International Journal of Computer Science and Engineering Communications
Vol.3, Issue 3, 2015, Page.1165-1170
ISSN: 2347–8586
www.scientistlink.org

Public Auditing and Data Dynamics for Cloud Storage

[1]Elakkiya.B, [2]Suvitha.S, [3]Vani Parvathi.G, [4]Saranya.A, [5]Sindhu.S
[1,2,3]UG Scholar, [4,5]Assistant professor
Department of Computer Science,
Rajalakshmi Institute of Technology Chennai,India
[1]elakkiya.b.2011.cse@ritchennai.edu.in,[2]suvitha.s.2011.cse@ritchennai.edu.in,[3] vaniparvathi.g.2011.cse@ritchennai.edu.in, [4]saranya.a@ritchennai.edu.in, [5] sindhu.s@ritchennai.edu.in

Abstract

Cloud Computing is emerging as the next-generation architecture of Information Technology Enterprise. Data is accessed from data center which act as a centralized server. Companies are rapidly shifting to the cloud to use the best resources that are available. The existing systems support either data dynamic operation or public verifiability at an instance of time .To ensure secured data integrity proposed system consider the task of Third Party Auditor which eliminates the involvement of client when auditing to identify the data stored in the cloud. Data dynamics provide data operations for insertion, deletion and modification on the block. To overcome the pitfalls in existing system, Multiple Auditing Mechanism (MAM) is used. Keys are generated by public key algorithm. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud. Scalability can be improved by reducing the number of re-signing keys and public auditing for multiple auditing tasks.

Keywords—*Public Auditing,Data Dynamics,Third party Auditor,Batch Auditing*

1 Introduction

With advanced computational technology over Internet Cloud Computing has become a new buzz in recent time. Users can access the data stored in the cloud and simultaneously share their outsourced data. To improve the storage limitation, enterprise and organization outsource their data to Cloud Service Provider (CSP). Cloud computing ensures more security challenges to ensure the integrity of outsourced data. Various new ideas give assurance to Data integrity and confidentiality in better way. The best way to protect the confidential data in cloud is to use encryption method for data storage and retrieval. Almost all cloud service providers support encryption for storing the data. Since the cloud servers may return an invalid result in some cases, such as server hardware or software failure, human maintenance and malicious attack, new forms of assurance of data integrity and accessibility are required to protect the security and privacy of cloud user's data. The new cooperation network model in cloud makes the remote data auditing schemes become infeasible, where only the data owner can update its data. Obviously, extending a scheme with an online data owner to update the data for a group is inappropriate for the data owner. It will cause tremendous communication and computation overhead to data owner, which will result in the single point of data owner. The major security issue is confidential data stored in cloud that is outsourced, leading to number of issues related to accountability and handling of personal identifiable information. This makes the security for data access more necessity.

2 Literature Review

Cloud encryption capability of service provider must match sensitivity level of data being stored [10]. Juels and Kaliski[8] proposed a model on Proofs of Retrievability (POR) one of the first most important attempts to formulize the notion "guaranteed remotely and reliable integrity of the data without the retrieving of data file". Hovav Shacham and Brent Watersy [4] gave a new model for POR enabling verifiability of unlimited number of queries by user with reduced overhead. This method proposed two proofs of verifiability. First scheme builds BLS Signatures and it is secure in random oracle model has its shortest query and response of any proof of retrievability with public verifiability. Second scheme which builds elegantly on pseudorandom functions and its secure has the shortest response of any proof of retrievability scheme with private verifiability but a longer query. Later Bowels and Juels[7] gave a theoretical model for the implementation of POR, but all these mechanisms proposed were weak in security because they all work for single server.

