IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation

Mr. Mangesh Nagarkar[1], Prof. Patole R.G[2]

Department of Computer Engineering, G.H. Raisoni College of Engineering and Management, Ahmednagar[1]

Department of Information Technology, G. H. Raisoni College of Engineering and Technology, Wagholi[2]

Abstract: The advent of the cloud computing makes storage outsourcing become a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research consider the problem of secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation in practical cloud storage system. In this paper, we figure out 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. We design a concrete scheme based on the our scheme definition. Our 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. Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

Index Terms: Public integrity auditing, dynamic data, victor commitment, group signature, cloud computing.

1. 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 constrain 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, human 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.

The formers are not practical because a recent IDC report suggests that data-generation is outpacing storage availability [9]. The later protocols ensure the availability of data when a quorum of repositories, such as k-out-of-n of shared data, is given. However, they do not provide assurances about the availability of each repositories, which will limit the assurance that the protocols can provide to relying parties.

For providing the integrity and availability of remote 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. However, the dynamic schemes above focus on the cases where there is a data owner and only the data owner could modify the data.

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 remote data auditing schemes become infeasible, where only the data owner can update its data. Obviously, trivially extending a scheme with an online data owner to update the data for a group is inappropriate for the data owner. It will cause tremendous communication and computation overhead to data owner, which will result in the single point of data owner. To support multiple user data operation, Wang et al. [22] proposed a 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. However, the scheme assumed that the private and authenticated channels exist between each pare of entities and there is no collusion among them. Also, the auditing cost of the scheme is linear to the group size. Another attempt to improve the previous scheme and make the scheme efficient, scalable and collusion resistant is Yuan and Yu [24], who designed a dynamic public integrity auditing scheme with group user

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

revocation. The authors designed polynomial authentication tags and adopt proxy tag update techniques in their scheme, which make their scheme support public checking and efficient user revocation. However, in their scheme, the authors do not consider the data secrecy of group users. It means that, their scheme could efficiently support plaintext data update and integrity auditing, while not ciphertext data. In their scheme, if the data owner trivially shares a group key among the group users, the defection or revocation any group user will force the group users to update their shared key. Also, the data owner does not take part in the user revocation phase, where the cloud itself could conduct the user revocation phase. In this case, the collusion of revoked user and the cloud server will give chance to malicious cloud server where the cloud server could update the data as many time as designed and provide a legal data finally. To the best of our knowledge, there is still no solution for the above problem in public integrity auditing with group user modification.

The deficiency of above schemes motivates us to explore how to design an efficient and reliable scheme, while achieving secure group user revocation. To the end, we propose a construction which not only supports group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation. Our idea is to apply vector commitment scheme [25] over the database. Then we leverage the Asymmetric Group Key Agreement (AGKA) [26] and group signatures [27] to support ciphertext data base update among group users and efficient group user revocation respectively. Specifically, the group user uses the AGKA protocol to encrypt/decrypt the share database, which will guarantee that a user in the group will be able to encrypt/decrypt a message from any other group users. The group signature will prevent the collusion of cloud and revoked group users, where the data owner will take part in the user revocation phase and the cloud could not revoke the data that last modified by the revoked user.

1.1 Our Contribution

In this paper, we further study the problem of construing public integrity auditing for shared dynamic data with group user revocation. Our contributions are three folds:

1) We explore on the secure and efficient shared data integrate auditing for multi-user operation for ciphertext database.
2) By incorporating the primitives of victor commitment, asymmetric group key agreement and group signature, we propose an efficient data auditing scheme while at the same time providing some new features, such as traceability and countability.
3) We provide the security and efficiency analysis of our scheme, and the analysis results show that our scheme is secure and efficient.

