International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Modified Public Auditing with Privacy Preservation for Shared Data in Cloud Computing

Jeur Nagaraj Shrikant[1], Pavan Kumar[2]

[1, 2]G.H.R.C.E.M Wagholi, Department of Computer Engineering Pune, Maharashtra, India

Abstract: ***Cloud data services, it is not only stored in the cloud but also multiple users to share the data across the common. The integrity of data and human cloud hardware/software failures is under suspicion because of the existence of Errors. Public shared data with the existing mechanism on the integrity of the audit will reveal confidential information essentially identity privacy public for verifiers. This paper have a novel privacy protection mechanisms shared data stored in the cloud can offer support to public audit. Shared data is necessary to verify the accuracy of the audit to calculate the metadata exploit ring signatures. These systems are shared with the public to identify each data block signature verifiers which efficiently retrieving the entire file without verifying the integrity of the shared data are kept private. In addition to this mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one and using multiple public verifier to improve the efficiency of auditing task and also using CP-ABE Algorithm between user and cloud server to and the protect user confidential data.The experimental results when sharing data integrity auditing effectiveness and demonstrate the efficiency of this system.***

Keywords: Public auditing, privacy-preserving, public Verifier, shared data, cloud computing.

1. Introduction

The CLOUD service supplier supply users efficient and scalable data storage services with a far lower marginal cost than ancient approaches. It is routine for users to leverage cloud storage services to share information with others in a group, as information sharing is getting as primary feature in most cloud storage offerings, as well as Dropbox,iCloud and Google Drive. The integrity of information in cloud storage, however, is subject to scepticism and scrutiny, as information keep within the cloud can easily be lost or corrupted correct to the unavoidable hardware/software failures and human errors. To do this matter even worse, the cloud service providers may be reluctant to inform users about data errors in order to avoid losing profits and to maintain the reputation of their services. And hence, the integrity of cloud information should be verified before any information utilization, like search or computation over cloud information. The regular approach for checking information correctness is to retrieve the complete information from the cloud, and so verify data integrity by checking the correctness of signatures or hash values of the complete data. [7] Particularly, this traditional approach is in a position to with success check the correctness of cloud information. However, the effectiveness of using this approach on cloud information is doubtful. The main reason is that the dimensions of cloud information are massive in general.Downloading the complete cloud information to verify data integrity may be result into wastage of resource, especially when information are corrupted within the cloud.[9] Besides, many uses of cloud information don't essentially want users to download the entire cloud information to native devices[4]. Its as a result of cloud providers, like Amazon, can give users computation services directly on large-scale information that already existed in the cloud. Recently, several mechanisms are planned to permit not solely data owner it however conjointly a public verifier to with efficiency Perform integrity checking while not downloading the entire knowledge from the cloud [10], that is remarked as public auditing. In these mechanisms, information is split into many little blocks, wherever every block is severally signed by the owner; and a random combination of all the blocks rather than the entire information is retrieved throughout integrity checking. A public verifies may be a knowledge user who would like to utilize the owners data via a public verifier or cloud who can give skilled integrity checking services [8]. Recently, several mechanisms have been proposed to allow not only a data owner myself, but also to a public verifier efficiently download without checking the integrity of performance Cloud, who is referred to as the public all data from auditing. These mechanisms, data are divided into many small blocks, where each blocks independently. Signed by owner; and all a random combination Instead of all data blocks have been taken during Integrity checking. A verifier may be data users who want to use the owners Cloud or a public verifier of data that Specialist integration services can provide a check. Further, the next step is an upgraded Wang et al. auditing mechanisms, so during the public cloud data, content auditing Disclosure of personal data of an individual user is not for any public verifiers.Unfortunately, the current public Solutions focus on the above mentioned auditing Personal data in the cloud.To believe that sharing information among multiple users is perhaps one amongst the foremost participating options that motivates cloud storage. More ever, it is necessary to make sure the integrity of shared information within the cloud is correct.Existing public auditing mechanisms will truly be extended to verify shared information integrity. A new important privacy issue introduced within the case of shared information with the employment of existing mechanisms is that the run of identity privacy to public verifiers.[1] For example, Alice and Bob work along as a bunch and share a enter the cloud. The shared file is divided into variety of little blocks, where every block is severally signed by one in all the two users with existing public auditing solutions. Once a block during this shared file is changed by a user, this user must give sign block victimization his/her personal key. Completely