Therefore Bowels [1] in their further work gave a HAIL protocol extending the POR mechanism for multiple servers. Priya Metri and Geeta Sarote[2] proposed a threat model to overcome the threat of integrity and provide data privacy for storing the data in cloud. It provides Third Party Auditor (TPA) and digital signature scheme for reliable data retrieval. Ateniese, et al. [5] provide Provable Data Possession (PDP) mechanism which verifies the integrity of outsourced data, detecting all kind of errors occurring in data but doesn't ensure complete data retrieval. In their later work Atienies and Pietro[6] proposed a scheme which overcome all problems in PDP, but the basic problem on both proposed system is they work on single server. Therefore, later Curtmola[13] proposed a scheme to ensure data reliability and retrievability of data for multiple servers. Filho[3] proposed a RSA-based hash data integrity mechanism for peer-to-peer file sharing networks and exponentiation of complete data file is done, but this mechanism can be followed for the files and data of large size, and also this mechanism focuses on the static data files and not on files being dynamic in nature having localization problem. Cao, Lou[14] recently proposed an LT code based secure cloud storage mechanism this mechanism can avoid high decoding computational costs for users. Public Auditing in cloud is of greater challenge so that user can resort to a TPA.TPA check the outsourced data integrity. There are two categories: private Auditing and Public Auditing. Public Auditing allow client or data owner can correct the data stored while keeping no secured information. Private auditing works within an organization to make the business more efficient. The advantages of auditing are to detect, prevent errors and maintain the database regularly. Auditing should not bring any new vulnerabilities towards privacy of data and no additional online burden to user [11].Based on the proxy re-signature method designs a public auditing scheme for data storage with proficient user revocation in cloud. The original user can acts as a group manager and able to retract the users if necessary .They provide two servers for data storage and signature storage to support their mechanism. For each block of data to be stored in cloud server, data owner is assigned with a signature that includes a block identifier, signature identifier and the integrity of data relies in the correctness of all the signatures. In a cloud if a user modifies a single block including insertion or deletion, the index of the modified block is changed and the user needs to compute a new signature for the modified block. User access the modified data with the new signature generated to perform. For security reasons, when a user leaves the group or misbehaves, user is revoked from the group. As a result, this revoked user should no longer able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group users. Therefore the content of shared data is not changed during user revocation, the blocks which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. A straightforward method to re-compute these signatures during user revocation is to ask an existing user to first download the blocks previously signed by the revoked user, verify the correctness of these blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. This Straight forward method includes the large computation of resources by downloading and verifying blocks, and by re-computing and uploading signatures [13].

Our proposed ideas are as follows;

We propose secure and efficient auditing mechanism for data storage in cloud. Our auditing mechanism can perform number of verifications without frequent Updation of file, which is lacking in most of the scheme. The major advantage is it can resist from attack when a random file is chosen. Our auditing mechanism can support Data Dynamic operations including data modification, data append, data deletion and data insertion. When additional file to be stored in cloud server it consumes less space. Keys are generated using Public Key algorithm(asymmetric method).We evaluate our auditing mechanism based on experimental and theoretical results to prove it is secure, reliable and resistant to attack.

3.2 Security measures

We try to improve security by the following measures proposed in our paper

- **Security**: A scheme is secure, unless verifier should accept an invalid output from user.
- **Auditing performance:** To reduce the number of undetected polluted blocks in shared data, the detection probability of the random selected blocks in one auditing task on the shared data can be improved by spending more communication and computational cost during auditing.

4 Assumptions

In this section we discuss some assumptions including admissible bilinear map and Homomorphic authenticators

4.1 Admissible bilinear map

A bilinear map establishes relationship between cryptographic groups. Let $e:G_1XG_2 \rightarrow G_t$ be a bilinear map with g1 and g2 be generators of G_1 and G_2 respectively. The map e is an admissible bilinear map if e(g1,g2) generates G_t and e is efficiently computable.

4.2 Homomorphic key authenticator

Homomorphic key authenticator allows a TPA to check the integrity of data stored in cloud. Users with proper authentication can generate valid keys. Let (pk,sk) denote the data owner's public/secret key pair,α1 denote the key on block s1€$Z_{p,}$and α2 denote the key on block s2€$Z_{p..}$

4.3 Security measures

Security is improved by the following measures .They are validation and auditing performance

- **Validation**: A scheme is secure, unless verifier should accept an invalid output from user.
- **Auditing performance:** To reduce the number of undetected polluted blocks in shared data, the detection probability of the random selected blocks in one auditing task on the shared data can be improved by spending more communication and computational cost during auditing.

