International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

SECURE PRIVACY PRESERVING BATCH AUDITING MECHANISM IN CLOUD STORAGE

1.K.MUKESH 2. S.AYYAPPAN 3. N.ROHITH 4. Mrs.K.RAJAMMAL,M.E,(Ph.D).

1,2,3 Final Year Student, 4 Assistant professor
Department of Computer Science and Engineering
E.G.S Pillay Engineering College(Autonomous),Nagapattinam.

Abstract: ***There is a need to create an efficient public auditing protocol that gets around the shortcomings of the current auditing system. The suggested solution is designed to allow TPA to regularly or on- demandly verify the accuracy of cloud data without having to download the complete database or place an additional online strain on cloud users or cloud servers. It ensures that no data material during the auditing process is disclosed to TPA. It preserves the secrecy, integrity, and accuracy of stored data. The data owner, cloud server storage, and TPA are the three fundamental components of the proposed approach. The user or data owner is in charge of dividing the file into blocks, using the AES algorithm to encrypt them, producing an MD-5 hash value for each, concatenating hashes, and creating an AES signature on it. The encrypted file blocks are kept on the cloud server.***

Keywords: Public auditing, TPA (third party auditor), AES algorithm, MD-5 Hash values, AES signature.

1.INTRODUCTION

Public auditing suggest an unique privacy-preserving method that permits open auditing of shared data kept in the cloud. To compute the verification metadata necessary to audit the accuracy of shared data is specifically use ring signature. With the help of public verifiers who can effectively check the integrity of shared data without downloading the complete file are able to do so without learning the identity of the signer on each block. Furthermore, rather than validating each auditing work separately, our mechanism is able to conduct many auditing tasks at once**.**

The proposed method is a public auditing tool for cloud-based shared data that protects privacy. Added homomorphism authenticators using ring signatures such that a public verifier can audit shared data integrity without having to retrieve all of the data, but it is unable to determine who signed each block. Further enhance our mechanism to handle batch auditing in order to increase the effectiveness of confirming numerous auditing task.

AES is an unchanging alternative to the feistel cypher. The "substitution-permutation network" is supported. It consists of a number of connected operation, some of which require swapping inputs for particular outputs and others of which entail moving bits about. It's interesting to note that AES uses bytes rather than bits for all of its calculations. As a result, AES considers a plaintext blocks 128 bits to be sixteen bytes. For use as a matrix, these sixteen bytes are arranged in four columns and four rows.

2.LITERATURE REVIEW

The challenges surrounding public auditing prevention have been addressed by numerous researchers. The research of [1], privacy-preserving public auditing system for data storage security in Cloud Computing**,** It is provably secure and highly efficient, the techniques are implemented, (Homomorphism linear authenticator and random masking using MAC). There are challenges in implementation of this concept, The individual auditing of these growing tasks can be *time consuming* and unmanageable.

The Ranking method, and Symmetric key Encryption techniques is used in [2], The effective and safe ranked multi-keyword search on the encrypted remote database paradigm, which protects database users' privacy. The difficulty this method encounters is the extra network traffic is caused by them obtaining all files with the requested keyword.

The Ring signature techniques is used in [3], To calculate the verification data required to audit the integrity of shared data to use ring signature. The difficulty this method encounters is Since the identities of signers on shared data may signal that a certain user in the group or a particular block in shared data is a more lucrative target than others, it is important to protect identity privacy from the TPA.

The Resigned techniques is implemented in [4], A novel, effective user revocation system with public auditing for shared data in the cloud. The Remote Data Checking technique is used in [5], For network coding-based distributed storage systems that depend on untrusted servers, a secure and effective RDC scheme is needed.

The RSA Algorithm is used in [6], With the same security, signatures in our system are around the size of typical RSA signatures. The PDP(Provable Data Possession) and Signature technique is implemented in[7], By using a security mediator, the decouples the proved data possession technique from the anonymity protection mechanism.

3.PROPOSED METHODOLOGY:

The proposed method is a public auditing tool for cloud-based shared data that protects privacy to build homomorphism authenticators using ring signatures so that a public verifier can check the integrity of shared data without having to download the entire file, but it is unable to determine who signed each block.

