a
Journal of Engineering Sciences

Vol 13, Issue 06, June/2022

ISSN NO:0377-9254

Efficient Privacy-PreservingCertificateless Public Auditing Of Data In Cloud Storage

A.Vennala #1,M.Radha #2, M.Rohini #3,Md.AneesFathima #4, P.Dharani Lakshmi #5

#1 Assistant Professor, #2,3,4,5 B.Tech., Scholors

Dept of Information Technology, QIS Institute of Technology, Ongole,Prakasam(Dt)

Abstract

Cloud storage service supplies people with an efficient method to share data within a group. The cloud server is not trustworthy, so lots of remote data possession checking (RDPC) protocols are proposed and thought to be an effective way to ensure the data integrity. However, most of RDPC protocols are based on the mechanism of traditional public key infrastructure (PKI), which has obvious security flaw and bears big burden of certificate management. To avoid this shortcoming, identity-based cryptography (IBC) is often chosen to be the basis of RDPC. Unfortunately, IBC has an inherent drawback of key escrow. To solve these problems, we utilize the technique of certificateless signature to present a new RDPC protocol for checking the integrity of data shared among a group. In our scheme, user's private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. To ensure the right public keys are chosen during the data integrity checking, the public key of each user is associated with her unique identity, for example the name or telephone number. Thus, the certificate is not needed and the problem of key escrow is eliminated too. Meanwhile, the data integrity can still be audited by public verifier without downloading the whole data. In addition, our scheme also supports efficient user revocation from the group. The security of our scheme is reduced to the assumptions of computational Diffie-Hellman (CDH) and discrete logarithm (DL). Experiment results exhibit that the new protocol is very efficient and feasible.

Keywords-cloud storage, certificateless cryptography, privacy-preserving, remote data integrity checking

1. Introduction

Cloud storage service offers user an efficient way to share data and work as a team. Once someone of the team uploads a file to the server, other members are able to access and modify the file by Internet. Many real applications such as Dropbox for Business and TortoiseSVNare

used in many companies for their staff to work together. The most important problem of such applications is whether the cloud server provider (CSP) can ensure the data to be kept intact. In fact, the CSP is not fully trustworthy and the failure of software or hardware is inevitable in some way, so serious accidents of the data corruption may occur at any time. Therefore, the user needs to audit the CSP to confirm the data on the cloud server is original.

To ensure the integrity of stored data, a great number of RDPC schemes are proposed. In these schemes, each data block generates an authentication tag which is bound with the block. By checking the correctness of the tags, the verifier is able to learn the status of the data. However, most of these schemes only focus on checking the integrity for personal data, which is not valid under the situation of data shared in a group. When data is shared among multiple users, some new challenges appear which are not well solved in the RDPC schemes for personal data. For example, block tags may be generated by any group user, and different group user will output different tags even if the block is the same one. Moreover, when a group user updates a block, it should regenerate the tag again. When auditing the data integrity, all the authentication tags generated individually need to be aggregated and the information of all the generators for these tags will be involved in. It brings great complexity for the checking scheme. Furthermore, the group is dynamic, any group member may initiatively leave or be fired from the group at any time, so the user revocation is also an important problem that must be addressed. More specifically, once a user is revoked, he should not be allowed to access or modify the data and all his public/private keys are invalid. Under this situation, it is impossible to check the correctness of the tags made by revoked user. Thus, all the tags made by revoked user should be renewed by other normal user. The traditional method is to download the blocks signed by revoked user from the CSP, calculate the new tags and upload the new tags to the cloud again. It will increase heavy computation and communication cost for the normal user. Therefore, this task should be performed by the CSP rather than the normal user. How to design an efficient and secure method to outsource the task is a challenge issue. Besides, public verification is an attractive feature of the data integrity checking work. That is, the integrity of shared data can be verified by not only the data owner but also everyone who is interested in

the cloud data. It is very important for RDPC protocol to support public verification under current open environment.

Until now, lots of schemes have been presented for the integrity verification of data shared in group. However, most of existing RDPC schemes are based on PKI. Although PKI is widely used and occupies an important position in public key cryptography, there are still some security threats in it. For example, the security of PKI is based on the trustworthy of certificate authority (CA), but it is not an easy work to ensure the trustworthiness of CA. Besides, the management of certificate such as distribution, storage, revocation and verification is also a big burden. To avoid these problems, some ID-based RDPC scheme are proposed. Unfortunately, ID-based RDPC schemes suffer from key escrow problem. Namely, the private key generator (PKG) generates all the private keys for the users. If PKG is untrusted, the scheme is not secure either. Thus, ID-based RDPC schemes may be restricted to small, closed settings. Compared with PKI and IBC, certificate less cryptography solves the problems of certificate management and key escrow at the same time. To construct certificate less RDPC scheme is a good method for cloud data integrity checking.