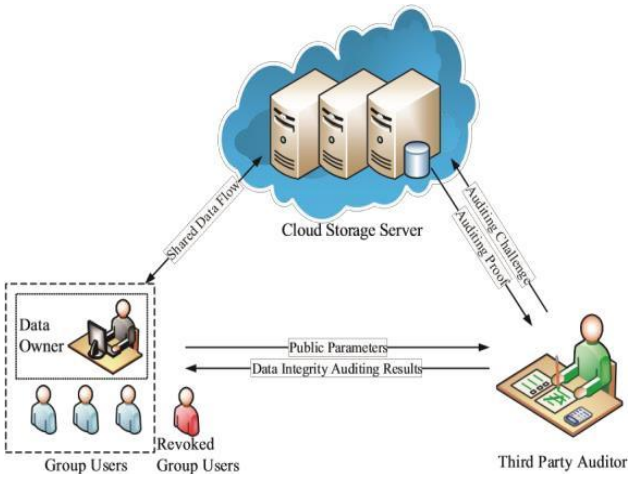

Figure 1 the cloud storage model

1.2 Organization

The rest of this paper is organized as follows: In section 2, we describe the problem formulation. In section 3, we present the used preliminaries. Then, we provide the detail of our scheme in section 4. We conduct the security and efficiency analysis in section 5 and section 6 and leave the related works in section 7. Finally, we show our conclusion in section 8.

2. PROBLEM FORMULATION

In this section, we first describe the cloud storage model of our system. Then, we provide the threat model considered and security goals we want to achieve.

2.1 Cloud Storage Model

In the cloud storage model as shown in Figure 1, 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. The cloud storage server is semi-trusted, who provides data storage services for the group users. 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 our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users. The TPA could efficiently verify the integrity of the Data last modified Data last modified legitimate data

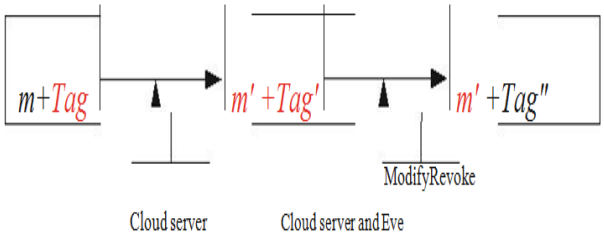

Figure 2. Security problem of server proxy group user revocation

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

authorized by user Eve by cloud server by the data owner data stored in the cloud storage server, even the data is frequently updated by the group users. 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.

2.2 Threat Model and Security Goals

Our 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.

Actually, in cloud environment, we assume that the cloud storage server is semi-trusted. Thus, it is reasonable that a revoked user will collude with the cloud server and share its secret group key to the cloud storage server. In this case, although the server proxy group user revocation way [24] brings much communication and computation cost saving, it will make the scheme insecure against a malicious cloud storage server who can get the secret key of revoked users during the user revocation phase. Thus, a malicious cloud server will be able to make data m, last modified by a user that needed to be revoked, into a malicious data m'. In the user revocation process, the cloud could make the malicious data m' become valid. To overcome the problems above, we aim to achieve the following security goals in our paper:

1) **Security.** A scheme is secure if for any database and any probabilistic polynomial time adversary, the adversary can not convince a verifier to accept an invalid output.
2) **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 ciphertext if the scheme could efficiently support encrypted database.
3) **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.
4) **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.
5) **Traceability**. We require that the data owner is able to trace the last user who update the data (data item), when the data is generated by the generation algorithm and every signature generated by the user is valid.

3. PRELIMINARIES

Our scheme makes use of bilinear groups. The security of the scheme depends on the Strong DiffieHellman assumption and the Decision Linear assumption. In this section, we review the definitions of bilinear groups and the complexity assumption.

3.1 Bilinear Groups

We review a few concepts related to bilinear maps, which follow the notation of [28]. Let G1 and G2 be two multiplicative cyclic groups of prime order p, g1 is a generator of G1 and g2 is a generator of G2. ψ is an efficiently computable isomorphism from G2 to G1 with $\psi(g2) = g1$, and $e : G1 \times G2 \rightarrow GT$ is a bilinear map with the following properties:

1) **Computability:** there exits an efficiently computable algorithm for computing map e;
2) **Bilinearity:** for all $u \in G1$, $v \in G2$ and $a,b \in Zp$, $e(u^a,v^b) = e(u,v)^{ab}$;
3) **Non-degeneracy:** $e(g1,g2) \neq 1$.

3.2 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. We describe these problems as follows.

