JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 5, ISSUE 06, 2018

Dependable Argument Auditing for Allot Cloud Data with Message Authentication Code

[1]Sujit Kumar Panda, [1]Sasmita Pani

[1]Professor, [1]Dept. of CSE

[1]Gandhi Institute for Technology, Bhubaneshwar, India

ABSTRACT: In modern days the cloud data storage is present generations that promote the secure remote data auditing. The existing system considers the problem secure and efficient public integrity auditing for shared dynamic data storage. Cloud data assign stores data in the cloud as well as distribute data number of users. We found the collusion attack in the exiting model .An efficient public integrity auditing method with secure group user revocation based on vector commitment plus verifier total revocation group signature. We find the proposed a new public integrity auditing function to help of Message Authentication Code (MAC) generation and symmetric cryptographic algorithm. The main aim of this paper is to improve privacy and an efficient cloud data storage model to reduce the bandwidth and to improve the data security. This work modify to number groups to access the data. We deplore scheme for group signature. The cipher text support public checking and efficient user revocation in properties like confidently, efficiency, count ability and traceability. Finally we compare our algorithm with old which shows good result in security. The experimental results are analyzed and evaluated in terms of computation time, block size, key size, number of rounds and cycles per block.

Index Terms: *Data integrity, Public auditing, User revocation component, Cloud Computing, Message Authentication Code (MAC), Message Digest (MD), Symmetric Key Cryptography, Public Integrity Auditing, Security and Data Storage.*

1. Introduction

The improvements and enhancements in cloud computing motivates enterprises and also organizations to outsource data to third party cloud service providers (CSP's) which will result in improvements in the data storage limitation of resource constrain local devices. In market already some cloud storage services are available like simple storage service (S3) online data backup services of Amazon and software like Google Drive, Drop box, Mozy, Bitcasa and Memopal built for cloud application. Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid [1]. The criticisms about it are mainly focused on its social implications. This happens when the owner of the remote servers is a person or organization other than the user, as their interests may point in different directions, for example, the user may wish that his or her information is kept private, but the owner of the remote servers may want to take advantage of it for their own business [4]. 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 [2]. 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. Cloud computing is a new paradigm that is mainly used to provide an economic resource utilization over the internet [5]. It is a method of computing in which the users can increase or decrease their computing resources. Generally, the cloud contains three models as shown Fig 1.

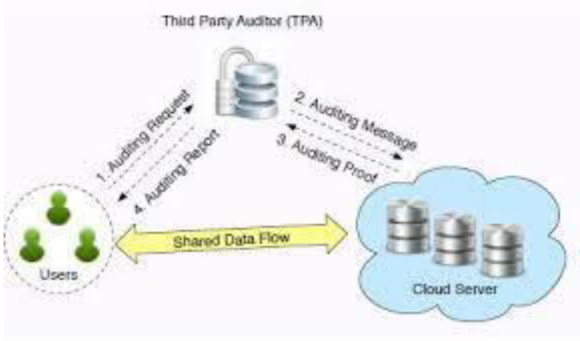


Fig1. Types of cloud security data

The major contributions are as follows:

- The secure and efficient shared data integrate auditing process is explored for cipher text database with the help of multi-user operation [3].

- Here, an efficient data auditing scheme is proposed for providing data integrity by incorporating the primitives of victor commitment, asymmetric group key agreement and group signature [7].

2. Related Work

A large number 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 [6]. They proposed methodology to detecting a malicious server, in an efficient result verification method. YongjunRen, (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 [8]. 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 [10]. The asymptotic complexity in computations were more in key generation methodologies. Gentry and Halevi [12] discussed the implementation of Fully Homomorphism Encryption (FHE). The complete working of any encryption methodologies required the functionality called bootstrapping. They provided the optimization in key generation that reduced the complexity with n-dimensional lattices. In a data storage outsourcing services, the permission assigned to the data owner to check whether they stored data correctly or not [9]. In previous work focused on TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data and introduce no additional on-line burden to the cloud user. This paper entirely different compare with previous in the case of privacy. Privacy preserving public auditing for data storage security in cloud computing [11], by C. Wang, Q. Wang, K. Ren, and W. Lou utilize and uniquely combine the public key-based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. In this design, propose to uniquely integrate the homomorphic authenticator with random masking technique. In this protocol, the linear combination of sampled blocks in the server’s response is masked with randomness generated by a pseudo random function (PRF). By using random masking, [13] The TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user’s data content, and no matter how many linear combinations of the same set of file blocks can be collected. A public verifier, such as a third-party auditor providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server. When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data.

Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and- response protocol between a public verifier and the cloud server [15].

