ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Security Enhancement in Cloud Computing with Group User Revocation

Aishwarya Shah[1], Pushkar Zagade[2], Ravindra Bachate[3], Shruti Yadav[4,]

Assistant Professor, Dept. of Computer Engineering, JSCOE, Hadapsar, Pune, India[3]

UG Student, Dept. of Computer Engineering, JSCOE, Hadapsar, Pune, India[1, 2, 4]

ABSTRACT: The enhancement of cloud computing make storage outsourcing become an exceeding trend, which results a secure data auditing as cool topic that emerge in research literature. Recently, some researches consider the problem of efficient and secure public data authentication inspection for shared dynamic data. However, these schemes are still not secure against the collusion and leakage of cloud storage server from unauthorized attacker and revoked group users during user revocation in cloud storage system. This paper focuses on auditing the integrity of shared data with dynamic groups in cloud. A new user can be added into the group. Also, an existing group member can be revoked by preserving privacy including backup of data using vector commitment and verifier-local revocation group signature. This scheme supports the public validation, efficient user revocation and also some good properties such as traceability, efficiency, confidently, countability. Finally, the security and experimental analysis show that our scheme is also secure and efficient. This scheme also supports avoid duplication of data which is one of important data compression techniques which is used for removing duplicate copies of repeating data, and have been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To support protection for the confidentiality of sensitive data the convergent encryption technique has been suggested to encrypt the data before outsourcing.

KEYWORDS:Public integrity auditing, dynamic data, group signature, vector commitment, cloud computing, confidentiality, De-duplication, authorized duplicate check, hybrid cloud.

.

I. INTRODUCTION

The improvements and enhancements in cloud computing motivates enterprises and also organizations to outsource their data to third party cloud service providers (CSP's) which will result in improvements in the data storage limitation of resource constrain local devices. In market, already some cloud storage services are available like simple storage service (S3) online data backup services of Amazon and software like Google Drive, Drop box, Mozy, Bitcasa and Memopal built for cloud application. In some cases cloud server sometime returns invalid results such as hardware/software failure, malicious attack and human maintenance. Security and privacy of cloud user's data should be protected by data integrity and accessibility. To overcome the security issues of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme are not sufficient for practical application. For achieving the integrity and availability of remote cloud storage, some various solutions and their different variants have been proposed. In these solutions, when a scheme supports modification of data, it is known as dynamic scheme, otherwise static one. A scheme is *publicly verifiable* that means the integrity check of data can be performed not only by data owners, but also by the third party auditor (TPA). However, the focus of the dynamic scheme is on the cases where only and only data owner could modify the data of cloud. Recently, the development of cloud computing emerged some applications where the services of cloud can be used as a collaboration platform. In these software development environments, one or more than one (multiple) users in a group need to share source code as well as they needs to access, compile, modify and run the source code share by user at any time. The new model of cooperation network in cloud provides the infeasibility of data for auditing the remote data, where only the data owner can update its data. It will result in terrific communication and computation to the data owner which causes the single point of data owner. To achieve multiple data operation, Wang et al. put forth data integrity based on ring signature. In the scheme, it does not consider the user revocation problem and the cost of auditing is linear to the data size and group size. To

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

further raise up the previous scheme and support group user revocation, Wang et al. proposed a scheme based on proxy re-signatures. However, this scheme assumes that authenticated and private channels exist between the pair of entities and there is no collusion among them. Also, cost of auditing the scheme is linear to the size of the group. Another attempt to improve the previous scheme and make the scheme scalable, efficient and collusion resistant, Yuan and Yu designed a dynamic public integrity auditing scheme with group user revocation. However, in their scheme, the authors do not consider the secrecy of data among the group users. That means, their scheme could efficiently support plain text of data update and integrity auditing, while not ciphertext data. In their scheme, if data owner shares group key among the users of group, revocation of any group user allow the group users to update their shared key. Also, the owner of the data does not take part in the user revocation phase, where the user revocation phase is itself conducted by the cloud. In this case, the malicious cloud server will result in collusion of revoked user and the cloud server where the cloud server could update data number of times as designed and provide a legal data finally. Due to above mentioned deficiency; we propose a construction which includes data encryption and decryption during the data modification processing, secure and efficient user revocation and also removal of redundant data. Here, vector commitment scheme will be applied over the database. Then we apply the Asymmetric Group Key Agreement (AGKA) to support ciphertext database update among group users and we also use group signatures for efficient group user revocation. The user in the group will be able to encrypt or decrypt a message from any other group users when the group users use the AGKA protocol to encrypt or decrypt the share database. The collusion of the cloud and revoked group users will be prevented by the group signature.