Definition 1. q-Strong Diffie-Hellman problem. Let G1, G2 be cyclic group of prime order p, where possibly G1 = G2. Let g1 be a generator of G1 and g2 be a generator of G2. Given a $(q + 2) - tuple(g1, g2, g_2^{\gamma}, g_2^{(\gamma^2)}, ..., g_2^{(\gamma^q)})$ as input, output a pair $(g_1^{1/(\gamma+x)}, x)$ where $x \in Z^*p$.
The assumption could be used to construct short signature scheme without random oracles [29]. The assumption has properties similar to the Strong-RSA assumption [30] and the properties are adopted for building short group signature in our scheme.

Definition 2. Decision Linear problem. Let g1 be a generator of G1, and G1 be a cyclic group of prime order p. Given u, v, h, u^a, u^b,$u^c \in G1$ as input, output yes if a + b = c and no otherwise.
Boneh et al. [31] introduced the Decision Linear assumption and they proved that the problem is intractable in generic bilinear groups.

Definition 3. Square Computational Diffie-Hellman (Square-CDH) problem. With $g \in G1$ as above, given (g,g^x) for $x \in_R Zp$ as input, output g^{x2}.
It has been proved that the Square-CDH assumption is equivalent to the classical CDH assumption [32], [33].

3.3 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

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

hiding property of commitment requires that it should not reveal information of the committed message, and the binding property requires that the committing mechanism should not allow a sender to change his/her mind about the committed message.

Recently, Catalano and Fiore [25] put forward a new primitive called Vector Commitment. 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. We provide the formal definition of Vector Commitment [25] as follows.

Definition 4. (Vector Commitment) A vector commitment scheme is a collection of six polynomial-time algorithms (VC.KeyGen, VC.Com, VC.Open, VC.Ver, VC.Update, VC.ProofUpdate) such that:

VC.KeyGen(1^k,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). This algorithm is run by the committer to produce a proof i that m is the i-th 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,Λi). The verification algorithm accepts (i.e., it outputs 1) only if Λi 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 committer 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,Λj,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 Λ′j (and the updated commitment C′) such that Λ′j 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 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 attack. 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. The solution in their scheme is easy to apply in our scheme, which will overcome the attacks they figured out in our scheme.

3.4 Group Signature with User Revocation

We present the formal definition of group signatures with verifier-local revocation [27] as follows.

Definition 5. A verifier-local group signature scheme is a collection of three polynomial-time algorithms

(VLR.KeyGen, VLR.Sign, VLR.Verify), which behaves as follows:

VLR.KeyGen(n). This randomized algorithm takes as input a parameter n, the number of members of the group. It outputs a group public key gpk, an n-element vector of user keys gsk =

(gsk[1],gsk[2],...,gsk[n]), and an n-element vector of user revocation tokens grt, similarly indexed.

VLR.Sign(gpk,gsk[i],M). This randomized algorithm takes as input the group public key gpk, a private key gsk[i], and a message M ∈ {0,1}*, and returns a signature σ.

VLR.Verify(gpk,RL,σ,M). The verification algorithm takes as input the group public key gpk, a set of revocation tokens RL (whose elements form a subset of the elements of grt), and a purported signature σ on a message M. 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.

4. SCHEME CONSTRUCTION

In this section, we provide the formal definition of our scheme according to the definition in [23], [24]. Then, we design the concrete scheme based on our definition.

4.1 New Framework

We consider the database DB as a set of tuple (x,mx), where x is an index and mx 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.

According to previous researches, the proposed framework of our public integrity auditing for shared dynamic cloud data with secure group user revocation is given as follows:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

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

Let the database be DB = (i,mi) for 1 ≤ i ≤ q and the database is shared by a group of n users with only one data owner.

1) The data owner run the key generation algorithm of vector commitment to obtain the public parameters pp

← VC.KeyGen(1^k,q).

2) Run the key generation of verifier-local revocation to obtain the user keys and revocations (**gsk**, **grt**) ←

VLR.KeyGen(1^k,n), where **gsk** = (gsk[1],gsk[2]...gsk[n]) and an n-element vector of user revocation tokens **grt**.

