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 9, September 2016

A Survey on Efficient Data Integrity Checking with Group User Revocation in Cloud

Dhamale Swapnali[1], Bagul Sonali[2], Dhadge Madhuri[3], Garad Priyanka[4], Prof. Sonali A. Patil[5]

B.E. Student, Dept. of Computer Engineering, BSIOTR, Wagholi, Maharashtra, India[1,2,3,4]

Asst. Professor, Dept. of Computer Engineering, BSIOTR, Wagholi, Maharashtra, India[5]

ABSTRACT: Now a days in cloud computing technology data storage outsourcing on cloud is growing rapidly. To calculate how much data access data auditing collect reviews. On the basis of company performance and profit system work on profiling data avoid collision to access data. Now a days some researchers believed on save data effectively and securely on cloud.On the other hand, these systems are stillnot secure beside the collusion of cloud storage server as well as revoked group users during user revocation inpractical cloud storage system. In previous paper we found that collusion attack an efficient public integrity auditing scheme with secure group user revocation based on vector commitment plus verifier-local revocation group signature. We invented a concrete scheme. We propose a new structure called Decrypt key, which provides efficiency and reliability assurance for convergent key management on mutually user along with cloud storage sides. The design is to apply de-duplication to the convergent keys to influence secret sharing techniques. In particular, we build secret shares for the convergent keys and share out them across multiple independent key servers. Our proposed system rigging the public checking and efficient user revocation, as well as also some fine assets, such as confidently, efficiency, count ability and trace ability. There is efficient use of vector commitment and verifier local revocation group signature. We implement concrete scheme for group signature. The scheme support public checking, efficient user revocation, and properties like confidently, efficiency, count ability and traceability. Finally we compare our scheme with old which shows good result in security. The enhancement of cloud computing make storage outsourcing becomes an exceeding trend, which result a secure data auditing a 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. In this paper, there will be auditing the integrity of shared data with dynamic groups in cloud. A new user can be added into the group and an existing group member can be revoked by preserving privacy including data backup based on vector commitment and verifier-local revocation group signature. This scheme supports the public validation and efficient user revocation and also some nice properties such as traceability, efficiency, confidently, accountability. Finally, the security and experimental analysis show that our scheme is also secure and efficient.

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

I. INTRODUCTION

Mobile The growth of cloud computing encourages the endeavours and organization to subcontract their data to third-party cloud service providers. This will progress the storage drawbacks of resource limit local devices. In recent times, various profitable cloud storage services, such as the simple storage service, data backup services, realistic cloud based

Software Google Drive are built for cloud application. Ever since the cloud servers may return unacceptable results, it's because of server's hardware failure or software failure. Sometimes human maintenance may lead to problems. And malicious attack will lead to unacceptable loss or result of data. To prevent from this situation, we are in need of data integrity and accessibility. This data integrity and accessibility are helps to protect data of cloud users. It also helps to provide privacy to the user's data. The improvements and enhancements in cloud computing motivates organization as well as enterprises to outsource their data to third party cloud service providers (CSP's) which will result in improvements the data storage limitation of resource constrain local devices. In market, already some cloud storage services are available like simple storage service (S3) [1] on-line data backup services of Amazon and software like

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 9, September 2016

Google Drive, [2] Dropbox, [3] Mozzie, [4] Bitcasa and [5] 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 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.Cloud Storage service are such as simple storage services in online data backup services of amazon, and practical cloud based software Google drive, drop box, mozzie, bitcasa and memo pal 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.

II. RELATED WORK

In A large amount of researchers have committed significant concentration to the troubles on how to securely outsource local pile up to remote cloud server. The problem of remote data integrity and availability auditing attacks the attestation of many researchers.

SagarikaDev Roy, et.al (2014) proposed a methodology for secure outsourcing oflinear Computations into the cloud environment. Outsourcing is a common procedure engaged in the business worldwhen the customer chooses to farm out a certain task to an agent for the benefit of the firm in terms of time and cost.They proposed methodology to detecting a malicious server, in an efficient result verification method.