Licensed Under Creative Commons Attribution CC BY

different blocks square measure signed by different users thanks to the modification introduced by these Two different users. After, so as to properly audit the integrity of the whole knowledge, a public friend must select the appropriate public key for every block. As a result, this public friend can inevitably learn the identity of the signer on every block thanks to the unique binding between AN identity and a public key via digital certificates below public key infrastructure (PKI).[12] Failing to preserve identity privacy on shared information throughout public auditing can reveal vital wind to public verifiers. Specifically, once performing arts several auditing tasks, this public admirer will first learn that Alice is also an additional vital role within the cluster as a result of most of the blocks within the shared file square measure continuously signed by Alice; on the opposite hand, this public admirer may also simply deduce that the eighth block could contain information of the next value, as a result of this block is usually changed by the two completely different users. So as to protect this wind, its essential and critical to preserve identity privacy from public verifiers during public auditing [13]. In this paper, the issue of confidentiality of shared data to solve unique privacy protection Oruta[1],public auditing mechanisms is proposed. In particular, To give a lot of in order that do not retrieve data complete a public champion while sharing information is to verify the integrity of the Oruta,To build authenticators ring homomorphism in signatures to use while unbroken non-public information shared in every block from general public champions is to identify the signatory. In addition, to do these mechanisms to support batch audit, which can display multiple auditing functions extend the side by side and the power of multiple auditing functions to improve verification [11]. Oruta that has been used and public at WWRL verifiers can protect the privacy of information from random masking is compatible with. In addition, for one of the last public auditing conjointly index hash table dynamic data to support the resolution to take advantage of it.

2. Literature Survey

i) B. Wang, B. Li, and H. Li [1], with cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to scepticism due to hardware or software failures and human errors. Many mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. Nevertheless, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information identity privacy to public verifiers.

ii) K. Ren, C. Wang, and Q.Wang [2], Cloud computing represents today are most exciting computing paradigm shift in information technology. Beside, privacy and security are perceived as primary obstacles to its wide adoption. Here, the authors motivate further investigation of security solutions and outline several critical security challenges for a trustworthy public cloud environment.

iii) D. Song, E. Shi, I. Fischer, and U. Shankar[3],offering strong data protection to cloud users while enabling rich applications is a challenging task. Researchers explore a new cloud platform architecture called Data Protection as a Service which pretty much reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance.

IV)B. Wang, M. Li, S.S. Chow, and H. Li [5], The emergence of cloud computing brings users abundant opportunities to utilize the power of cloud to perform computation on data contributed by multiple users. This cloud data should be encrypted under multiple keys due to its privacy concerns. However, existing secure computation techniques are either still far from practical or limited to single key. In this paper to designed two schemes to secure outsourced computation over cloud data encrypted under multiple keys.

v) R. Rivest, A. Shamir, and L. Adleman [6], an encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: Couriers or other secure means are not needed to transmit keys; therefore a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only they can decipher the message, since only they know the corresponding decryption key. A message can be signed using a private decryption key.

3. Problem Statement

Cloud service is commonplace for data to not only stored in the cloud but also shared multiple user however public auditing for such shared data. In existing system not secured data sharing between cloud and multiple user.in existing system is usage single public verifier the problem associated with this is common, as number of user increases single public verifier getting more loads.