5 Proposed System

5.1 Architecture Diagram

The proposed system has a cloud storage system with three entities which have been shown in figure 5.1.The three entities are the data owner, third party auditor (TPA) and the cloud. The cloud, which is managed by the cloud service provider, stores the data and provides computation resources. The users create data and store their data to the cloud with proper authentication from TPA Since the storage and computation resources are limited, the users doesn't keep a local copy of their data .TPA is able to check the integrity of the out- sourced data. The data owner can modify any block of the outsourced data by performing an insertion, deletion or update operation on the block while the auditor can still check the integrity.

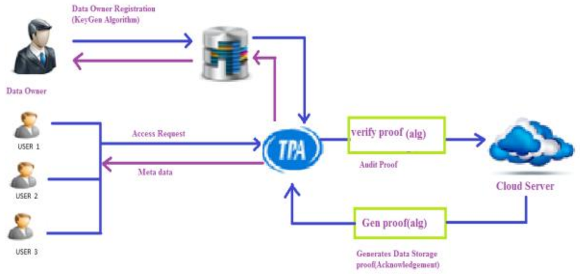


Figure 5.1 Architecture diagram for public auditing

To enable the public auditing for cloud storage scheme, proposed scheme achieves the performance and security guarantees: Public Auditing is used to allow a TPA to verify the correctness of the data stored on the cloud server on demand without downloading a whole data or introducing an additional burden to the cloud server.

- **Storage correctness:** This is used to ensure that there is no TPA can audit the user's data are send by the fake cloud server.
- **Privacy preserving:** During auditing, TPA is not allowed to derive the user's data from the information stored in cloud.
- **Batch auditing:** This is used to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users
Simultaneously.
- **Efficiency:** TPA is allowed to perform auditing with minimum communication and computation overhead.

5.2 Methodology

To Support public auditing the four schemes are proposed .They are Keygen, Siggen, Genproof, Verify proof

- **Keygen:** The keygen process execute between user and cloud server. The public key and secret key are represented as sk,pk. Using both secure key and public key Keys are generated using Public Key Algorithm(asymmetric method).Data owner can access the cloud server .The generated key is known only to the Data owner and the cloud server.
- **Siggen:** In Siggen process data file stored in cloud server is preprocessed. Data owner creates metadata for the file to be stored in a Cloud server. Data owner can send the metadata to the TPA after publishing in the cloud for later audit.

- **Genproof:** In Genproof process, the TPA issues an audit message to the cloud server to indicate that the data has retained properly at the time of later audit. The Cloud generates proof of possession of stored data under a challenge of the TPA.
- **Verifyproof:** In Verify proof process the TPA has to check the proof response from the cloud. This algorithm verifies the message from the cloud by using the metadata stored in TPA. The user can verify with TPA by sending the private key and public key to view whether the data is stored in cloud server.TPA send the response to the cloud server for the verification of data file.TPA matches the user’s metadata with the metadata stored in cloud.TPA can authenticate the user to the cloud server if metadata matches.

5.3 Scheme construction

The public auditing can be constructed in two different phases such as Setup and Audit

5.3.1 Setup: In the setup scheme, the user register with the TPA and initializes the secret keys(public key and private key) to store the data file in cloud by executing the KeyGen process. Metadata is created when data file is preprocessed using siggen. User has some access rights to add some additional metadata to the cloud.

5.3.2 Audit:

In Audit scheme, to ensure that data file is retained properly and audit message is issued by TPA to cloud. Response message is executed by GenProof for the stored data file with the help of verification metadata.

5.3.3 Batch auditing:

With the establishment of privacy preserving public auditing, TPA simultaneously handles multiple auditing upon different users’ allocation. The individual auditing of these tasks for the TPA can be tedious and very inefficient. If the auditing allocation on distinct data files from different users is given then it is more profitable for the TPA to batch these multiple tasks together and audit at one time. So a secure batch auditing protocol for simultaneous auditing of multiple tasks can be obtained. This batch auditing reduces the computation cost on the TPA side. This is because of aggregation. Also invalid responses are identified in a fast manner than individual verification.