Each file uploaded to the cloud is also requires a set of privileges to specify which kind of users can access the files and which users is allowed to perform the duplicate check and. Before submitting this duplicate check request for some file, the user needs to take his own privileges and also files as inputs. The user is able to find a duplicate for this file if and only if there is a copy of this file and matched privileges stored in cloud. For example, in a company, many different privileges will be assigned to the employees. The data will be moved to the storage server provider (SCSP) in the public cloud with specified privileges and the de-duplication technique will be applied to store only one copy of the same file in order to save cost and efficient management. Because of privacy consideration, some files will be encrypted and will also be allowed the duplicate check by employees with specified privileges to realize the access control. Traditional de-duplication systems based on convergent encryption, although providing confidentiality to some extent, do not support the duplicate check with differential privileges. In other words, in the de-duplication based on convergent encryption technique no differential privileges have been considered. If we want to realize both de-duplication and differential authorization duplicate check at the same time, it seems to be contradicted.

II. LITERATURE SURVEY

Boyang Wang, Baochun Li and Hui Li are the members of IEEE explore the concept of "Oruta: Privacy-Preserving Public Auditing for Shared data in the Cloud" [4] in 2014. It shows that cloud provide services like data storage as well as data sharing across multiple users .In this proposed system public auditing of shared data which is stored in the cloud by using privacy preserving mechanism. This paper explains the concept of group signature which computes the verification information required for integrity auditing of shared data.. According to this mechanism, the identity of signature in each block in shared data remains private from a third party auditor (TPA) which can publicly verify shared data integrity without accessing whole data. This mechanism supports batch auditing and also responsible for auditing multiple shared data in just single auditing task.

B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912[9] represents that users can easily modify and share data as a group with the help of data storage and sharing services in the cloud. Shared data integrity is verified publicly. On all the blocks in shared data, users in the group need to compute signatures. As the data modifications are performed, different blocks in shared data are generally signed by different users. For security reasons, once a user is left from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The existing users download the corresponding part of the shared data. The existing users can also re-sign it during user revocation by using the straightforward method. This becomes inefficient because of the large size of shared data in the cloud. In this paper, we propose a public auditing mechanism for the integrity of shared

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

data with efficient user revocation. The cloud is allowed to re-sign blocks on behalf of existing users during user revocation by utilizing the idea of proxy re-signatures. Hence, the existing users do not need to download and re-sign blocks by themselves. In addition to this, even if some part of shared data has been re-signed by the cloud without retrieving the entire data from the cloud, a public verifier is able to audit the integrity of shared data. Moreover, batch auditing is also supported in our mechanism. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.[8] represents the study of a new primitive called Vector Commitment. Informally, Vector Commitment allows committing to an ordered sequence of values in such a way that one can later open the commitment at specific positions. For security, Vector Commitments are required to satisfy a notion that we call position binding which states which are adversary should not be able to open a commitment to two different values at the same position. We show two realizations of VCs. These applications include: Verifiable Databases with Efficient Updates, Updatable Zero-Knowledge Databases, and Universal Dynamic Accumulators.

III. PROPOSED SYSTEM

In this paper, we study the problem of Public Authentication Inspection for Shared Dynamic Cloud Data with Group User Revocation Including Backup And Data Storage Our contributions are:

1) For cipher text database, we explore on the efficient and secure shared data integrity auditing for multi-user operation.
2) We intend an efficient data auditing scheme along with new features such as countability by incorporating the vector commitment primitives, traceability, asymmetric group key agreement and group signature.
3) The analysis results show that our scheme is secure and efficient as we provide the efficiency and security analysis of our 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 de-duplication constructions and this authorized duplicate check scheme comparatively incurs minimum overhead than normal operations.
5) The below diagram 3.1 shows cloud storage model which has been referred from "Public integrity auditing for shared dynamic cloud data with group user revocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.[1]