Yongjun Ren, et.al (2012) proposed designated verifier provable data possession. This plays a major role in public clouds. Designated verifier provable data possession is a matter of crucial importance when the client cannot perform the remote data possession checking. By using the system security model and homomorphism authenticator they designed a new scheme. The scheme removed luxurious bilinear computing process. Furthermore in this proposal, the cloud storage server is stateless and independent of the verifier. This is an important secure property of any other schemes. In the course of security analysis and performance analysis, their scheme is secure and high efficiency.

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 9, September 2016

FrancescSebe, et.al (2008) proposed a methodology to check the efficient of remote data control or possession. For checking the data possession in a complex information system such as power facilities, airports, data vaults, anddefense systems is a matter of vital importance. Data possession checking protocols permits us to check a remote server is able to admission an uncorrupted file. In such a way that the verifier need not to know about the whole file, that isgoing to be verified. Regrettably, present protocols only allow a limited number of successive verifications or just theimpractical from the computational point of view. In this presents a new protocol for remote data possession checking.

Giuseppe Ateniese, et.al (2008) proposed a methodology to operate on the remote storage data in a high secured manner. The main concern is how much frequently, efficiently and securely the system will verify that a storage server is realistically storing its client's. Key thing is the client's outsourced data are potentially very large. The storage server is assumed to be not trusted in terms of both the security and reliability. It might unkindly or unintentionally wipe out data being hosted. But the problem is exacerbated by the client being a small computing device with partial resources. Previous work has deal with this problem that is use public key cryptography or outsource its data in encrypted structure. In this paper, they constructed a extremely efficient and secure technique based completely on symmetric key cryptography. If detection of any modification or deletion of small parts of the file is important then erasure codes could be used.

Jiawei Yuan, et.al (2014) proposed a new method based on some modern procedures such as based on authentication polynomial tags and linear authenticators. Data integrity auditing is achieved concurrently in this approach. The proposed idea is to characterize the constant real time communication and also the computational cost on the user's side. It supports both public auditing along with batch auditing process.Many data loss and corruption events are reported against the well-known cloud service providers, data owners, to resolve these issues they need to periodically audit the integrity of theiroutsourced data. And also every cloud service providers must improve their efficiency of cloud storage. To minimizethe unnecessary redundant copies, the cloud storage servers would deduplication the data. By having only one or fewcopies for each file and making a link to the file for every user who asks the same file stored in the disk.

III. PROPOSED ALGORITHM

In this paper, we study the problem of constructing public authentication inspection for shared dynamic data with group user revocation. Our contributions are:

1) For cipher text database, we explore on the secure and efficient shared data integrate auditing for multi-useroperation.

2) We intend an efficient data auditing scheme along with new features such as traceability and countability by incorporating the vector commitment primitives, asymmetric group key agreement and group signature.

3) The analysis results show that our scheme is secure and efficient as we provide the security and efficiency 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 deduplication constructions and this authorized duplicate check scheme comparatively incurs minimum overhead than normal operations.

The conventional encryptions have need of particular users to encrypt their data, with the own keys of the user. Therefore, the same data copies of different users will lead to dissimilar cipher texts. It creates integrity checking process is an impossible task. Data outsourcing hoist security and privacy worry. We need to trust third-party providers for proper implementation of confidentiality, integrity checking, and access control mechanisms. The present system use standard encryption scheme for identifying duplicate blocks, the blocks are stored in cloud. In Cloud Storage, standard encryption of identical files generates same key and same cipher text. As a result Data de duplication is impossible in encrypted data. When user lost the key, there was impossible to restore the original content of the file. Message digest algorithm provides a viable option to enforce data confidentiality while realizing duplication.

