figure there are three entities, namely the cloud storage server, group users and a Third Part Auditor (TPA).

Group users consist of a data owner and a number of users who are authorized to access and modify the data by the data owner. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In this paper, the system gives us the data owner could encrypt and upload its data to the remote cloud storage server.

The data owner is different from the other group users, he/she could securely revoke a group user when a group user is found malicious or the contract of the user is expired.

Threat Model and Security Goals

The threat model considers two types of attack:

1) An attacker outside the group (include the revoked group user cloud storage server) may obtain some knowledge of the plaintext of the data. Actually, this kind of attacker has to at least break the security of the adopted group data encryption scheme.

2) The cloud storage server colludes with the revoked group users, and they want to provide a illegal data without being detected.

To overcome the problems above, we aim to achieve the following security goals in this paper:

Security. A scheme is secure if for any database and any probabilistic polynomial time adversary, the adversary cannot convince a verifier to accept an invalid output.

Correctness. A scheme is correct if for any database and for any updated data m by a valid group user, the output of the verification by an honest cloud storage server is always the value m. Here, m is a cipher text if the scheme could efficiently support encrypted database.

Efficiency. A scheme is efficient if for any data, the computation and storage overhead invested by any client user must be independent of the size of the shared data.

Countability. A scheme is countable, if for any data the TPA can provide a proof for this misbehavior, when the dishonest cloud storage server has tampered with the database.

Traceability. It requires that the data owner is able to trace the last user who updates the data (data item), when the data is generated by the generation algorithm and every signature generated by the user is valid.

Complexity Assumption

The security of our scheme relies on the difficulty of some problems: the Strong Diffie-Hellman problem, the Decision Linear problem, and the Computational Diffie-Hellman problem.

Vector Commitment

Commitment is a fundamental primitive in cryptography and it plays an important role in security protocols such as voting, identification, zero-knowledge proof, etc. The hiding property of commitment re-quires that it should not reveal information of the committed message, and the binding property re-quires that the committing mechanism should not allow a sender to change his/her mind about the committed message.

The primitive of verifiable database with efficient update based on vector commitment is useful to solve the problem of verifiable data outsourcing. Recently, Chen et al. [34], [35] figured out that the basic vector commitment scheme suffers from forward automatic update attack and backward substitution update at-tack. They also proposed a new framework for verifiable database with efficient update from vector commitment, which is not only public verifiable for dynamic outsourced data but also secure against the two attacks.

Group Signature with User Revocation

It presents the formal definition of group signatures with verifier-local revocation [27] as follows. It returns either valid or invalid. The latter response can mean either that σ is not a valid signature, or that the user who generated it has been revoked.

Systematization:

It provides the formal definition of our scheme according to the definition in [23], [24]. Then, we design the concrete scheme based on our definition.

New Framework

Consider the database DB as a set of tuple (x, m_x), where x is an index and m_x is the corresponding value. Informally, a public integrity auditing scheme with updates allows a resource-constrained client to outsource the storage of a very large database to a remote server. Later, the client can retrieve and update the database records stored in the server and publicly audit the integrity of the updated data.

A Concrete Scheme

In this section, we provide a concrete scheme from vector commitment [25] and verifier-local revocation group signature [27].

Setup(1^k, DB**)**

Query(P K, pp, aux, DB, i**)**

Verify(P K, i, τ **)**

Update(i, τ **)**

ProofUpdate(C, Λ_j, m'_i, i, U **)**

UserRevocation(P K, i, τ **)**

Supporting Ciphertext Database

In cloud storage outsourcing environment, the outsourced data is usually encrypted database, which is usually implicitly assumed in the exiting academic research. Actually, our scheme could support the auditing of database of both plaintext and cipher text database.

However, when the scheme needs to support multi-user data modification, while at the same time keeping the shared data encrypted, a shared secret key among group users will result in single point failure problem. It means that any group user (revoked or leave) leak the shared secret key will break the confidentiality guarantee of the data.

To overcome the above problem, we need to adopt a scheme, which could support group users data modification. Luckily, Wu et al. [26] designed an Asymmetric Group Key Agreement scheme (ASGKA). The scheme has a nice property that, instead of a common secret key, only a shared encryption key is negotiated in an ASGKA protocol. Also, in the scheme, the public key can be simultaneously used to verify signatures and encrypt messages while any signature can be used to decrypt ciphertext under this public key.

