© 2017 IJSRST | Volume 3 | Issue 4 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

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

Ritu A. Rangari[1], Dr. Dhananjay M. Dakhane[2]

[1]ME Student, Department of Computer Science and Engineering, SIPNA College of Engineering and Technology, Amravati, Maharashtra, India
[2]Associate Professor, Department of Computer Science and Engineering, SIPNA College of Engineering and Technology, Amravati, Maharashtra, 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. 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 our scheme definition. Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, countability 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.

Keywords: AGKA, TPA, Cloud Server

I. INTRODUCTION

In past years, the rapid development of cloud storage services makes it easier than ever for cloud users to share data with each other. To ensure users' confidence of the integrity of their shared data on cloud, a number of techniques have been proposed for data integrity auditing with focuses on various practical features, e.g., the support of dynamic data, public integrity auditing, low communication/computational audit cost, low storage overhead. However, most of these techniques consider that only the original data owner can modify the shared data, which limits these techniques to client read-only applications. 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 services(S3) in online data backup services of Amazon, and practical cloud based software Google drive, drop box, mozy, bitcas and memopal have been built for cloud application. There is invalid result in cloud server such as server hardware, software failure, human maintenance and malicious attack. Rabin data dispersion scheme implemented for practical application and overcome above challenges. The limited dynamic scheme cloud only efficiently supports Special field operation (e.g. Append).These applications provide secure file sharing within dynamic group in corporate company with some security features in cloud. Main objectives is to develop secure file storage system on cloud for corporate and to prevent from internal leakage.The static scheme not supports data modification. In publicly verifiable, data integrity check can be performed by data owner and by any third party auditor. Multiple user in group need to share source code they need to access, modify compile and run the shared source code at any time and place. Remote data auditing is only data owner can update its data. Ring signature supports multiple user data operation. The proxy Re-signature is private and authenticated channels exist between each pair of entities. Till today is no solution for above problem in public integrity auditing with group user modification. For providing the integrity and

availability of remote cloud store, some solutions and their variants have been proposed.

II. LITERATURE SURVEY

To support multiple user data operation, Wang et al. [7] proposed a data integrity based on ring signature. In this 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. [7] designed a scheme based on proxy designators.

To make the scheme efficient, scalable and collusion resistant is Yuan and Yu [6], who designed a dynamic public integrity auditing scheme with group user 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. It means that, their scheme could efficiently support plaintext data update and integrity auditing, while not ciphertext data.

Plenty of researchers have devoted considerable attention to the problems on to securely outsource local store to remote cloud server. Among which, the problem of remote data integrity and availability auditing attacks the attestation of many researchers. The concepts and solution Provable Data Possession (PDP)and Proofs of Retrievability (PoR) were first proposed by Ateniese et al.[9] And Juels et al[10].In their scheme, the homomorphic authentication technique was adopted to reduce both the communication and computation cost. Later, a number of variants of PDP and PoR schemes are designed to improve the efficiency and enhance the function of basic schemes, such as allowing public auditing [3], [5], [6] and supporting data update.

To enhance the previous works, Wang et al. [5] designed a scheme to support share data integrity auditing, whose scheme adopted ring signature to protect the privacy of users. The limitation of the scheme is that it does no support dynamic group and also suffers from a computational overhead linear to the group size and the number of data auditing. To further support user revocation, Wang et al. [5] designed another scheme based on the assumption that no collusion occurs between cloud servers and revoked user.Group signatures without revocation.

The provably coalition-resistant scalable group signature was described by Ateniese, Camenisch, Joye and Tsudik [10]. At that time, the security of group signatures was not totally understood and proper security definitions were given later on by Bellare, Micciancio and Warinschi [9] (BMW) whose model captures all the requirements of group signatures in three properties. In (a relaxation of) this model, Boneh, Boyen and Shacham [9] obtained a construction in the random oracle model with signatures shorter than 200 bytes . In the BMW model, the population of users is frozen after the setup phase beyond which no new member can be added.

Ateniese et al. [9] also gave a construction without random oracles using interactive assumptions. In the BMW model [9], Boyen and Waters independently came up with a different standard model proposal using more classical assumptions and they subsequently renamed their scheme to obtain constant-size signatures.

III. PROPOSED WORK

All Proposed Model explore on the secure and efficient shared data integrate auditing for multi-user operation for cipher text database. By incorporating the primitives of victor commitment, asymmetric group key agreement and group signature and an efficient data auditing scheme while at the same time providing some new features, such as traceability and countability. Also provide the security and efficiency analysis and the analysis results show that it is secure and efficient. A system model for the cloud storage architecture, which includes three main network entities: users, a cloud server, and a trusted third party.

In below system model the data owner could encrypt and upload its data to the remote cloud storage server. Also, the access and modify privileges is shared to a number of group users. Even if the data is frequently updated by the group users, the TPA efficiently verifies the integrity of the data stored in the cloud storage server. The owner of data is different from other group users. When a group user is found malicious or the contract of the user is expired, he/she could securely revoke a group user.

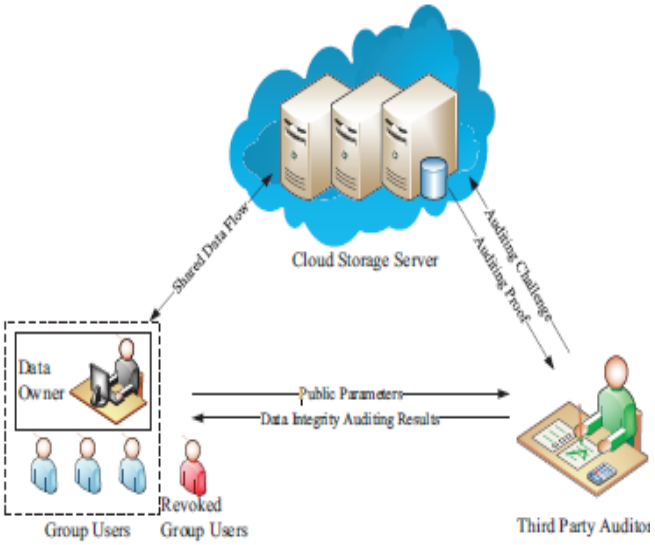

Figure 1. System Model

A. User

An individual or group entity, which owns its data stored in the cloud for online data storage and computing.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.

B. Cloud server

An entity, which is managed by a particular cloud service provider or cloud application operator to provide data storage and computing services. The cloud storage server is semi-trusted, who provides data storage services for the group users.The cloud server is regarded as an entity with unrestricted storage and computational resources.

C. Trusted Third Party

An optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration. In the cloud storage, a user remotely stores its data via online infrastructures, platforms, or software for cloud services, which are operated in the distributed, parallel, and cooperative modes. 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.During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other users.

IV.CONCLUSION

The preserving of verifiable database with efficient and secure updates is an important way to solve the problem of verifiable data storage. The proposed system securely share the data file among the dynamic groups without revealing their identity members in the same group can share the data efficiently. Cryptography is used for over all security. It is used for efficient revocation without updating private keys of remaining users. In future, concentrate on key management, how to revoke the private keys from the group members. Here provide security analysis, and it shows that propose system model provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users.

V. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. of IEEE CLOUD2012, Hawaii, USA, Jun. 2012, pp. 295–302.

[6] 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.

[7] 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.
[8] Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation Tao Jiang, Xiaofeng Chen, and Jianfeng Ma.
[9] 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.
[10] 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.