Further extend our mechanism to support batch auditing in order to increase the effectiveness of verifying multiple auditing tasks to keep research two intriguing issues for our upcoming work. One of them is traceability, which refers to the group manager's capacity to, in certain exceptional circumstances, divulge the signer's identity based on verification metadata.

SMTP Protocol used for sending cause-and-effect e-mail over the internet; It stands for "Simple Mail Transfer Protocol". The client uses SMTP to send a message to the mail server, which then relays it to the appropriate receiving mail server using the same protocol. SMTP is essentially a series of instructions that authorise and control the transmission of electronic messages.

4.TECHNIQUES USED IN PROPOSED SYSTEM:

4.1 AES: The Substitution permutation network design principle forms the foundation of AES. Both the hardware and the software are quick. AES does not employ a Feistel network, in contrast to DES, its predecessor. Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits, as opposed to AES, which has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

The key size has no theoretical upper limit, block size has a maximum of 256 bits. AES uses a 4 by 4 column-major order byte matrix known as the state to operate (versions of Rijndael with a larger block size have additional columns in the state). A special field is used for the majority of AES calculations. The AES cypher is defined as a number of transformation rounds that are repeated until the input plaintext is transformed into the desired final output of ciphertext. There are several processing steps in each round, one of which is dependent on the encryption key. Using the same encryption key, a series of reverse rounds are used to convert the ciphertext back into the original plaintext.

4.1.1 DIAGRAM:

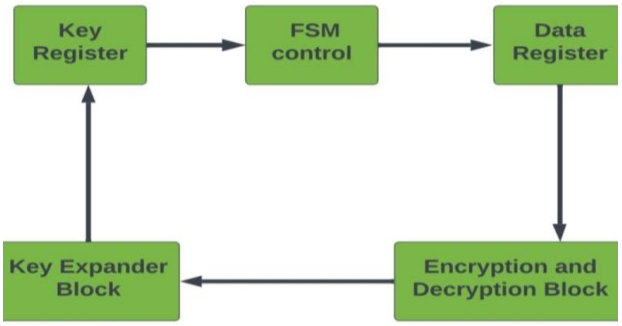


Figure 4.1.1 AES Archietecture

4.2 MD-5: The 128-bit message digest produced by the MD5 method, which is used to verify data integrity, is said to be as unique to the particular data as a fingerprint is to the particular

person. The message input can be any length message. MIT Professor Ronald L. Rivest created the MD5 algorithm for use in digital signature applications, which demand that, in a public key cryptosystem, big files must first be compressed using a safe manner before being encrypted with a secret key. Request for Comments (RFC) 1321 from the Internet Engineering Task Force (IETF) lists MD5 as a standard. The standard states that it is "computationally infeasible" for any two messages that have been entered into the MD5 algorithm to produce the same message digest as the output or for a bogus message to be produced by misinterpreting the message digest. Rivest's third message digest technique is called MD5.

4.2.1 DIAGRAM:

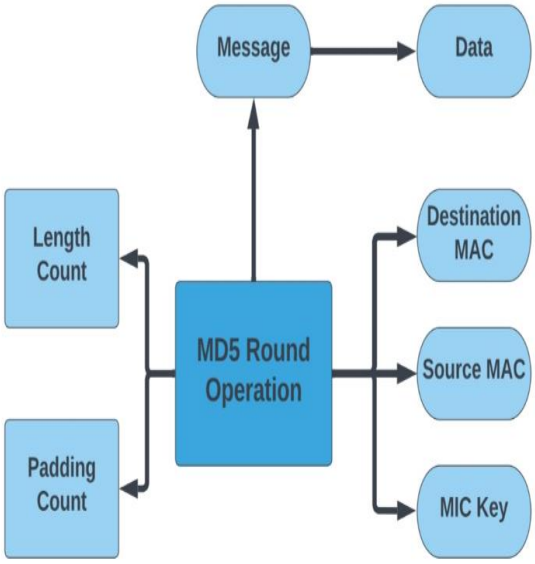


Figure 4.2.1 MD-5 architecture

4.3 BATCH AUDITING:

With the establishment of privacy-preserving mechanism, the TPA is now able to manage numerous audits simultaneously under the delegation of various users. These specific audits for the TPA can be very time-consuming and ineffective. It is more advantageous for the TPA to batch these various duties together and audit all K auditing delegations on K unique data files from K different users at once. In order to accommodate this natural requirement to slightly alter the protocol in the case of a single user. This results in the consolidation of K verification equations (for K auditing tasks) into a single one. In addition to enabling TPA to complete several auditing jobs at once, batch auditing significantly lowers TPA's computation costs.