3) Run the computing algorithm to compute commitment and auxiliary information (C, aux) ← VC.Compp(c1,...,cq). Let the current database modifier be group user s(0 ≤ s ≤ n − 1), and

(gsk[s],gpk) be the secret/public key pair of the group user. Let $C^t = VC.Com_{\mathsf{PP}}(c_1^t, ..., c_q^t)$ be the commitment on the latest database vector, where t is a counter with 0 as its initial value.

4) Run the signing algorithm over the commitment C. Specially, for the t-th time the group user s(0 ≤ s ≤ n − 1), whose secret key is gsk[s], compute and output

a signature σ^t ← VLR.Sign(gpk,gsk[s],{C(t − 1),C^t,t}). Then, sends the signature σ^t to the cloud storage server. If σ^t is valid, then the server computes C(t) = $\sigma^t \cdot C^t$. Also, the cloud storage server adds the
information of Σ(t) = (C(t − 1),C^t,t,σ^t) to aux.

5) Finally, set public key parameter
PK = (pp,gpk,C(t − 1),C(t)).

Query(PK, PP, aux,DB,i**):**

1) A group user run the opening algorithm to compute a proof Λi ← VC.Openpp(ci,i, aux), where Λi is the proof of the i-th committed message and return τ = (ci,Λi,Σ(t)).

Verify(PK,RL,i,τ**):**
1) Parse τ = (ci,Λi,Σ(t)). If the signature is valid after running the algorithm VLR.Verify(gpk,RL,Σ(T)). Then, run the verification algorithm of vector commitment {0,1} ← VC.Verpp(C(t),σ^t,ci,i,Λi). The algorithm accepts when it output 1, which means that Λi is a valid proof that C^t was created by a sequence c1,...cq, such that c = ci. Otherwise, return an error ⊥.

Update(i,τ**):**

1) A group user first queries and verifies the database to make sure the current database is valid. More precisely, the group user obtain τ ←**Query(**PK, PP, aux,DB,i**)** and check that **Verify**(PK,i,τ) = mi.

2) Run the update algorithm over the new data and output the updated commitment and the update information

(C′,U) ← VC.Update(C,m,m′,i).

ProofUpdate(C,Λj,c′i,i,U**):**

1) A third part auditor can first verify that, compared with the stored counter t, the latest counter equals t + 1. Then, run the proof of update algorithm of vector commitment to compute an update proof Λj ←

VC.ProofUpdatepp(C,Λj,m′i,i,U) for the message at position j, such that Λj is valid with respect to C′ which contains m′ as the new message at position j. Here, U = (m,m′,i) is the update information.

2) Verify the commitment C′, and its corresponding proof Λi is also valid over message m′i.

UserRevocation(PK,i,τ**):**

1) The third part auditor can run the verification algorithm of verifier-local revocation and return either valid or invalid {0,1} ← VLR.Verify(gpk,RL,σ,M). Here, RL are a set of revocation tokens.

4.2 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**):**
Let k be a security parameter and DB = (i,mi) for 1 ≤ i ≤ q be the database. The database DB = (i,mi) is shared by a group of n users with only one data owner. The message space is M = Zp.

1) Let G,GT be two bilinear groups of prime order p equipped with a bilinear map e : G × G → GT, and g be a random generator of G.

Randomly choose z1,...,zq ←R Zp. For all i = 1,...,q, set hi = g^{zi}. For all i,j = 1,...,q,i 6= j, set hi,j = g^{zizj}. The data owner runs the key generation algorithm of vector commitment VC.KeyGen(1^k,q) to obtain the public parameters PP = (p, q, G, GT, H, g, ({hi})i∈[q], {hi,j} i,j∈[q],i=6 j) and the message space M= Zp. By using a collision resistant hash function H: {0,1}* → Zp, our scheme can be easily extended to support arbitrary messages in {0,1}*.