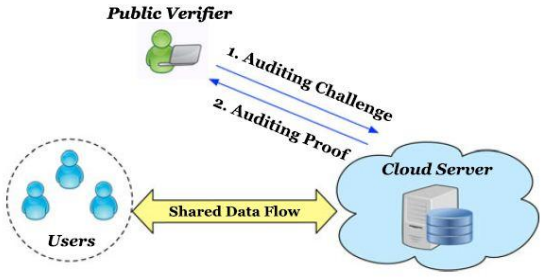

Figure 1: Architecture of Existing system

4. Proposed Approach Framework and Design

Licensed Under Creative Commons Attribution CC BY

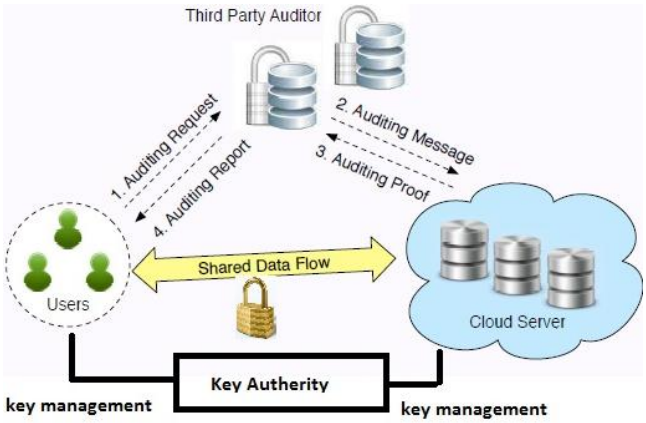

Figure 2: Architecture of proposal system

With our mechanism, the identity of the signer on each block in shared data is kept private from a multiple public verifier, who is still able to publicly verify the integrity of shared data without retrieving the entire file.Along with to provide security for sharing the data between user and cloud. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.

5. Proposed Algorithms

Propose In the addition to this the mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one and using multiple public verifier to improve the efficiency of auditing task and also using CP-ABE Algorithm between user and cloud server to and the protect user confidential data.The experimental results when sharing data integrity auditing effectiveness and demonstrate the efficiency of this system.for this purpose using three algorithms such as AES,SHA and CP-ABE.In that AES and SHA are used for to generate the public key and ring signature for each file.CP-ABE Algorithm between user and cloud server to and the protect user confidential data.This Algorithm does not allowed the Unauthorized users to access the file from cloud server.

5.1 CP-ABE Algorithms

Two methods in the fine-grained access control based on ABE first one is KP-ABE and second is CP-ABE. In KP-ABE, each of the private key attribute is link with an access structure is specifies which type of cipher texts the key is used to decrypt, and cipher text is labelled with a sets of attributes. In a CP-ABE system, a user's key is link with a set of attributes and an encrypt the cipher text will specifies an access policy over attributes. In KP-ABE constitution to realized the monotones access structures for key policies. The constitution is only proved the secure for the generic group model. To overcome this problem presented another constitution that is proved to be secure under the drastic standard model. Attribute-based encryption [ABE] means that encrypted access control. Cipher texts not necessary for encrypt to one particular user[9]. User private keys and cipher texts link with a set of attributes or a policy over the attributes. When A match in between the user's private key and the cipher text, then only decryption is possible.

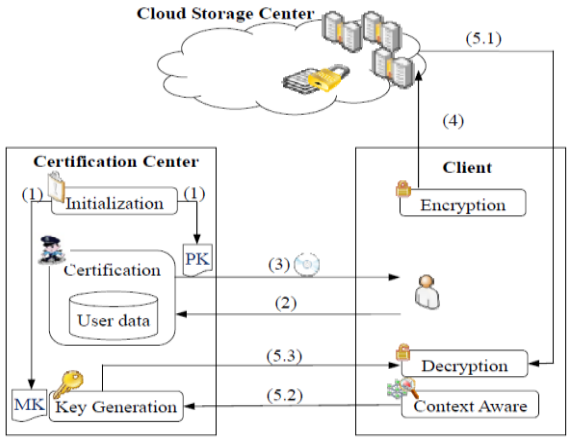

Figure 3: CP-ABE Algorithm structure.

a) **Initialized system**: The First the certification centre can generate the system security parameters like PK and MK, after transmitted PK to the user and MK to the key generation.
- First need to register for the user inputs ID and password to be log in the system.
- The user authentication unit should be verifies the CC in the first in first out manner, then distributes the security parameter
- like PK and the client element to the authorized users.
- The user can accessing or receiving the data or resources from the cloud storage centre.
- The context collector can collects the user's current contexts and transport or move to the key generation of the CC.
- The key generator of the CC generates decryption key according to MK and the get the contexts, and sends it to the decryption unit in the client. After decryption unit can be decrypt the resource.

b) **Context-aware:** Access control is Policy based on CP-ABE algorithm with context its awareness.

5.2 Secure Hash Algorithm

Secure Hash Algorithm is one of the most important cryptographic hash functions and SHA is short. File verification purpose use SHA-1 is smart to contrast the checksums created after running the algorithms and require two files for contrasting purpose. This SHA-1 is the second iteration of the cryptographic hash function and destroy the last SHA-0. An SHA-2 cryptographic hash function is prepared and also SHA-3 is being developed. SHA-256 transport an input messages into the 256 bits message digest[10]. SHA is use to generate the key signature.SHA having six steps.