2. Literature Survey

- **Identity-Based Distributed Provable Data Possession in Multicloud Storage**

Authors:H.Wang, D. He,J. Yu and Z. Wang

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multicloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multicloud storage. The formal system

model and security model are given. Based on the bilinear pairings, a concrete ID DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness

assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification, and public verification.

- **Privacy-Preserving Public Auditing for Secure Cloud Storage**

Authors:C. Wang, S. S. M. Chow, Q. Wang

Using cloud storage, users canremotely store their data and enjoy the ondemand high-quality applications andservices from a shared pool ofconfigurable computing resources,without the burden of local data storageand maintenance. However, the fact thatusers no longer have physical possessionof the outsourced data makes the dataintegrity protection in cloud computing aformidable task, especially for users withAuthors78FiguresKRconstrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

- **Provable Data Possession in Cloud Computing**

Authors: Tan Shuang,Jian Feng Zhang,ZhiKun Chen

Several trends are opening up the era ofcloud computing. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This work studies the problem of ensuring the

integrity of data storage in cloud computing. We use RSAS homomorphic property to construct the protocol of provable data possession. In our protocol, we can aggregate multiple Provable Data possession into one, and reduce the overhead of communication. While prior work on ensuring remote data integrity often lacks the specific implementations, this paper achieves an effective proof of storage protocol. Extensive security and performance analysis show that the proposed

3. Proposed System Architecture

To solve these problems, we utilize the technique of certificateless signature to present a new RDPC protocol for checking the integrity of data shared among a group. In our scheme, user's private key includes two parts: a partial key generated by the group manager and a secret value chosen by herself/himself. To ensure the right public keys are chosen during the data integrity checking, the public key of each user is associated with her unique identity, for example the name or telephone number. Thus, the certificate is not needed and the problem of key escrow is eliminated too. Meanwhile, the data integrity can still be audited by public verifier without downloading the whole data. In addition, our scheme also supports efficient user revocation from the group.

During the data verification, all the tags are aggregated to decrease the computation and communication cost. Based on CDH and DL assumptions, we prove the security of our scheme. Besides, our scheme supports public verification and efficient user revocation. We implement our scheme and perform some experiments. The experiment results indicate that our scheme has good efficiency.

A) Complexity Assumption:

Definition 1 (Computational Diffie-Hellman (CDH) problem): Suppose G1 is a multiplicative cyclic groups. G is a generator of G1 . Given the tuple (g, ga, gb,) with the unknown elements , the CDH problem is to compute * ∈Zq a b, ab g .

Definition 2 (CDH assumption): For any probabilistic polynomial time (PPT) algorithm , the advantage for to solve the CDH problem in is negligible, which can be defined as: A ,) b g AG1 , a g g 1 * Pr[(: ,] R CDH ab Adv q ==← g a b Z εΓAA≤ .

Definition 3 (Discrete Logarithm (DL) problem): Assume that is a multiplicative cyclic group. G1 g is a generator of . Given the values of (G1 g , a g) with unknown element , the DL problem is to output a . * a ∈Zq

Definition 4 (DL assumption): For any PPT algorithm , the advantage for to solve the DL problem in is negligible, which can be defined as: AA 1) a g G1 * Pr[(, :] R DL Adv q = g a a Z =←≤εΓAA . Notably, ε denotes a negligible value in the above definitions.

B)The system model:

Group Users, Cloud Servers, Public Verifier, and Group Manager comprise our scheme's suggested cast of characters.

Referring to the papers [25-28], the system model of our scheme is composed of three major entities: user group, cloud service provider (CSP) and public verifier. The user group includes numbers of users, who can upload, access and update the data shared within the group, and honestly execute the protocol. Without loss of generality, the original creator of the group plays the role of group manager, who sets up the system and generates partial keys for general group users. CSP ownspowerful storage and computational abilities to supply cloud users with data storage service. In our scheme, the shared data is divided into many blocks and each block is attached with an authentication tag. Thus, the CSP stores all the blocks and the corresponding tags for cloud user. The data verifier is a person who checks the integrity of the data on CSP. Due to the feature of public verification, anyone could be the verifier in our scheme. The Fig.1 shows the relationships and the interactions among the three entities of the system. As most previous works [4-32], we assume the CSP is semi-trusted. That is, the CSP can honestly execute the protocol, but may cheat the verifier about the incorrectness of the data so as to keep its reputation or get extra benefits.