2) Run the key generation of verifier-local revocation VLR.KeyGen(1^k,n). Let G1, G2 be cyclic group of prime order p, and g1 be a generator of G1 and g2 be a generator of G2. Consider bilinear groups (G1,G2) with isomorphism ψ, where g1 ← ψ(g2). Select γ ←R Z* p and set $w = g_2^{\gamma}$. For each user, generate an SDH tuple (Ai,xi) by selecting xi ←R Z* p such that γ+xi 6= 0, and setting

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

$A_i \leftarrow g_1^{1/(\gamma+x_i)}$. Then, set the group public key gpk = (g1,g2,w). The private key is a tuple gsk[i] = (Ai,xi).

The revocation token corresponding to a user's secret key is grt[i] = Ai. Finally, the algorithm outputs (gpk, **gsk**, **grk**). γ is only known to the private-key issuer (the data owner).

3) Run the computing algorithm VC.Compp(m1,...,mq) to compute commitment $C = h_1^{m_1}, h_2^{m_2}, ..., h_q{}^{q}$ m and auxiliary information aux = (m1,...,mq).

4) Employ hash functions H0 and H as random oracles, with respective ranges $G^2 2$ and Zp. For the t-th time data updating, run the signing algorithm

VLR.Sign(gpk,gsk[i],{C(t − 1),C^t,t}) over the commitment. Assume that the input message is {C(t −

1),C^t,t} ∈ {0,1}*. Then, pick a random nonce r ←R Zp and obtain generators (u,ˆ vˆ) ← H0(gpk,{C(t −

1),C^t,t},r) ∈ $G^2 2$ and compute their images in G1 with u ← ψ(uˆ) and v ← ψ(vˆ) . Select an exponent α ←R Zp

and compute T1 ← u^α and T2 ← Aiv^α. Set δ ← xiα ∈ Zp. Pick blinding values rα, rx, and rδ ←R Zp. Compute helper values R1 ← u^{rα}, R2 ← e(T2,g2)^{rx} · e(v,w)$^{−rα}$ · e(v,g2)$^{−rδ}$ and $R_3 \leftarrow T_1^{r_x} \cdot u^{-r_\delta}$.

Compute a challenge value c ← H(gpk,(C(t−1),C ,t),r,T1,T2,R1,R2,R3) ∈ Zp using H. Compute sα = rα + cα, sx = rx + cxi, and sδ = rδ + cδ ∈ Zp. Finally, output a signature σ^t ← (r,T1,T2,c,sα,sx,sδ). Then, sends the signature σ^t to the cloud storage server. If σ^t is valid, then the server computes C(t) = σ^t · C^t. Also, the cloud storage server adds the information of Σ(t) = (C(t − 1),C^t,t,σ^t) to aux. 5) Set public key parameter PK = (pp,gpk,C(t −1),C(t)).

Query(PK, pp, aux,DB,i**):**

1) We assume that the current public key is PK = (PP,gpk,C(t − 1),C(t)). A user runs the opening algorithm VC.Open $_{pp}(c_i^t, i, \text{aux})$ to compute a proof $\Lambda_i^t = \prod_{j-1,j\neq i}^{q} h_{i,j}^{m_j} = (\prod_{j=1,j\neq i}^{q} h_j^{m_j})^{z_i}$ of the i-th committed message and return τ = (m^{t}i,Λ^{t}i,Σ(t)).

Verify(PK,i,τ**):**

1) On input a group public key gpk, a purported signature σ^t, and the message {C(t − 1),C^t,t}, the auditor first verify whether the signature is valid.

2) If τ = (m^{t}i,Λi,Σ(t)), run the verification algorithm of vector commitment VC.Verpp(Ci^t,c^{t}i,i,Λ^{t}i) to verify that the equation $e(C^t/h_i^{m_i^t}, h_2) \stackrel{?}{=} e(\Lambda_i^t, g)$ holds. The algorithm accepts when it outputs 1, which means that Λ^{t}i is a valid proof that C^t was created to a sequence m1,...mq, such that m = mi.

Update(i,τ**):**

1) A group user first queries and verifies the database to make sure the current database is valid.

2) If the user wanted to update mi to m′i, the user runs the update algorithm VC.Update(C,m,m′,i) and outputs the updated commitment C′ = C · hi$^{m'-m}$ and the updated information U = (m,m′,i).