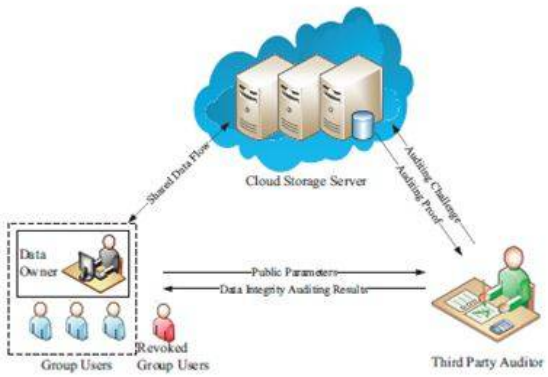


Fig. 3.1

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

3.1Vector Commitment

We have referred and studied this algorithm from T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.[1] In cryptography, commitment is a fundamental primitive and it plays an important role in security protocols such as voting, identification, etc. The committed message's information should not be revealed and it is given by the hiding property of the commitment. The binding property requires that the committing mechanism should not allow a sender to change his/her mind about the committed message.

Vector Commitment satisfies position binding that an adversary should not be able to open a commitment to two different values at the same position, and the Vector Commitment is concise, which means that the size of the commitment string and its openings have to be independent of the vector length.

Concept 1: A vector commitment is a collection of six polynomial-time algorithms *(VC.KeyGen, VC.Com, VC.Open, VC.Ver, VC.Update, VC.ProofUpdate)* such that: *VC.KeyGen(*1k*, q).* Given the security parameter k and the size q of the committed vector (with q =poly(k)), the key generation outputs some public parameters pp. *VC.Compp(m1, ...,mq).* On input a sequence of q messages *m1, ...,mq*∈*M*(M is the message space) and the public parameters pp, the committing algorithm outputs a commitment string C and an auxiliary information aux. *VC.Openpp(m, i, aux).* To produce a proof i,this algorithm is run by the committee where m is the ith committed message. In particular, notice that in the case when some updates have occurred the auxiliary information aux can include the update information produced by these updates.

*VC.Verpp(C,m, i,*Λ*I).*The verification algorithm accepts (i.e., it outputs 1) only if _i is a valid proof that C was created to a sequence m1, ... , mq such that m = mi. *VC. Updatepp(C,m,m′, i).* This algorithm is run by the committee who produces C and wants to update it by changing the i-th message to m′. The algorithm takes as input the old message m, the new message m′ and the position i. It outputs a new commitment C' together with an update information U. *VC. ProofUpdatepp(C,_j ,m′, i,U).* This algorithm can be run by any user who holds a proof Λj for some message at position j w.r.t. C, and it allows the user to compute an updated proof Λj (and the updated commitment C′) such that Λj will be valid with regard to C′ which contains m′ as the new message at position i. Basically, the value U contains the update information which is needed to compute such values. The problem of verifiable data outsourcing is solved by the primitive of verifiable database with efficient update based on vector commitment. Recently, it was figured that the basic vector commitment scheme includes issues like forward automatic update attack and backward substitution update attack. To avoid these attacks and also to provide public verifiable for dynamic outsourced data, a new framework for verifiable database with efficient update from vector commitment was proposed.

Group Signature with User Revocation

T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user evocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.[1] describes group signature with User Revocation as follows.

Concept 2: The signature scheme of authorized group user is a collection of three polynomial-time algorithms, which are VLR.KeyGen, VLR.Sign, and VLR.Verify behave as follows: *VLR.KeyGen(n).* This randomized algorithm takes n parameter as input where n represent number of group user. Its output result in group public key(gpk), an n-element vector of user keys *gsk = (gsk(1),gsk(2),..,gsk(n)),* n-element vector of group user revocation tokens *grt=(grt(1),grt(2),…,grt(n)). VLR.Sign(gpk, gsk[i], M).* This randomized algorithm takes group public key(gpk), a private key(gsk[i]) and a message M ϵ {0,1}* , and return user signature σ. VLR.Verify(*gpk, RL, σ ,M*). The randomized verification algorithm takes group public key gpk, a set of revocation tokens RL, and a purported signature σ on a message M input as a parameter. It returns either valid or invalid result. It represent that σ is not a valid signature, or the user has been revoked who has generated it.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

