ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

SECURED DATA STORAGE FOR RDPC PROTOCOL WITH ENHANCED TPA AUDITING SCHEME USING MHT IN CLOUD COMPUTING

Ms.N.Elamathi[1], B.Selvanayagi[2]

Department of Information Technology, Adhiparasakthi Engineering College, Melmaruvathur, India[1,2]

ABSTRACT: Cloud computing enables vastly scalable services consumed over the Internet.Cloud storage is a model of data storage where the digital data is stored in logical pools.These cloud storage providers are responsible for keeping the data available and accessible.but the security of cloud storage is always the focus of several potential cloud clients,and huge impact for its widespread application. Therefore,it is of great importance for users to check whether the data is kept intact.in this paper RDPC protocol based on homomorphic hash algorithm is proposed. And to enable dynamics of data MHT is used to find the location of each data operation in the RDPC protocol. it allow the third party auditor (TPA) to check the integrity of outsourced data. d. The scheme allows unlimited times verification without the need for the verifier to compare against the original data, which reduces the communication and computation complexity.and implementing Secure Multi Owner Authentication technique is by which we can secure the data Stored in the Cloud Server's Database.the security and routine analysis shows that the scheme is practical for real time.

Keywords: security model,batch auditing trust party auditor,privacy preserving,RDPC,MHT.

1. INTRODUCTION

Cloud storage is an important service of cloud computing [12] which allows data owners (owners) to move data from their local computing systems to the cloud. More and more owners start to store the data in the cloud [1]. However, this new paradigm of data hosting service also introduces new security challenges [6]. Owners would worry that the data could be lost in the cloud. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take [5]Sometimes, cloud service providers might be dishonest. They could discard the data which has not been accessed or rarely accessed to save the storage space and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud. Traditionally, owners can check the data integrity based on two-party storage auditing protocols [6, 9, 12]. In cloud storage system, however, it is inappropriate to let either side of cloud service providers or owners conduct such auditing, because none of them could be guaranteed to provide unbiased auditing result. In this situation, third party auditing is a natural choice for the storage auditing in cloud computing. A third party auditor (auditor) that has expertise and capabilities can do a more efficient work and convince both cloud service providers and owners. For the third party auditing in cloud storage systems, there are several important requirements which have been proposed in some previous works [10]. The auditing protocol should have the following properties:

1. **Confidentiality** The auditing protocol should keep owner's data confidential against the auditor
2. **Dynamic Auditing** The auditing protocol should support the dynamic updates of the data in the cloud.
3. **Batch Auditing** The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds. Recently, several remote integrity checking protocols were proposed to allow the auditor to check the data integrity on the remote server content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor. In [12], the authors extended their dynamic auditing scheme to be privacy-preserving and support the batch auditing for multiple owners

2.RELATED WORK

The remote data possession checking schemes can be categorized into two types, namely "provable data possession" (PDP) and "proof of retrievability" (POR). Usually, a PDP can be transformed to a POR by adding erasure or error correcting codes. Ateniese et al. first formally define protocols for PDP and present two provably secure PDP schemes in [1].They utilize RSA based homomorphic verifiable tags to achieve public auditability. In [2], Ateniese integrates forward error-correcting code with PDP scheme, which can correct a small corruption of data or detect a large corruption of data. In Ref. [3], Sebe et al.present an RDPC protocol such that it allows an unlimited number of verifications and the maximum running time can be chosen at setup time and traded off against storage at the verifier. In Ref. [4], Curtmola et al. firstly provide a provably secure multiple-replica PDP (MR-PDP) scheme. It allows a client who