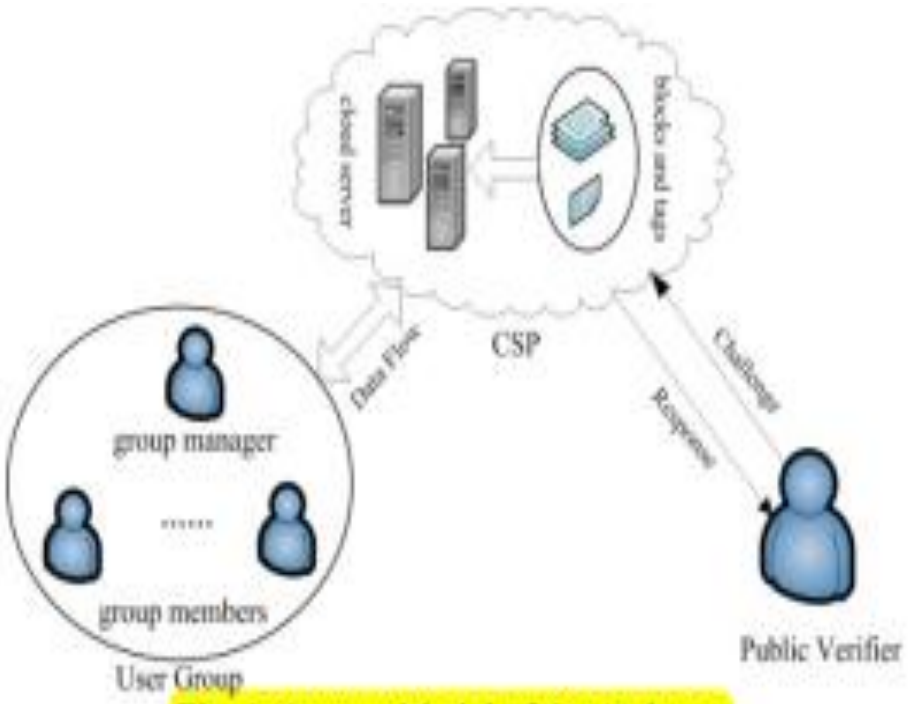

Fig. 1. System Model of Our Scheme

4. Conclusion

In this project, we present a novel RDPC scheme for data outsourced on cloud server. Our scheme devotes to solve the integrity checking for the group data which is shared among many clients of a team. We utilize the idea of certificate less signature to generate all the block tags. Because each user of a group has both partial key and secret value, the problem of key escrow is eliminated in our scheme and the certificate management in PKI does not exist. Besides, our scheme supports public verification, efficient user revocation multiuser data modification detailed description of the system model and security model of our scheme. At last, based on the CDH and DL assumption, we prove the security of our scheme. The experiment results show that our scheme has good efficiency.

References

[1] Shamir A. Identity-Based Cryptosystems and Signature Schemes, Berlin, Heidelberg, F, 1985 [C]. Springer Berlin Heidelberg.

[2] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography, Berlin, Heidelberg, F, 2003 [C]. Springer Berlin Heidelberg.

[3] Ateniese G, Burns R, Curtmola R, et al. Provable Data Possession at Untrusted Stores [J]. Proceedings of the ACM Conference on Computer and Communications Security, 2007, 598-609.

[4] Juels A, Kaliski B S. Pors: proofs of retrievability for large files [M]. Proceedings of the 14th ACM conference on Computer and communications security. Alexandria, Virginia, USA; Association for Computing Machinery. 2007: 584±97.

[5] Shacham H, Waters B. Compact Proofs of Retrievability [J]. journal of cryptology, 2013, 26(3): 442-83.

[6] Ren Z, Wang L, Wang Q, et al. Dynamic Proofs of Retrievability for Coded Cloud Storage Systems [J]. IEEE Transactions on Services Computing, 2018, 11(4): 685-98.

[7] Curtmola R, Khan O, Burns R, et al. MR-PDP: Multiple-Replica Provable Data Possession; proceedings of the 2008 The 28th International Conference on Distributed Computing Systems, F 17-20 June 2008, 2008 [C].

[8] Erway C, Küpçü A, Papamanthou C, et al. Dynamic Provable Data Possession [J]. Acm T Inform Syst Se, 2009, 17(213-22.