ProofUpdate(C,Λj,m′i,i,U**):**

1) The third part auditor can run the proof of update algorithm of vector commitment to compute an update proof Λj ← VC.ProofUpdatepp(C,Λj,m′,i,U) for the message at position j, such that Λj is valid with respect to C′ which contains m′ as the new message at position j.

2) For the auditor who owns a proof Λj, the auditor uses the update information U = (m,m′,i) to generate the proof of update. If i 6= j,

compute $C' = C \cdot h_{i'}^{m'-m}$

the updated commitment and the updated proof is Λ′j = Λj · (hi$^{m'-m}$) $\Lambda_j \cdot h_{j,i}^{m'-m}$; If $i = j$,zj = , compute the updated commitment C′ = C·hi$^{m'-m}$ while do not change the proof Λi. Verify the commitment C′ and its corresponding proof Λi is also valid over message m′i.

UserRevocation(PK,i,τ**):**

1) To verify the validity of the signature, the auditor need to conduct the signature check. The third part auditor runs the verification algorithm of verifier-local revocation VLR.Verify(gpk,RL,σ,M), M = C(t − 1),C^t,t. More precisely, compute uˆ and vˆ and their image u ← ψ(uˆ) and v← ψ(vˆ) in G1. Derive R˜1 ← usα/T1c, R˜2 ← e(T2,g2)sx · e(v,w)$^{−sα}$ · e(v,g2)$^{−sδ}$ · (e(T2,w)/e(g1,g2))^c and

$\tilde{R_3} \leftarrow T_1^{s_x} \cdot u^{-s_\delta}$. Check the challenge that c =$^?$ H(gpk,(C(t − 1),C^t,t),r,T1,T2,R˜1,R˜2,R˜3) and return either valid or invalid. Then, conduct the revocation check.

2) For each element A ∈ RL, check whether A is encoded in (T1,T2) by checking if e(T2/A,uˆ) $^{=?}$ e(T1,vˆ). If no element of RL is encoded in (T1,T2), the signer of σ has not been revoked. Here, RL is a set of revocation tokens.

4.3 Supporting Ciphertext Database

In cloud storage outsourcing environment, the outsourced data is usually encrypted database, which is usually

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

implicitly assumed in the exiting academic research. Actually, our scheme could support the auditing of database of both plaintext and ciphertext database. However, it is not straightforward to extend a scheme to support encrypted database.

In order to achieve the confidentiality of the data record mx, the client can use his/her secret key to encrypt each mx using a encryption scheme. When there is only one user (data owner) in the group, the user only needs to choose a random secret key and encrypt the data using a secure symmetric encryption scheme. 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. Using the bilinear pairings, the authors instantiate a one-round ASGKA protocol tightly reduced to the decision Bilinear Diffie-Hellman Exponentiation (BDHE) assumption in the standard model. Thus, according to the ASGKA protocol, we consider the case of encrypted database (x,cx), where x is an index and cx is the corresponding cipher value.

We provide the detailed changes upon our scheme to support encrypted database.

1) In the **Setup** phase, the scheme has to run the key agreement of ASGKA for the group users. Then, the database DB = (i,mi) is encrypted by the group key gpk of data owner. Finally, the stored database is a ciphertext database DB = (i,ci).

2) In the second step of the **Update** phase, a group user firstly decrypts the record ci using the ASGKA secret key gsk[∗] to get plaintext database DB = (i,mi). Then, update the data to m′i, and later encrypt the data with the public key gpk of ASGKA scheme to get the new encrypted database DB = (i,c′i).

4.4 Probabilistic Detection

Actually, the position binding property of vector commitment of the scheme allows the cloud storage server to prove the data item correctness of certain position. Ateniese et. al. [10] figured out that the sampling ability greatly reduces the overhead on the server and provides high detection probability of server misbehavior. Then, among the q data items, we assume that the third part auditor randomly select x items out of the q-block item database as the target item. In the database, only y items of the database are incorrect. Then, if x, y and q satisfy the specific relationship, the third part auditor could provide a high possession detection ability over the database. The result is interesting that when y is a fraction of the total item number q, the detection probability of server misbehavior is a constant amount of item. For example, if y = 1% of q, then the third part auditor asks for 460 blocks and 300 blocks in order to achieve the detection probability of at least 99% and 95%, respectively.