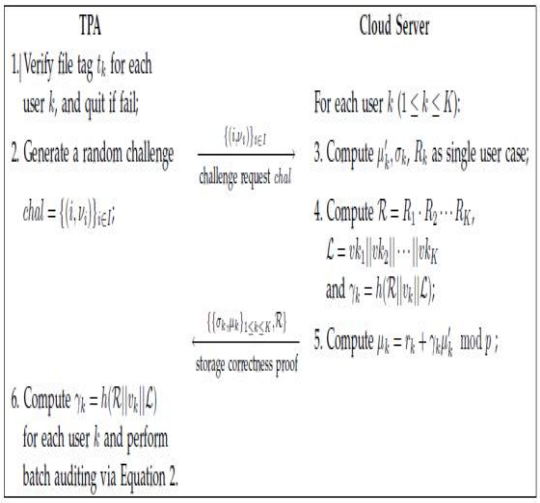


Figure 4.3.1 Batch Auditing Protocol

4.3.1 Batch Auditing Efficiency:

A batch auditing asymptotic efficiency analysis that only takes into account the overall number of pairing operations. However, Practically speaking, extra less expensive operations like modular exponentiations and multiplications are needed for batching. The amount of sampled blocks, or various sampling strategies, is another variable factor that influences batching efficiency. It remains to be seen whether the advantages of eliminating pairings outweigh these extra operations considerably. where the number of auditing tasks is raised from 1 to roughly 200 with intervals of 8, to obtain a full picture of batching effectiveness. As a starting point for the measurement, the performance of the equivalent non-batched (individual) auditing is offered.

4.3.2 Comparison on auditing time:

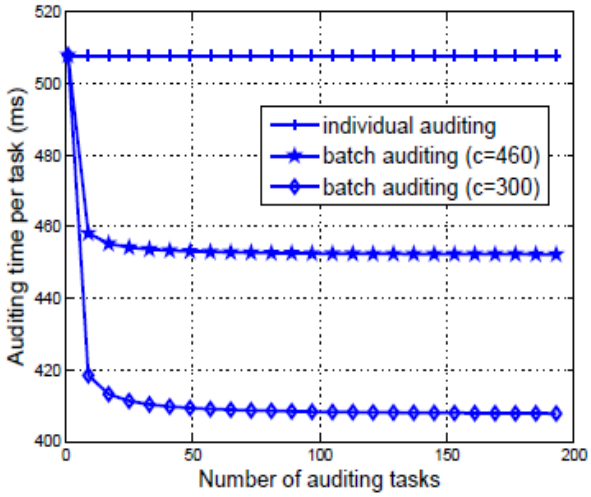
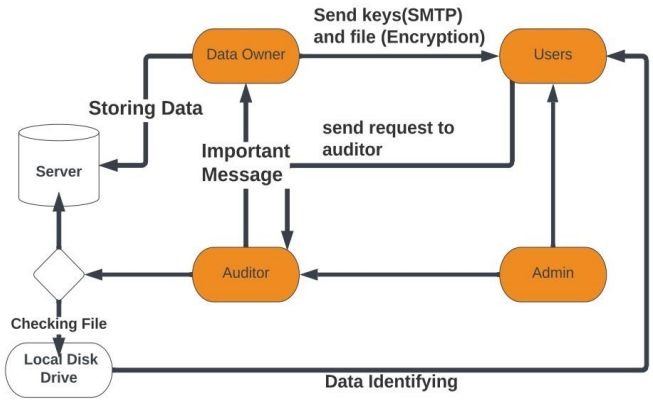


Figure 4.3.2 Auditing time between multiple and individual auditing

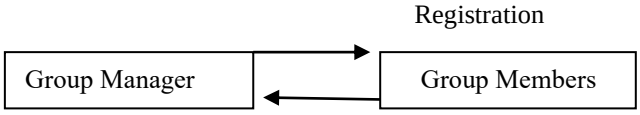
Duration comparison between batch and individual auditing. The overall auditing time divided by the number of tasks equals the per task auditing time.many duties. To remove the straight curve for individual auditing when c=300 for the sake of clarity.

