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. 3, Issue 11, November 2015**

# Public Integrity Auditing for Shared Dynamic Cloud Data

**Radhika.S[1], Sukumar.M[2]**

PG Scholar, Dept. of CSE, Sri Vidya College of Engineering & Technology, Virudhunagar, Tamil Nadu, India[1]

Assistant Professor, Dept. of CSE, Sri Vidya College of Engineering & Technology, Virudhunagar, Tamil Nadu, India[2]

**ABSTRACT**: The arrival of cloud computing technology makes the storage outsourcing become a growing trend, which encourages the secure remote data auditing. Data auditing is the process of conducting a data review to measure how company's data is fit for agreed function. This engages profiling of data and assesses the collision of pitiable quality data on the organization's performance and profits. In recent times, some research believes the problem of secure with efficient public data integrity auditing for unified dynamic data. On the other hand, these systems are still not secure beside the collusion of cloud storage server as well as revoked group users during user revocation in practical cloud storage system. In this paper, we found out that the collusion attack in the exiting scheme .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 traceability.

**KEYWORDS**: Key management, Insider attacks, Outsider attacks, Data confidentiality, Integrity Checking

## I. INTRODUCTION

The growth of cloud computing encourages the endeavors 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 servers' 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 users' data.

To triumph over the above vital security dispute of today's cloud storage services, simple replication, data dispersion scheme are far from sensible claim. To ensure the availability of data when a quorum of repositories we need later protocols. On the other hand, they do not offer guarantee about the availability of each repository. This will obviously limit the assurance, which the protocols can be able to provide relying parties. To provide integrity and availability of distant cloud storage, we have some resolution and their alternatives. In this explanation, if a system supports data modification, we say it is a dynamic scheme, if not static one. Another alternative method is Limited dynamic scheme, it is similar to that one, but it competently support few specified operations, namely append operation.

We introduce publicly verifiable scheme, it helps in various aspects. That is data integrity can be performed not only by data owners, but also by one or more third party auditor. Conversely, the dynamic schemes we mentioned only focus on the gears where there is a data owner and only the data owner could change the data. In recent times, the growth of cloud computing, improves that some applications uses cloud service, can use as a collaboration platform. Few of the software development surroundings, one or more users in a group may need to share some of the source code, need to access, modify. At some times they may need to compile and run the shared source code at any time and place.

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. 3, Issue 11, November 2015**

The new collaboration network model in cloud computing makes some of the remote data auditing schemes turn out to be infeasible. We can say that only the data owner can update its data, others cannot modify the data in the storage. Evidently, irrelevantly extending a scheme with data owner to update the data for a group is unsuitable for the data owner. It will cause terrific communication overhead and computation overhead to data owner. It will results in the single point of data owner. To support multiple user data operation, we have data integrity based on ring signature. The user revocation problem is not considered and the auditing cost is linear to the group size and data size.

## II. RELATED WORK

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. *Sagarika Dev Roy, et.al (2014)* proposed a methodology for secure outsourcing of linear Computations into the cloud environment. Outsourcing is a common procedure engaged in the business world when 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.

*YongjunRen, 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.

*FrancescSebe, et.al (2008)* proposed a methodology to check the efficent of remote data control or possession. For checking the data possession in a complex information system such as power facilities, airports, data vaults, and defence 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 is going to be verified. Regrettably, present protocols only allow a limited number of successive verifications or just the impractical 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 clients' 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 users' side. It supports both public auditing along with batch auditing process. The security of our proposed scheme is fully based on the Computational Diffie-Hellman hitch. 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 their outsourced data. And also every cloud service providers must improve their efficiency of cloud storage. To minimize the unnecessary redundant copies, the cloud storage servers would deduplicate the data. By having only one or few copies for each file and making a link to the file for every user who asks the same file stored in the disk.