5. CONCLUSION

The primitive of verifiable database with efficient updates is an important way to solve the problem of verifiable outsourcing of storage. We propose a scheme to realize efficient and secure data integrity auditing for share dynamic data with multi-user modification. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data. Beside the public data auditing, the combining of the three primitive enable our scheme to outsource ciphertext database to remote cloud and support secure group users revocation to shared dynamic data. We provide security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users. Also, the performance analysis shows that, compared with its relevant schemes, our scheme is also efficient in different phases.

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. 19–26.
[18] E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Proc. of ACM CCS 2013, Berlin, Germany, Nov. 2013, pp. 325–336.
[19] Cloud9. (2011) Your development environment, in the cloud. Cloud9. [Online]. Available: https://c9.io/
[20] Codeanywhere. (2011) Online code editor. Codeanywhere. [Online]. Available: https://codeanywhere.net/
[21] eXo Cloud IDE. (2002) Online code editor. Cloud IDE. [Online]. Available: https://codenvy.com/
[22] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. of IEEE CLOUD 2012, Hawaii, USA, Jun. 2012, pp. 295–302.
[23] 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.
[24] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121–2129.
[25] D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.
[26] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in Proc. of EUROCRYPT 2009, Cologne, Germany, Apr. 2009, pp. 153–170.
[27] D. Boneh and H. Shacham, "Group signatures with verifierlocal revocation," in Proc. of ACM CCS, DC, USA, Oct. 2004, pp. 168– 177.
[28] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proc. of Asiacrypt 2001, Gold Coast, Australia, Dec. 2001, pp. 514–532.
[29] D. Boneh and X. Boyen, "Collision-free accumulators and failstop signature schemes without trees," in Proc. of EUROCRYPT 2004, Interlaken, Switzerland, May 2004, pp. 56–73.
[30] N. Baric and B. Pfitzman, "Collision-free accumulators and fail-stop signature schemes without trees," in Proc. of EUROCRYPT 1997, Konstanz, Germany, May 1997, pp. 480–494.
[31] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. of CRYPTO 2004, CA, USA, Aug. 2004, pp. 41–55.
[32] U. M. Maurer and S. Wolf, "Diffie-hellman oracles," in Proc. of CRYPTO 1996, CA, USA, Aug. 1996, pp. 268–282.
[33] F. Bao, R. Deng, and H. Zhu, "Variations of diffie-hellman proble," in Information and Communications Security, Huhehaote, China, Oct. 2003, pp. 301–312.
[34] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," in Proc. of ESORICS 2014, Wroclaw, Poland, Sep. 2014, pp. 148–162.
[35] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," to appear in IEEE Transactions on Dependable and Secure Computing, Accepted.
[36] B. Lynn. (2006) The pairing-based cryptography library. [Online]. Available: http://crypto.stanford.edu/pbc/
[37] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Proc. of CRYPTO 2010, CA, USA, Sep. 2010, pp. 465– 482.
[38] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. of ACM STOC 2009, Washington DC, USA, May 2009, pp. 169–178.
[39] C. Gentry and S. Halevi, "Implementing gentrys fullyhomomorphic encryption scheme," in Proc. of EUROCRYPT 2011, Tallinn, Estonia, May 2011, pp. 129–148.
[40] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation of computation over large datasets," in Proc. of CRYPTO 2011, CA, USA, Aug. 2011, pp. 111–131.
[41] M. Backes, D. Fiore, and R. M. Reischuk, "Verifiable delegation of computation on outsourced data," in Proc. of ACM CCS 2013, Berlin, Germany, Nov. 2013, pp. 863–874.
[42] D. Chaum and E. van Heyst, "Group signatures," in Proc. of EUROCRYPT 1991, Brighton, UK, Apr. 1991, pp. 257–265.
[43] E. Bresson and J. Stern, "Efficient revocation in group signatures," in Public-Key Cryptography - PKC 2001, Cheju Island, Korea, Feb. 2001, pp. 190–206.

DOI 10.17148/IJARCCE.2016.51104