Stage 1: Packaging Message: Input binary message is 1 and filled is 0 until length = 448 mod 512.Then attached 64-bit binary number. The filled message length is a Multiple of 512 bits, which decides how many '0' to be filled.
Stage 2: Parsing: The padded message is separate into the N 512-bit blocks.
Stage 3: Message Extension (Scheduler): Each 512 bit block can be split into 16 –bit words 32-bit words

Licensed Under Creative Commons Attribution CC BY

Stage 4: Message squeezing: The words from scheduler stage are then passed to the SHA squeezing function.
Stage 5: The algorithm is implemented by 64-cycle repeated each block.
***Stage 6*:** After 64 emphasis of the squeezing function, an median the hash value.

5.3 AES- Advanced Encryption Standard

In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. AES algorithm is used to provide security on the data stored. AES is symmetric encryption algorithm in which to encrypt the message sender uses public key of receiver and its private key is used by receiver to decrypt the message.

Begin
1. Data is stored on cloud server
2. Data is encoded
3. Verification of data is should be done by CSP using AES
4. **If** data is valid

Go To Module T

Else
Invalid data

End

Module T:

Begin
1. Checked the data stored.
2. **If** proof = direct then
Report = direct access

Else
Return {1, 0}
1: if integrity of data is verified as accurate
0: if integrity of data verified is improper

END

- AES is preferred over DES algorithm as it is more secure.
- AES data encryption is mathematically more efficient and elegant cryptographic algorithm. Key length option is the main strength of the algorithm. Time required to crack an encryption algorithm is directly related to the length of the key used to secure the communication. AES gives an option to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger as compared to the 56-bit key of DES.
- Block size of DES is small compared to AES
- A balanced Feistel structure is used by DES while substitution-permutation is used by AES.

6. Results

User can upload his file on cloud server and public verifier can generate the keys for each file.

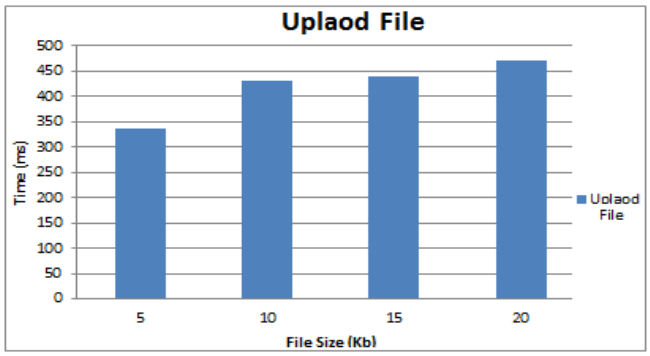

Figure 4: Upload the file in Cloud Server Graph

Public verifier can do the batch auditing and give keys for each file.

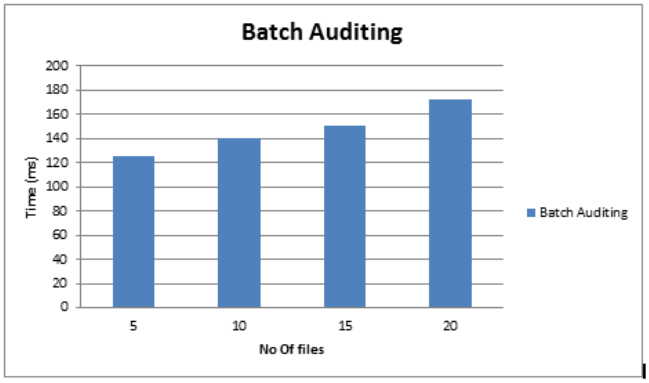

Figure 5: Batch Audting Graph

Public verifier can do the batch auditing and give keys for each file.using these keys user can easily encrypt the his file from cloud server.