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

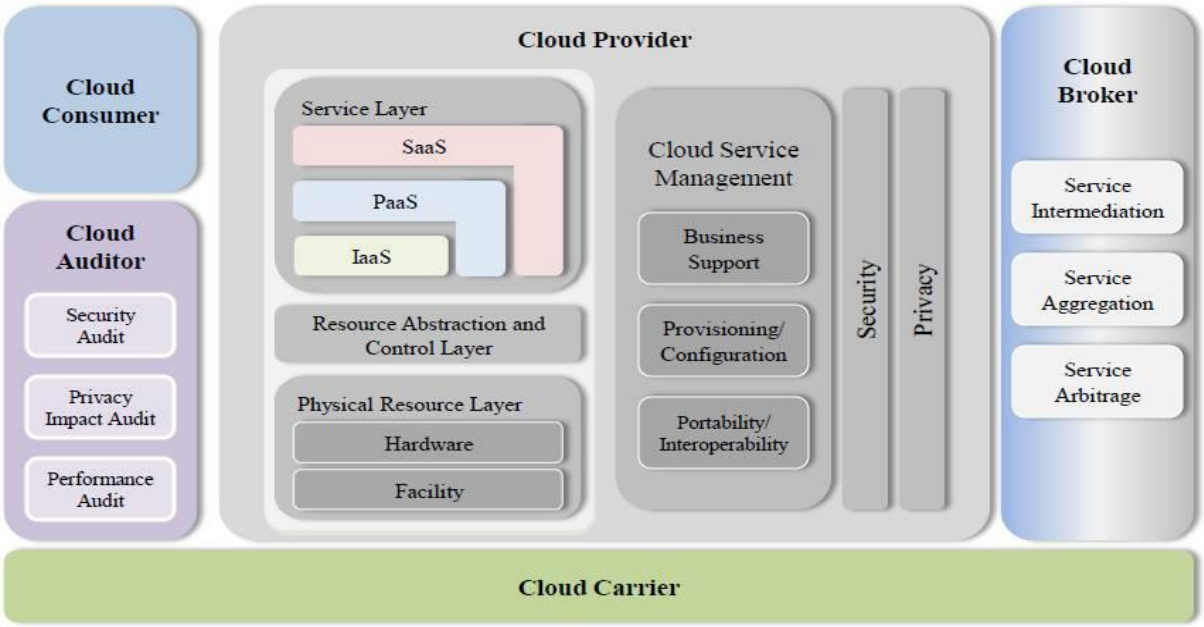


Fig 1. The Conceptual Refernce Model

stores replicas of a file to verify that the server have held thet copies.Liu et al. [5] propose a PDP scheme which fully supports dynamic data operations, however, the storage, communicationand computation complexities are linear increase with thefile in the storage.Erway et al. [6] also extended the PDP model to support dynamic updates on the stored data and proposed two dynamic provable data possession scheme by using a new version of authenticated dictionaries based on rank information. However, their schemes may cause heavy computation burden to the server since they relied on the PDP scheme proposed by the Ateniese. Xiao et al.[7] provide a schemebased on symmetric key cryptography which is called data possession checking (DPC). The main contribution is that they proposed a challenge renewal mechanism based on verification block circular queue to allow the dynamic increase of the number of effective challenges which can be issued by the checker. Wang et al. [8] propose to combine BLS-based HLA with MHT to support fully data dynamics. Concurently, Erway et al. develop a skip list based scheme to also enable provable data possession with full dynamics support. However, the verification in both protocols requires the linear combination of sampled blocks as an input, like the designs and thus doesnot support privacy-preserving auditing. In [9] Bowers et al. introduce HAIL (High-Availability and Integrity Layer), a distributed cryptographic system which allows a set of servers to prove the integrity and retrievability of stored file to a client. Shah et al. [10] propose a scheme which allowing a trust public auditor (TPA) to keep online storage honest by first encrypting the data then sending a number of precomputed symmetric-keyed hashes over the encrypted data to the auditor. This scheme only works for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up. In [11] Zhu et al. proposed a cooperative provable data possession scheme that can support the batch auditing for multiple clouds and also extend it to support the dynamic auditing On the other hand, some data owners may store their data on more than one cloud servers. To ensure the owner's data integrity in all the clouds, the auditor will send the auditing challenges to each cloud server which hosts the owner's data, and verify all the proofs from them.In [12], Wang et al. consider dynamic datastorage in a distributed scenario, and the proposed challenge-response protocol can both determine the datacorrectness and locate possible errors. In their scheme, they utilize RSA-based homomorphic tags for auditing outsourced data, thus public auditability is achieved