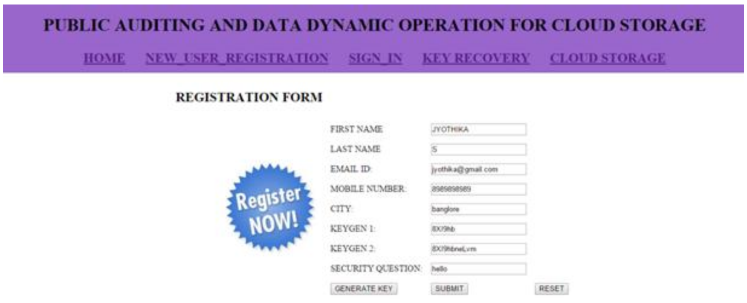
5.3.4 Data dynamics:

Data dynamic means the users can perform data insertion, data modification and deletion at any instance of time, TPA checks the integrity of outsourced data to be stored in the cloud server. Data can be inserted by Data owner in cloud server by creating metadata along with the file name to be inserted. File size should not exceed. In cloud data storage, sometimes the user may need to modify file stored in the cloud, from its current value to a new one. Data owner can delete the file by viewing the metadata from table .Users cant delete file unless they are provided permission from Data owner. Data owner want to increase the size of his stored data by increasing size of file for appending. We anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of files (not a single file) at one time.

6 Result and Discussion

For Implementation Eclipse tool is used. Front end part is written in java and back end connection is implemented using SQL Server. For cloud storage, MYSQL hosting is used.

6.1 Registration Module



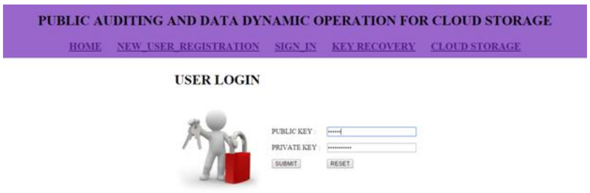
REGISTRATION FORM

FIRST NAME	JYOTHIKA
LAST NAME	S
EMAIL ID	jyothika@gmail com
MOBILE NUMBER	8989898989
CITY	banglore
KEYGEN 1:	8X09hb
KEYGEN 2:	8X09hbneLvm
SECURITY QUESTION	hello

Figure 6.1 represents the user registration module. Data owner

Register to the cloud server by providing their personal details. Using Keygen random keys are generated.

6.2 Data Owner Registration


PUBLIC AUDITING AND DATA DYNAMIC OPERATION FOR CLOUD STORAGE

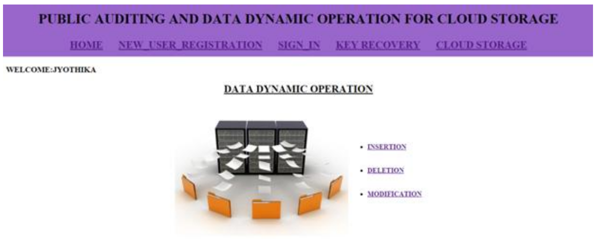
USER LOGIN

PUBLIC KEY : ••••••

PRIVATE KEY : ••••••••••••

Figure 6.2 represents data owner registration module .Data owner register to the cloud server by the public and private keys generated

6.3 Data Dynamics Operation

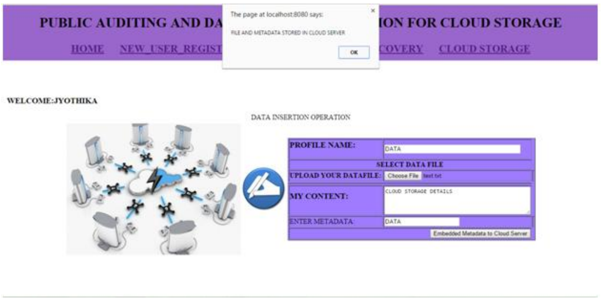

PUBLIC AUDITING AND DATA DYNAMIC OPERATION FOR CLOUD STORAGE

WELCOME:JYOTHIKA

DATA DYNAMIC OPERATION

Figure 6.3 represents data dynamics operation such as insertion, deletion and modification of records. Data owner access the cloud server with the help of TPA.

