ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

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

Saraswati Gore[1], Ashokkumar Kalal[2]

M. E Student, Dept. of Computer Engineering, Alard College of Engineering and Management, Savitribai Phule Pune University, Pune, India[1]

Assistant Professor, Dept. of Computer Engineering and Management, Savitribai Phule Pune University, Pune, India[2]

ABSTRACT: The approach of the distributed computing makes stockpiling outsourcing turn into an expanding pattern, which advances the protected remote information examining a fundamental theme that showed up in the examination writing. Recently some research considers the problem of secure and efficient public data integrity auditing for disseminate dynamic data. However, these plans are still not secure against the collusion of cloud storage server and revoked group users during user revocation unsuitable 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 cancelation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the scheme definition. Our scheme keeping 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: Cloud Computing, Centrality, Cloud Security, Fragmentation, Replication, Performance, Internet Protocol Vulnerability.

I. INTRODUCTION

The improvement of distributed computing rouses endeavors and associations to outsource their information data to third-party cloud service providers (CSPs), which will improve the storage limitation of resource, constrain local devices. Recently, some trading cloud storage services, such as the simple storage service (S3) on-line data backup services of Amazon and some practical cloud based software Google Drive, Dropbox , Mozy , Bitcasa, and Memopal, have been construct 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, 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 dare of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme. are far from practical application. Recently, the development of cloud computing boosted some applications, 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 demand to access, modify, compile and run the shared source code at any time and place. The recent cooperation network model in cloud makes the remote data auditing schemes become impractical, where only the data owner can be update its data. Evidently, trivially expanding a scheme with an online data owner to update the data for a group is inappropriate for the data owner. It will cause enormous communication and computation overhead to data owner, which will result in the single point of data owner. To carry multiple user data proposed data integrity based on ring signature. To increase the previous scheme and make the scheme efficient, scalable and collusion resistant designed a dynamic public integrity auditing scheme with group user revocation. 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 disannualationgroup signature. It provide

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure opposed to the collusion attack from the cloud storage server and revoked group users.

II. LITERATURE SURVEY

J. Yuan and S. Yu,[1] presented efficient public integrity checking for cloud data sharing with multi-user modification in which is featured by salient properties of public integrity checking and continual computational cost on user side. We achieve this through our novel design on polynomial based authentication tags which allows accumulation of tags of different data blocks.

X. Chen, J. Li, J. Weng, J. Ma, and W. Lou,[2] proposed verifiable computation over large database with incremental updates. Authors formalize the notion of verifiable database with incremental updates (Inc-VDB). Besides, they propose a general Inc-VDB framework by incorporating the primitive of vector commitment and the encrypt-then-incremental MAC mode of encryption. They present a concrete Inc-VDB scheme based on the computational Diffie-Hellman (CDH) assumption and prove that system can achieve the desired security properties.

E. Shi, E. Stefanov, and C. Papamanthou,[4] proposed practical dynamic proofs of retrievabilitywith constant client storage whose bandwidth cost is comparable to a Merkle hash tree, thus being very practical. There construction outperforms the constructions of Stefanov et al. and Cash et al., both in theory and in practice. Specifically, for n outsourced blocks of β bits each, writing a block requires $\beta + O(\lambda \log n)$ bandwidth and $O(\beta \log n)$ server computation (λ is the security parameter). Audits are also very efficient, requiring $\beta + O(\lambda^2 \log n)$ bandwidth. They also show how to make there scheme publicly verifiable, providing the first dynamic PoR scheme with such a property. They finally provide a very efficient implementation of our scheme.

B. Wang, L. Baochun, and L. Hui,[5] presented public auditing for shared data with efficient user revocation in the cloud. By utilizing the idea of proxy re-signatures, they allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud.

C. Wang, Q. Wang, K. Ren, and W. Lou,[6] presented privacy-preserving public auditing for data storage security in cloud computing utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files.

III. EXISTING SYSTEM APPROACH

For providing the integrity and availability of faraway cloud store, existing systems provides some solutions. In these solutions, when a scheme helps 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 openly 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. The user revocation problem is not examine and the auditing cost is linear to the group size and data size.

Disadvantage:

1) The user revocation problem is not considered and the auditing cost is linear to the group size and data size.
2) In previous systems could efficiently support plaintext data update and integrity auditing, while not ciphertext data.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

3) 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.
4) The data owner does not take part in the user revocation phase, where the cloud itself could conduct the user revocation phase.
5) 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.

IV. PROPOSED SYSTEM APPROACH

We propose a new idea called Public Integrity Auditing for shared dynamic cloud data with group user revocation which explore how to design an efficient and reliable scheme, while accomplishing secure group user revocation. The system not only keeps group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation. The proposed system, inspect on the secure and efficient shared data integrate auditing for multi-user operation for ciphertext database. It proposes an efficient data auditing scheme while at the same time providing some new features, such as traceability and countability.