[9] Wang H. Proxy Provable Data Possession in Public Clouds [J]. Services Computing, IEEE Transactions on, 2013, 6(551-9.

[10] He C. Public Batch Auditing for 2M-PDP Based on BLS in Cloud Storage [M]. 2014.

[11] Wang B, Li B, Li H. Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud [J]. ieee transactions on services computing, 2015, 8(1): 92-106.

[12] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing, Berlin, Heidelberg, F, 2001 [C]. Springer Berlin Heidelberg.

[13] Cash D, Küpçü A, Wichs D. Dynamic Proofs of Retrievability Via Oblivious RAM [J]. Journal of Cryptology, 2017, 30(1): 22-57.

[14] Wang Q, Wang C, Ren K, et al. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing [J]. 2011,

[15] Merkle R C. Protocols for Public Key Cryptosystems; proceedings of the 1980 IEEE Symposium on Security and Privacy, F, 1980 [C].

[16] Zhu Y, Ahn G, Hu H, et al. Dynamic Audit Services for Outsourced Storages in Clouds [J]. IEEE Transactions on Services Computing, 2013, 6(2): 227-38.

[17] Hao, Jin, Ke, et al. Full integrity and freshness for cloud data [J]. 2018, 80(640-52.

[18] Cong W, Qian W, Ren K, et al. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing; proceedings of the 2010 Proceedings IEEE INFOCOM, F, 2010 [C].

[19] Yang K, Jia X. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(9): 1717-26

[20] Wang C, Chow S S M, Wang Q, et al. Privacy-Preserving Public Auditing for Secure Cloud Storage [J]. 2013,

[21] Wang B, Li B, Li H. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud; proceedings of the Applied Cryptography and Network Security, Berlin, Heidelberg, F 2012//, 2012 [C]. Springer Berlin Heidelberg.

[22] Wang B, Li B, Li H. Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud; proceedings of the 2012 IEEE Fifth International Conference on Cloud Computing, F 24-29 June 2012, 2012 [C].

[23] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing; proceedings of the Advances in Cryptology ² CRYPTO 2001, Berlin, Heidelberg, F 2001//, 2001 [C]. Springer Berlin Heidelberg.

[24] Wang H. Identity-Based Distributed Provable Data Possession in Multicloud Storage [J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-40.

[25] Yu Y, Au M H, Ateniese G, et al. Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage [J]. Ieee T Inf Foren Sec, 2017, 12(4): 767-78.

[26] Zhang J, Dong Q. Efficient ID-based public auditing for the outsourced data in cloud storage [J]. Inform Sciences, 2016, 343-344(1-14.

[27] Wang H, He D, Yu J, et al. Incentive and Unconditionally Anonymous Identity-Based Public Provable Data Possession [J]. IEEE Transactions on Services Computing, 2019, 12(5): 824-35.

[28] Li J, Yan H, Zhang Y. Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage [J]. IEEE Transactions on Services Computing, 2021, 14(1): 71-81.

[29] Wang B, Li B, Li H, et al. Certificateless public auditing for data integrity in the cloud; proceedings of the 2013 IEEE Conference on Communications and Network Security (CNS), F 14-16 Oct. 2013, 2013 [C].

[30] He D, Kumar N, Zeadally S, et al. Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems [J]. IEEE Transactions on Industrial Informatics, 2018, 14(3): 1232-41.

[31] Zhang Y, Xu C, Yu S, et al. SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors [J]. IEEE Transactions on Computational Social Systems, 2015, 2(4): 159-70.

[32] He D, Chen J, Zhang R J I C e A. An efficient and provably-secure certificateless signature scheme without bilinear pairings [J]. 2012, 2010(632.

[33] He D, Huang B, Chen J. New certificateless short signature scheme [J]. Information Security, IET, 2013, 7(113-7.

[34] He D, Kumar N, Zeadally S, et al. Certificateless Provable Data Possession Scheme for Cloud-Based Smart Grid Data Management Systems [J]. IEEE Transactions on Industrial Informatics, 2018, 14(3): 1232-41.

[35] Li J, Yan H, Zhang Y. Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage [J]. IEEE Transactions on Services Computing, 2021, 14(1): 71-81.

[36] Wu G, Mu Y, Susilo W, et al. Privacy-Preserving Cloud Auditing with Multiple Uploaders; proceedings of the Information Security Practice and Experience, Cham, F 2016//, 2016 [C]. Springer International Publishing.