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. 3, Issue 11, November 2015**

## III. LITERATURE REVIEW

A literature study has been made on the different algorithms and various methodologies to produce Public Integrity Auditing for Shared Dynamic Cloud Data. Every author has their own perspective for the security and privacy of the files and documents stored on the remote host or server. Some of them suggest high form of encryption like Convergent Encryption, Integrity checking. By analysing the views and aspects of various authors we may get an efficient way for securing the data stored in a third party environment. The table following shows the literature studies for Public Integrity Auditing for Shared Dynamic Cloud Data.

| AUTHOR & YEAR | TITLE | METHODOLOGY | DISADVANTAGES |
|---|---|---|---|
| Mihir Bellare, et al., 2013 | Message-Locked Encryption and Secure De duplication | In this paper, they provide definitions for privacy and for a form of integrity .This we call it as the tag consistency. This gives more secured encryption and also eliminates the redundant files in the storage. | Conventional encryption makes de duplication impossible. |
| Austin T, et al., 2014 | Decentralized De duplication in SAN Cluster File Systems | In this paper, they propose DEDE, a block-level de duplication system for live cluster file systems. This does not require any central coordination, tolerates host failures.<br>It takes advantage of the block layout policies of an existing cluster file system.<br>Each host periodically and independently processes the summaries of its locked files. Then merges them with a shared index of blocks, and reclaims any duplicate blocks. | Users' cannot recover the original content of the data block. |
| Danny Harnik, et al. 2002 | Side Channels in Cloud Services: De duplication in Cloud Storage | They demonstrate how de duplication can be used as a side channel which reveals information about the contents of files of other users.<br>De duplication reduces the space and bandwidth requirements of data storage services, and is most effective when applied across multiple users, a common practice by cloud storage offerings. | De duplication can be used as a side channel which reveals information about the contents of files of other users. |
| Mingqiang Li, et al. 2012 | On the Confidentiality of Information Dispersal Algorithms and Their Erasure Codes | To achieve strong confidentiality, this paper explores a sufficient and feasible condition on the adopted erasure code.<br>Then, this paper shows that Rabin's IDA has strong confidentiality.<br>This paper constructs an IDA with strong confidentiality from a Reed-Solomon code. | User cannot recover the original content of the data block. |
| Vipul Goyal Omkant, et | Attribute-Based Encryption for Fine- | They developed a new cryptosystem for fine-grained sharing of encrypted | Secret-sharing schemes (SSS) are used to divide a secret among a |

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. 3, Issue 11, November 2015**

| | | | |
|---|---|---|---|
| al. 2006 | Grained Access Control of Encrypted Data | data. That we call Key-Policy Attribute-Based Encryption (KP-ABE). The cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt.<br>This situation is not particularly appealing from a security standpoint | number of parties |
| Maged Hamada Ibrahim, et al. 2009 | A Method for Obtaining Deniable Public-Key Encryption | In this paper, they we presented a methodology namely sender deniable public-key encryption. The sender is able to recline about the encrypted message to a coercer. It may leads to flee coercion.<br>Although the receiver is able to decrypt for the true message, the sender has the ability to open a fake message of his choice to the coercer. The message sent by the user can be verified and gives the same ciphertext as the true message.<br>The coerced user after transmission forcing him to reveal all his random inputs used during encryption or decryption. | The schemes are unplanned deniable and are not secure as plan-ahead-deniable unless the coercer has no control on the sender's local randomness. |
| Nuttapong Attrapadung, et al. 2001 | Attribute-Based Encryption Schemes with Constant-Size Ciphertexts | This paper proposes the first attribute-based encryption (ABE) system allowing for truly expressive access structures and with constant ciphertext size. Our first result is a ciphertext-policy attribute-based encryption scheme with O(1)-size ciphertexts for threshold access policies and where private keys remain as short as in previous systems.<br>In key-policy ABE schemes, attribute sets are used to annotate ciphertexts and private keys are associated with access structures | This was necessary since prior IBR systems with short ciphertexts were not directly amenable to fulfill these requirements. |
| Paolo Gasti, et al. 2010 | Deniable Cloud Storage: Sharing Files via Public-key Deniability | They analyzed various existing techniques and systems and proved that do not sufficiently solves the problems. So they designed a model, it is first sender-and-receiver deniable public-key encryption scheme.<br>That is both practical and is built from standard tools. Furthermore, they treat practical aspects of user collaboration and provide an | The existing deniable encryption schemes normally do not use standard tools. |

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. 3, Issue 11, November 2015

| | | | |
|---|---|---|---|
| | | implementation of a deniable shared file system, DenFS. To perform this task, the trusted agent needs to know the password used to protect the deniable files. | |
| Elaine Barker, et al. 2012 | Recommendation for Key Management | This provides information for end users regarding application options left under their control in normal use of the application. Finally, the system provides guidance when using the cryptographic features of current systems. This term is used to indicate an important recommendation. Ignoring the recommendation could result in undesirable results. | It may not always reflect a comprehensive view of current products and technical specifications. |

Table 1 literature study

## IV. PROPOSED WORK

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 the content of the data copy we can obtain the key. After key generation process and data encryption process, users can hang on to the keys. Then the user sends the cipher text to the cloud environment. Ever since encryption is deterministic, the same data copies will generate similar convergent key and the identical cipher text. This permits the cloud to perform de duplication over the cipher texts. Cipher texts are able to decrypt by the corresponding users' with their convergent keys. Convergent encryption practical is to efficiently and reliably manage a huge number of convergent keys.