It encrypts or decrypts a data copy with the help of a convergent key. By computing cryptographic hash value of thecontent of the data copy we can obtain the key. After key generation process and data encryption process, users canhang on to the keys. Then the user sends the cipher text to the cloud environment. Ever since encryption is

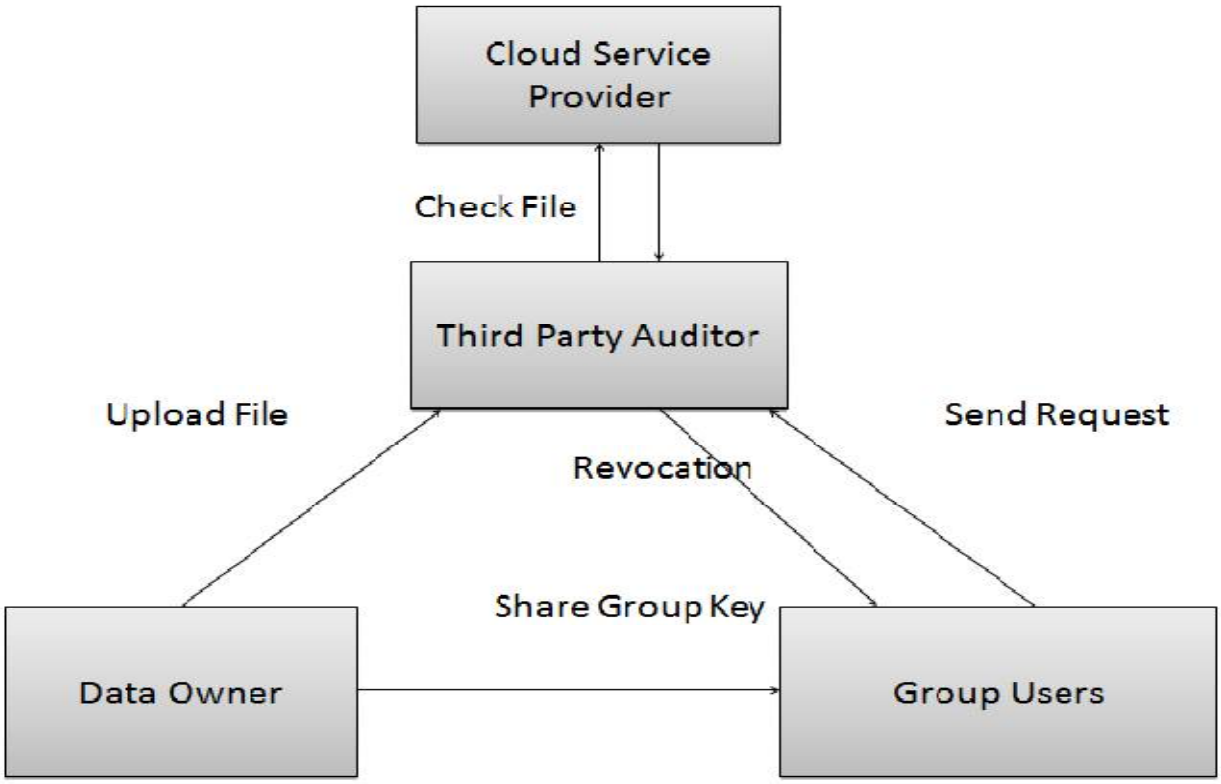
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

deterministic, the same data copies will generate similar convergent key and the identical cipher text. This permits the cloud to perform deduplication over the cipher texts. Cipher texts are able to decrypt by the corresponding user's with their convergent keys. Convergent encryption practical is to efficiently and reliably manage a huge number of convergent keys.



The unique Data block will be selected and those blocks are placed in the cloud service provider's space. We are using crypto graphic algorithm for integrity checking. Message authentication code is the scheme of producing Message digest for input file. The integrity checking should be done by Third party auditor by checking this message digest code.Before uploading file; data owner must send the hash key to the third party auditor. Third Party Auditor receives the key and verify with cloud service provider to check whether this file is already uploaded or not. In this module, user revokes the content by getting secret key of data owner. Data owner must share the secret key for group users. User downloads the file from the cloud service provider using hash key.

IV. CONCLUSION AND FUTURE WORK

In this paper, 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. When compared to other algorithm key size is very small, it isnot able to hack easily. It is used for efficient revocation without updating private keys of remaining users. Infuture, concentrate on key management, how to revoke the private keys from the group members. This paper proposed system to realize efficient and secure data integrity auditing for dynamic data. The proposed model consists of the public data auditing. This technique will provide better data confidentiality compare to other methodologies.

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 9, September 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 Deduplication," 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. 2904–2912IJCATM:www.ijcaonline.org.