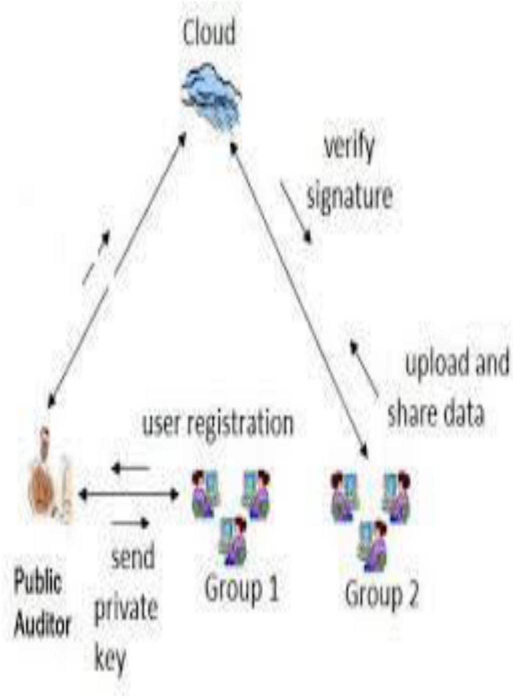


Fig2. System Flow

3. Proposed Work

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 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. [5] 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. [9] 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 [14].

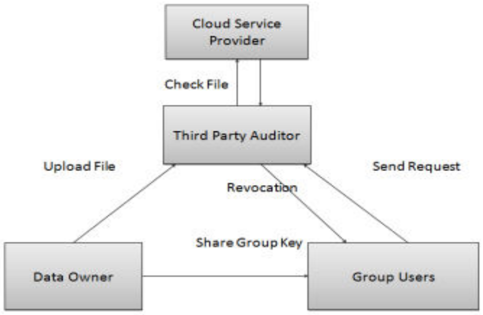


Fig3. Architecture of a proposed system

The proposed cloud storage model the problem of designing public integrity auditing based shared dynamic data with group user revocation is analyzed. The main contributions of this paper are listed as follows: [6]

- An efficient and secure public integrity auditing scheme is proposed for cipher-text base with the help of multi-user operation.
- The primitives of victor commitment, group signature and asymmetric group key agreement are integrated.
- The new features like, traceability and countability are provided at the time of auditing.

It is identified that the upload file is duplicated. Otherwise, it will divided into various blocks, after that the availability of the blocks is also verified. If the block is not exists, it will be given to the Cloud Service Provider (CSP). Hence, the file is downloaded from the server and to access that file, the hash key and data blocks are need to be decrypted. [15] In this work, the two different algorithms such as, Message Digest Code. Message Authentication Code (MAC) algorithm is used for code generation. Then, the symmetric key cryptography algorithm is used for encryption and decryption processes.

Algorithm – MAC Algorithm

Input: Block of file B = (B1, B2, B3 … BN}

Step 1: Generate the hash key;

Step 2: Encrypt the data block with the help of hash key;

Step 3: Generate the tag and hash key from the content of the file;

Output: Obtain the decrypted file with the help of hash key;

1. H(M) = K (Key Generation)
   Where,
   M= Input file
   H(M)=Hash value of file
   K= Hash Key
2. E(K, M)=C (Encryption)
   Where.
   M-File,
   K-Hash Key,
   E-Encryption
   C-Cipher Text
3. Tag(M)=T (Tag Generation)
   Where,
   M-File
   T-Tag from File M

4. Cipher Text Database

In cloud storage outsourcing environment, the outsourced data is usually encrypted database, which is usually implicitly assumed in the exiting academic research. Actually, our scheme could support the auditing of database of both plaintext and cipher text database [5]. It is not straightforward to extend a scheme to support encrypted database. In order to achieve the confidentiality of the data record mx, the client can use his/her secret key to encrypt each mx using a encryption scheme. When there is only one user in the group, the user only needs to choose a random secret key and encrypt the data using a secure symmetric encryption scheme. When the scheme needs to support multi- user data modification, while at the same time keeping the shared data encrypted, a shared secret key among group users will result in single point failure problem [3]. It means that any group user leak the shared secret key will break the confidentiality guarantee of the data. To overcome the above problem, we need to adopt a scheme, which could support group users data modification. Exponentiation (BDHE) assumption in the standard model according to the ASGKA protocol, we consider the case of encrypted database (x, cx), where x is an index and cx is the corresponding cipher value. We provide the detailed changes upon our scheme to support encrypted database [16].

1) In the Setup phase, the scheme has to run the key agreement of ASGKA for the group users. Then the database DB = (i,mi) is encrypted by the group key gpk of data owner. Finally, the stored database is a cipher text database DB = (i, ci).