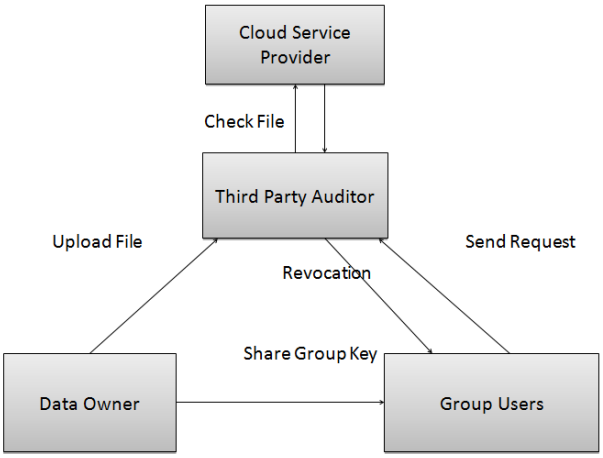


Fig. 1. Architecture of a proposed system

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. 3, Issue 11, November 2015**

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.

## V. CONCLUSION

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.

## REFERENCES

[1] OpenSSL Project. [Online]. Available: http://www.openssl.org/
[2] NIST's Policy on Hash Functions, Sept. 2012. [Online]. Available:http://csrc.nist.gov/groups/ST/hash/policy.html.
[3] AmazonCase Studies. [Online]. Available: https://aws.amazon.com/solutions/case-studies/#backup.
[4] P. Anderson and L. Zhang, ''Fast and Secure Laptop Backupswith Encrypted De-Duplication,'' inProc. USENIX LISA, 2010,pp. 1-8.
[5] M. Bellare, S. Keelveedhi, and T. Ristenpart, ''Message-LockedEncryption and Secure Deduplication,'' inProc. IACR CryptologyePrint Archive, 2012, pp. 296-3122012:631
[6] G.R. Blakley and C. Meadows, ''Security of Ramp Schemes,'' inProc. Adv. CRYPTO, vol. 196, Lecture Notes in Computer Science,G.R. Blakley and D. Chaum, Eds., 1985, pp. 242-268.
[7] A.T. Clements, I. Ahmad, M. Vilayannur, and J. Li, ''Decentralized Deduplication in San Cluster File Systems,'' in Proc.USENIX ATC, 2009.
[8] J.R. Douceur, A. Adya, W.J. Bolosky, D. Simon, and M. Theimer,''Reclaiming Space from Duplicate Files in a Serverless Distributed File System,'' inProc. ICDCS, 2002, pp. 617-624.
[9] Dario Catalano, Dario Fiore," Vector Commitments and their Applications", NSF grant CNS-1017471.
[10] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring," Provable Data Possession at Untrusted Stores", October 29–November 2, 2007, Alexandria, Virginia, USA.Copyright 2007 ACM 978-1-59593-703-2/07/0011
[11] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg,''Proofs of Ownership in Remote Storage Systems,'' in Proc.ACM Conf. Comput. Commun. Security,Y.Chen,G.Danezis,and V. Shmatikov, Eds., 2011, pp. 491-500.
[12] D.Harnik, B.Pinkas, A.Shulman-Peleg, ''Side Channels in Cloud Services: Deduplication in Cloud Storage,''IEEE SecurityPrivacy, vol. 8, no. 6, pp. 40-47, Nov./Dec. 2010.
[13] S. Kamara, K. Lauter, ''Cryptographic Cloud Storage,'' in Proc. Financial Cryptography: Workshop Real-Life Cryptograph. Protocols Standardization, 2010, pp. 136-149.
[14] M. Li, ''On the Confidentiality of Information Dispersal Algorithms and their Erasure Codes,'' inProc. CoRR, 2012, pp. 1-4abs/1206.4123.