V. PROBABILISTIC DETECTION

Actually, the position binding property of vector com-mitment of the scheme allows the cloud storage server to prove the data item correctness of certain position. In the database, only y items of the database are incorrect.

VI. ANALYSIS OF PROPOSED SCHEME

Some basic tools have been used to construct our scheme. Thus we assume that the underlying building blocks are secure, which include the vector commitment, group signature, and asymmetric group key agreement scheme.

Security of Our Scheme

The security of the scheme is based on the strong Diffie-Hellman assumption and the Decision Linear assumption in bilinear groups as defined in Definition 1 and Definition 2. Thus, if we assume the two building blocks of our scheme is secure, then our scheme can be proven to be secure similar to [25]

Countability of Our Scheme.

Since the update counter t is a public parameter, given the proof with the counter t', the client will firstly compare it with the public latest counter. if t' = t, then the auditor

Traceability of Our Scheme.

The traceability of our scheme is based on the traceability of the adopted group signature. In the theorem 2 of reference [25], the authors provide the formal proof of the traceability of the group signature adopted. It means that if SDH is hard on (G_1,G_2), the group signature scheme is traceable.

VII. RELATED WORK

The scheme is based on polynomial authentication tags and adopts proxy tag update techniques, which makes their scheme support public checking and efficient user revocation. However, the authors do not consider the ciphertext store. Also, to make the scheme efficient, the data owner (the data owner's private key is not necessary) does not take part in the user revocation phase, where the cloud could conduct some malicious operation of user's data when it col-ludes with the revoked users.

VIII. REFERENCES

[1] Amazon. (2007) Amazon simple storage service (amazon s3). Amazon. [Online]. Available: http://aws.amazon.com/s3/

[2] Google. (2005) Google drive. Google. [Online]. Available:http://drive.google.com/

[3] Dropbox. (2007) A file-storage and sharing service. Dropbox.[Online]. Available: http://www.dropbox.com/

[4] Mozy. (2007) An online, data, and computer backup software.EMC. [Online]. Available: http://www.dropbox.com/

[5] Bitcasa. (2011) Inifinite storage. Bitcasa. [Online]. Available:http://www.bitcasa.com/

[6] Memopal. (2007) Online backup. Memopal. [Online].Available: http://www.memopal.com/

[7] M. A. et al., "Above the clouds: A berkeley view of cloud computing," *Tech. Rep. UCBEECS*, vol. 28, pp. 1–23, Feb. 2009.

[8] M. Rabin, "Efficient dispersal of information for security," *Journal of the ACM (JACM)*, vol. 36(2), pp. 335–348, Apr. 1989.

[9] J. G. et al. (2006) The expanding digital universe: A forecast of worldwide information growth through 2010. IDC. [Online]. Available: Whitepaper

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. of ACM CCS*, Virginia, USA, Oct. 2007, pp. 598–609.

[11] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of ACM CCS*, Virginia, USA, Oct. 2007, pp. 584–597.

[12] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in *Proc. of CCSW 2009*, llinois, USA, Nov. 2009, pp. 43–54.

[13] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in *Proc. of TCC 2009*, CA, USA, Mar. 2009, pp. 109–127.

[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Proofs of retrievability via hardness amplification," in *Proc. of ESORICS 2009*, Saint-Malo, France, Sep. 2009, pp. 355–370.

[15] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. of ACM CCS*, Illinois, USA, Nov. 2009, pp. 213–222.

[16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. of IEEE INFOCOM 2010*, CA, USA, Mar. 2010, pp. 525–533.

[17] J. Yuan and S. Yu, "Proofs of retrievability with public verifiability and constant communication cost in cloud," in *Proc. of International Workshop on Security in Cloud Computing*, Hangzhou, China, May 2013, pp.

AUTHOR's PROFILE

K . Suresh Babu is pursuing his M-Tech in Dept of CSE, Krishna Chaitanya Institute of Technology and Sciences, Markapur, Prakasam Dist, AP Affiliated to JNTUK University.

J. Mahalakshmi Pursuing Ph.D from Bharthar university Tamil nadu. She has 9 years of experience in Teaching. Currently working as Associate Professor in Dept of CSE , Krishna Chaitanya Institute of Technology & Sciences ,Markapur, Prakasam Dist, Affiliated by JNTUK University.