2) In the second step of the Update phase, a group user firstly decrypts the record ci using the ASGKA secret key gsk[∗] to get plaintext database DB = (i,mi). Then, update the data to m′i, and later encrypt the data with the public key gpk of ASGKA scheme to get the new encrypted database DB = (i, c′ i)

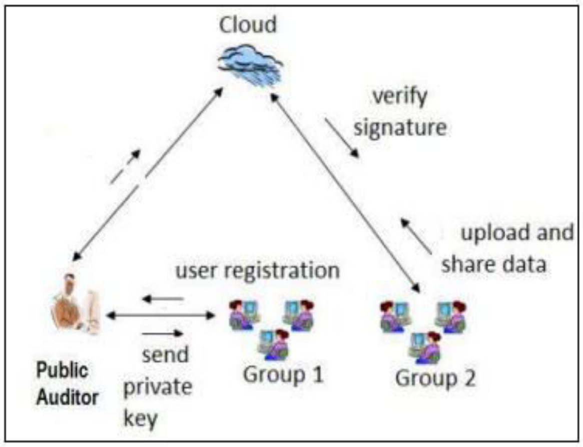
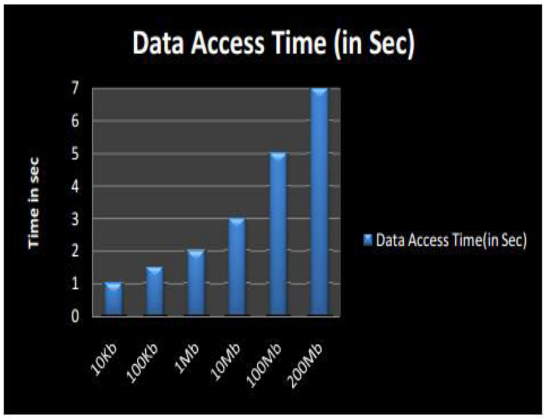


Fig 4. Cipher Text Model

The system is based on proxy re-signature concepts. Blaze et al first proposed the concept of proxy re-signature in [12]. Proxy signature is a digital signature scheme where original user delegates his signing capability to a proxy signer, and then the proxy signer performs message signing on behalf of the original signer [9]. In simple word it allows semi-trusted proxy to work as a converter of signatures between two users belonging to same group

5. Result

We have provided a scheme of auditing the integrity of the shared and dynamic cloud data along with group user revocation. The auditing of the data integrity is secure and reliable. In this paper, the concept of authorized data duplication was proposed to achieve the data security by including differential privileges of users in the duplicate check. The data and associated key primitives consume the space in cloud architecture refers block size. An algorithm effectiveness decided by the low space consumption. Fig 5 shows the variation of block size for both the proposed and existing AES method. The block size for AES is 128 bits and for proposed symmetric cipher block is 65 bits. The optimal steps reduction in proposed work offers 49. 21% reduction in block size. This section demonstrates the implementation results and experimental performance analysis is carried out on the basis of revocation time and overall auditing time by implementing our proposed mechanism. Graphically presented analysis is most feasible analysis of our mechanism with the existing public auditor.



6. Conclusion

A new public integrity auditing scheme for cloud data storage for this purpose algorithms such as, Message Authentication Code (MAC) generation and symmetric key cryptographic techniques are used in this work. 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. The main objective of this paper is to reduce the bandwidth and to improve the content integrity in cloud data storage. Our novel design allows efficient user revocation operations to the cloud. Because of keys generated for the data not a user. In addition, scheme allows aggregation of integrity auditing operations for multiple tasks (files) through our batch integrity auditing technique. When compared to other algorithm key size is very small, it is not able to hack easily. It is used for efficient revocation without updating private keys of remaining users. Cloud public verifier plays an important role when dealing with security aspects of cloud. In this paper, we have proposed a new public auditing mechanism for cloud for efficient user revocation while maintaining shared data integrity which allows cloud to re-sign blocks signed by revoked user. In future, concentrate on key management, how to revoke the private keys from the group members

7. Future Work

Designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability is still open. Future work includes improving performance of the overall system using distributed cloud. Even though there is greater performance and efficiency in this mechanism, there is a problem of traceability in this system which is been considered to be continued in future work. Since this mechanism is based on aggregate signatures which are group signatures with compressed storage, the identity of the signer is protected. Proxy re-signature can be carried out on two or more cloud servers which reduces risk of increased in data or users. It also helps in improving security factors

References

[1] Amazon. (2007) Amazon simple storage service (amazon s3). Amazon

[2] S Archana and Ananthi J, “Privacy-Preservation and Public Auditing for Cloud Data - A Survey”, International Journal of Science and Research (IJSR), Vol. 3, No. 10, October 2014, pp-1989-1992.

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT’03), pp. 416-432, 2014

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010

[5] 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

[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] 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] D. Catalano and D. Fiore, "Vector commitments and their applications, " in Public-Key Cryptography– PKC 2013, ed: Springer, 2013, pp. 55-72.

[12] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme,

[13] X. Jia and C. Ee-Chien, ―Towards efficient proofs of retrievability,‖ in Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '12, Seoul, Korea, 2012.

[14] D. Chaum and E. van Heyst, "Group signatures," in Proc. Of EUROCRYPT 1991, Brighton, UK, Apr. 1991, pp. 257–265.

[15] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,―Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing‖, Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

[16] H. Shacham and B. Waters, ―Compact Proofs of Retrievability,‖in the Proceedings of ASIACRYPT 2008. Springer-Verlag, 2008, pp.90–107.