6.4 Insertion


PUBLIC AUDITING AND DA ION FOR CLOUD STORAGE

The page at localhost:8080 says:

FILE AND METADATA STORED IN CLOUD SERVER

WELCOME:JYOTHIKA

DATA INSERTION OPERATION

PROFILE NAME: DATA

SELECT DATA FILE

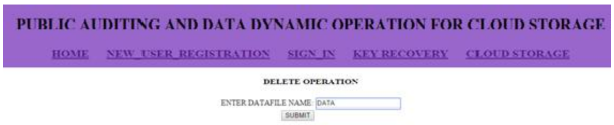
UPLOAD YOUR DATAFILE: test.txt

MY CONTENT: CLOUD STORAGE DETAILS

ENTER METADATA: DATA

Figure 6.4 Data owner uploads the file by entering the profile name, content and the metadata. File and the metadata are stored in cloud server.

6.5 Deletion

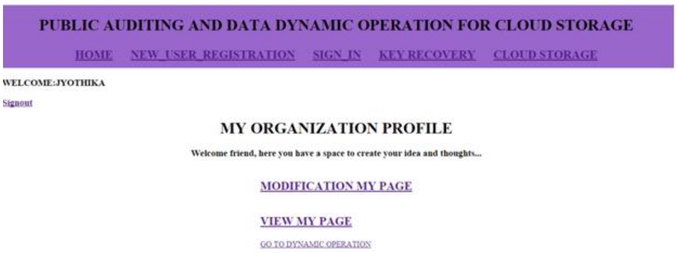

PUBLIC AUDITING AND DATA DYNAMIC OPERATION FOR CLOUD STORAGE

DELETE OPERATION

ENTER DATAFILE NAME: DATA

Figure 6.5 represents deletion module .Data owner deletes the file by entering the metadata.

6.6 Modification



WELCOME:JYOTHIKA

MY ORGANIZATION PROFILE

Welcome friend, here you have a space to create your idea and thoughts...

Figure 6.6 represents modification module. Data owner can modify the file by downloading .After modification done data owner can now upload the file again to the cloud server.

Conclusion

In this paper, public auditing for cloud data storage is proposed to support block less verifiable and non-malleability. During auditing process, TPA is unknown of the data content stored in cloud server by homomorphic linear authenticator technique. We propose an efficient data dynamic operation on data files stored in cloud including data insertion, deletion, and modification and append because cloud storage is not static. To verify the integrity, TPA monitors the user's data. We have also addressed the scalability that reduces the number of re-signing keys and Batch Auditing for Multiple Tasks. Privacy of data owner is secured in confidential manner.

Future work:

In future, user's private information and identities of keys should be preserved from TPA. With Homomorphic linear authenticator TPA can verify the integrity of shared data but the identity of key is not revealed. This can be improved by some advanced proxy techniques.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores," In Proceedings Of CCS "07, pp. 598–609, 2007.

[2] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," In Proceedings of Secure Communication "08, pp. 1–10, 2008.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[4] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology Print Archive, Report 2008/175,2008

[5] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," In Proceedings of ICDCS "08, pp.411–420,2008.

[6] D.L. Gazzoni Filho, and P. Barreto, "Demonstrating Data Possession and Uncheatable Data Transfer," Book Demonstrating data possession and uncheatable data transfer, Series Demonstrating data possession and uncheatable data trans

[7] Jia Xu and Ee-Chien Chang, "Towards efficient proofs of retrievibility in cloud storage".

[8] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS"07: Proceedings of the 14th ACM conference on Computer and communications security.

[9] Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage Jyoti R Bolannavar1P G Student, Department of Computer Science, Gogte Institute of Technology, Belgaum-590008, Karnataka, India7

[10]. Mohammed A. AlZain, Ben Soh and Eric Pardede AlZain, M.A.; Soh, B.; Pardede, E. A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012.TP

[11] H. Shacham and B. Waters, "Compact Proofs of Retrievability," In Proceedings of Asiacrypt "08, Dec. 2008.

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

[13] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912. [14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in the Proceedings of ACM/IEEE IW QoS 2009, 2009, pp. 1–9.

[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.

[16] J. Yuan and S. Yu. Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification. [Online]. Available: http://eprint.iacr.org/2013/484