5.ARCHITECURE DIAGRAM :



5.1.USER REGISTRATION:

For the registration of user with identity ID the group manager randomly selects a number. Then the group manager adds into the group user list which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.



5.2 PUBLIC AUDITING:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, The proposed technique to uniquely integrate the Homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF). The proposed scheme is as follows:

- Setup Phase
- Audit Phase

5.3 SHARING DATA:

The canonical application is data sharing. The public auditing property is especially useful to expect the delegation to be efficient and flexible. The schemes enable a content provider to share data in a confidential and selective way, with a fixed and small ciphertext expansion, by distributing to each authorized user a single and small aggregate key.

5.4 INTEGRITY CHECKING:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now to show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. To adopt

this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics. The user download the particular file not download entire file.

6.RESULT:

The result of the public auditing mechanism that the data and information are protected by the symmetric key encryption. When the client or data owner request for data auditing to the TPA, it immediately request for the encrypted data from the cloud server. After receiving the data, it generated the hash value for each block of encrypted files. It uses the same MD-5 algorithm which was used by client. It later concatenate those hash values and generates a AES signature for that file. In the Verification process, the signature generated by TPA and the one stored in the TPA which is provided by the data user are compared by the TPA. By this method the privacy of the data are preserved by this mechanism.

7.CONCLUSION:

In this paper the data security is improved and multiple auditing task can be performed through batch auditing. The use of ring signature preserves the identity of the data owners and data privacy is maintained. Data stored in the cloud can't be leaked easily and the auditor can view and verify the records without retrieving them. Performance of batch auditing mechanism is better when compared to the existing methods and suitable for mining and storing large amount of data.

8.REFERENCE:

1. privacy-preserving public auditing system for data storage security in Cloud Computing (2009),(eprint.iacr.org). Cong Wang, *Student Member, IEEE,* Sherman S.-M. Chow, Qian Wang, *Student Member, IEEE,*KuiRen, *Member, IEEE,* and WenjingLou,*Member, IEEE]*(https://eprint.iacr.org/2009/579)

2. Efficient and Secure Multi-Keyword Search on Encrypted CloudData(2012)1Y. Prasanna, 2Ramesh, (https://dl.acm.org/doi/10.1145/2320765.2320820).

3.Privacy-Preserving Public Auditing for Shared Data in the Cloud(2022), **(**Boyang Wan Baochun Li and Hui Li Email:{bywang,bli}@eecg.toronto.edu, lihui@mail.xidian.edu.cn) https://eprint.iacr.org/2009/579.pdf

4. Public Auditing for Shared Data with Efficient User Revocation in the Cloud (Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE)(2017), https://www.ijarnd.com/manuscripts/v2i5/V2I5-1139.pdf.

5.Remote Data Checking for Network Coding-based Distributed Storage Systems**(**Bo Chen, Reza Curtmola Department of Computer Science New Jersey Institute of Technology {bc47,crix}@njit.edu, Giuseppe Ateniese, Randal Burns Department of Computer Science Johns Hopkins University {ateniese, https://web.njit.edu/~crix/publications/acm-ccsw10.pdf .

6. Short Group Signatures(Dan Boneh1,?, Xavier Boyen2, and Hovav Shacham3 1 Stanford University, dabo@cs.stanford.edu 2 Voltage Security, xb@boyen.org 3 (2004), https://link.springer.com/chapter/10.1007/978-3-540-28628-8_3.

7. Storing Shared Data on the Cloud via Security-Mediator **(**Boyang Wang†§, Sherman S. M. Chow‡, Ming Li§, and Hui Li(2013), https://www.researchgate.net/publication/261465064_Storing_Shared_Data_on_the_Cloud_via_Security-Mediator.

8.The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.

9.B. Wang, B. Li, and H. Li, "Certificate less Public Auditing for Data Integrity in the Cloud," Proc. IEEE Conf. Comm. and Network Security (CNS'13), pp. 276-284, 2013, https://ieeexplore.ieee.org/document/6682701.

10.C. Wang, S.S. Chow, Q. Wang, K. Ren , and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

11.B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.