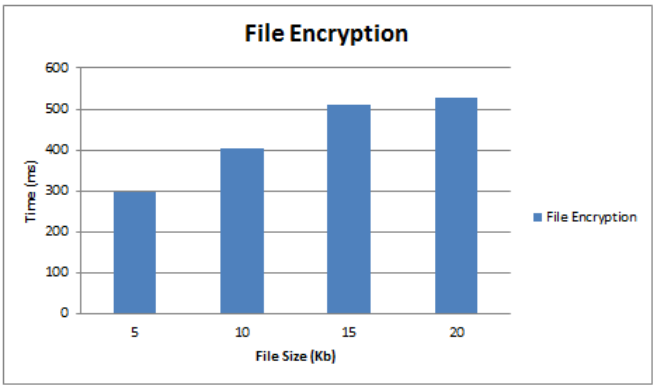

Figure 6: File Encryption Graph

Only valid user can decrypt the file from cloud server

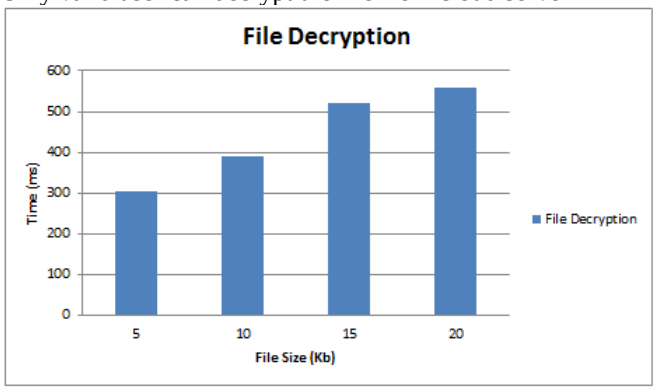

Figure 7: File Decryption Graph

Licensed Under Creative Commons Attribution CC BY

CP-ABE Algorithm will take less time for Encryption as compare AES Algorithm.

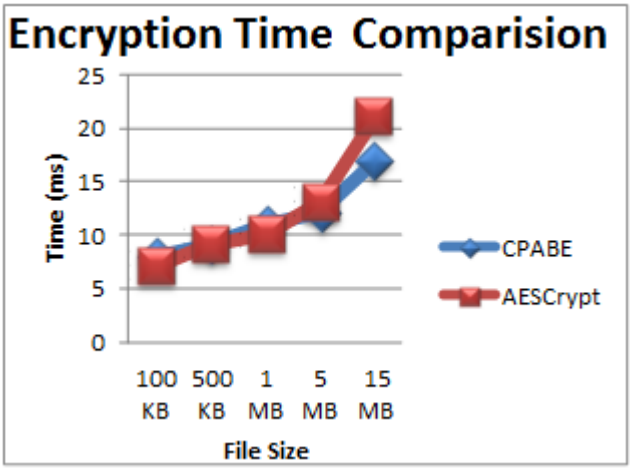

Figure 8: CP-ABE and AES Encrypt Graph

CP-ABE Algorithm will take less time for Decryption as compare AES Algorithm.

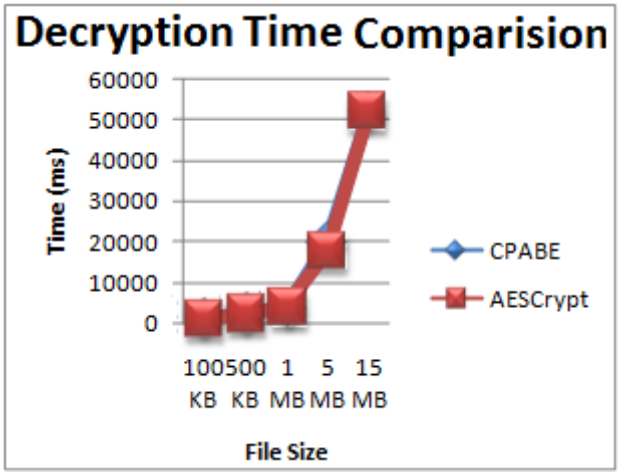

Figure 8: CP-ABE and AES Decrypt Graph

7. Conclusion

With our mechanism, the identity of the signer on each block in shared data is kept private from a multiple public verifier, who is still able to publicly verify the integrity of shared data without retrieving the entire file. using multiple public verifier to improve the efficiency of auditing task and also using CP-ABE Algorithm between user and cloud server to protect the user confidential data

References

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[3] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[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, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[10] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, 2012.

[12] 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.

[13] 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.

Licensed Under Creative Commons Attribution CC BY