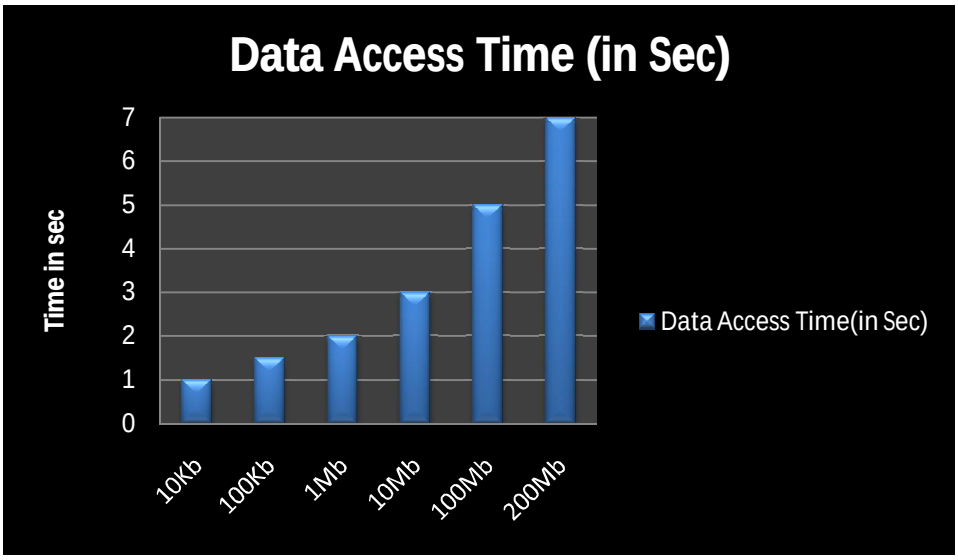
IV. MATHEMATICAL MODEL

ψ(g2) = g1, and e : G1 × G2 → GT is a bilinear map with the following properties:

1. Computability: there exits an efficiently computable algorithm for computing mape;
2. Bilinearity: for all u ∈ G1, v ∈ G2 and a, b ∈Zp, e(ua, vb) = e(u, v)ab;
3. Non-degeneracy: e(g1, g2) ≠1.

Framework:
DB = (i,mi) for $1 \leq i \leq q$
key generation of verifier-local revocation to obtain the
user keys and revocations *(gsk, grt)* ← *VLR.KeyGen(1k, n), where gsk* =(gsk[1], gsk[2]...gsk[n]) and an n element vector of user revocation tokens *grt.*
User Revocation (PK, i, τ):
VLR.Verify(gpk, RL, σ,M), M = C(t − 1),Ct,

V. RESULT AND GRAPH



In this system, we have provided a scheme of auditing the integrity of the shared and dynamic cloud data along with group user revocation. The auditing of the data integrity is secure and reliable. In this paper, the concept of authorized data deduplication was proposed to achieve the data security by including differential privileges of users in the duplicate check. Auditing the remote data integrity is achieved by using vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation. By combining the above three primitives, outsourcing ciphertext database to remote cloud is possible. This paper involves the successful implementation of data backup and efficient storage for maintaining the confidentiality of shared data. We have provided security analysis in our scheme which proves that our scheme provides confidentiality of shared data for different group users. Also, performance analysis proves our scheme to be efficient in different phases as compared to other relevant schemes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

REFERENCES

1. T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015
2. Hugo E. Camacho, J. Alfredo Brambila, Alfredo Peña, José M. Vargas, "A cloud environment for backup and data storage," in Engineering Information Technology, Polytechnic University of Altamira, Altamira Tamaulipas, México
3. Jin Li, Yan Kit Li, X. Chen, Patrick P. C. Lee, Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorize De duplication," in Proc. of IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM VOL:PP NO:99 YEAR 2014
4. Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" in Proc. Of IEEE TRANSACTIONS ON XXXXXX, VOL. X, NO. X, XXXX 201X
5. C. Wang Student Member, IEEE, Sherman S.-M. Chow, Q. Wang, Student Member, IEEE, K. Ren, Member, IEEE, and W. Lou, Member, IEEE , "Privacy Preserving Public Auditing for Secure Cloud Storage".
6. B. Wang, B. Li, Member, IEEE, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud" in Proc. Of IEEE TRANSACTIONS ON XXXXXX, VOL. X, NO. X, XXXX 201X
7. 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.
8. D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.
9. B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912