Advantage:

1) Provides data integrate auditing for multi-user operation for ciphertext database.
2) Provide the security and efficiency analysis of our scheme.
3) Provide reliability, confidentiality, traceability and countability.

V. PROPOSED ARCHITECTURE

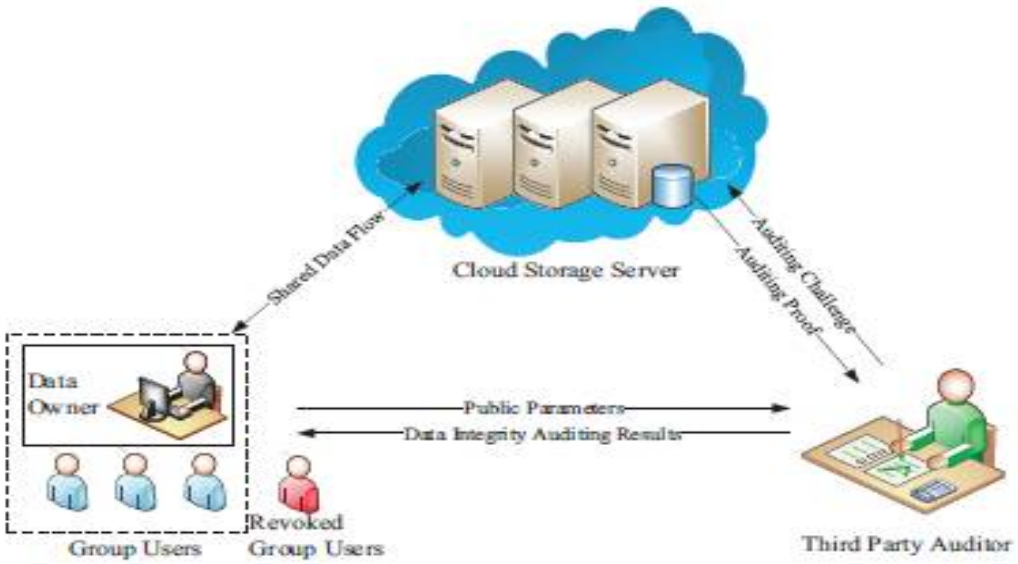

Fig 01: System Architecture

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

VI. MODULES

A. DATA OWNER:
Data owner is responsible for uploading file on cloud as well as view files uploaded by him or others. Data owner must have to register in our system.

B. DATA USER:
Data user is the one who is responsible for downloading files or view files uploaded by data owners. To download file from cloud he has to be authenticated user otherwise he will be considered as attacker.

C. THIRD PARTY AUDITOR(TPA):
Third party auditor is an authorized person who has rights to validate authorized data owner and user. He is also responsible for allocation of block and maintains information and authentication.

D. CLOUD STORAGE SERVER:
Cloud storage server holds files or data of the data owner on the cloud. Data owner must have to pay charges for this.

VII. CONCLUSION

The first of verifiable database with efficientupdates is an eventful way to solve the problemof verifiable outsourcing of storage. We propose ascheme to clear up efficient and secure data integrityauditing for share dynamic data with multi-user modification.The scheme vector commitment, AsymmetricGroup Key Agreement (AGKA) and group signatureswith user revocation are adopt to achievethe data integrity auditing of remote data. Besidethe public data auditing, the amalgamating of the threeprimitive enable our scheme to outsource ciphertextdatabase to remote cloud and support secure groupusers revocation to shared dynamic data. We providesecurity analysis of our scheme, and it shows that ourscheme provide data confidentiality for group users,and it is also secure against the collusion attack fromthe cloud storage server and revoked group users.Also, the performance analysis shows that, comparedwith its pertinent schemes, our scheme is also efficientin different phases.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preservingpublic auditing for data storage security in cloud computing,”inProc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp. 525–533.
[7] B. Wang, B. Li, and H. Li, “Oruta: Privacy-preserving publicauditing for shared data in the cloud,” in Proc. of IEEE CLOUD2012, Hawaii, USA, Jun. 2012, pp. 295–302.
[8] D. Catalano and D. Fiore, “Vector commitments and theirapplications,” in Public-Key Cryptography - PKC 2013, Nara,Japan, Mar. 2013, pp. 55–72.
[9] J. G. et al. (2006) The expanding digital universe: A forecast ofworldwide information growth through 2010. IDC. [Online].Available: Whitepape.
[10]M. A. et al., “Above the clouds: A berkeley view of cloudcomputing,” Tech. Rep. UCBEECS, vol. 28, pp. 1–23, Feb. 2009.