3. THE PROPOSED SCHEME

In this section, we present our security protocols for clouddata storage service with the aforementioned research goalsin mind. We start with some basic solutions aiming to provide integrity assurance of the cloud data and discuss their demerits. Then, we present our protocol which supports public auditability and data dynamics. We also show how to extent our main scheme to support batchauditing for TPA upon delegations from multiusers

DATA OWNER

In this module we are going to create an User application by which the Data owner or User is allowed to access the application from the Server of the Cloud Service Provider. First the Data Owner will register into Server of the Cloud Service Provider. Once registered the public and private key will be generated send to the Data Owner. Once the Data Owner registered into the Cloud Server, they are

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

allowed to upload the data into the Cloud Server. The Data will be Encrypted and Uploaded into the Cloud Server.

USER

Here first the User want to create an account and then only they are allowed to access the Network. Once the User create an account, they are to login into their account and request the Job from the Cloud Service Provider. Based on the User's request, the Cloud Service Provider will process the User requested Job and respond to them. All the User details will be stored in the Database of the Cloud Service Provider. In this Project, we will design the User Interface Frame to Communicate with the Cloud Server through Network Coding using the programming Languages like Java/ .Net. By sending the request to Cloud Server Provider, the User can access the requested data if they authenticated by the Cloud Service Provider.

CLOUD SERVICE PROVIDER

Cloud Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the all the User/ Data Owner information to authenticate when they want to login into their account. The User / Data Owner information will be stored in the Database of the Cloud Service Provider. Also the Cloud Server will redirect the User requested job to the any of the Queue to process the User requested Job. The Request of all the Users will process by the Virtual Machines in the Queue. To communicate with the Client and the with the other modules of the Cloud Network, the Cloud Server will establish connection between them. For this Purpose we are going to create an User Interface Frame. Also the Cloud Service Provider will send the User Job request to the Queues in Fist In First Out (FIFO) manner.

TRUSTED PARTY AUDITOR

Trusted Party Auditor will audit the data that are uploaded by the Data Owner based on their (Data Owner's) request. So that the data will audited by the Data Owner. To audit the User requested data the Trusted Party auditor have to be registered into the Cloud Server. So that they allowed to audit the data.

MERKLE HASH TREE ALGORITHM

Once the data owner send the request to audit the data the will be audited by the Trusted Party auditor using Merkle Hash tree Algorithm. The data will audited by dividing the data into multiple parts. After each time Period, the auditing information will be updated by the Trusted Party Auditor. So that we can ensure security. If there is any change while auditing the data, the TPA will address the same to the Data Owner.

4. REMOTE DATA POSSESSION CHECKING PROTOCOL

Remote data possession checking is a topic that focuses on how to frequently, efficiently and securely verify that a storage server can faithfully store its client's (potentially very large) original data without retrieving it. The storage server is assumed to be un-trusted in terms of both security and reliability. There are two types of schemes, namely provable data possession Research on Remote Data Possession Checking (PDP) and proof of retrievability (POR). The difference between PDP and POR is that POR checks the possession of data and it can recover data in case of a failure. Generally, to design an RDPC scheme, the following factors must be considered.

- **Computation complexity,** which refers to the initialization and authentication expenses in client and the proof generating expenses on the server. It means that the scheme should be efficient interms of computation.
- **Communication complexity**, which refers to the amount of communication between client and server required by the scheme. It means that the amount of communication should be low.
- **Storage cost**, which refers to the additional storage of client and server required by the scheme.It means that the additional storage should be as low as possible.
- **Data updating**, including modifying, inserting, adding and deleting etc. It can only be used for static data if it doesn't support data update, such as data archive.
- **The number of verification**. It ought to run the verification an unlimited number of times.
- **Public verification**. It must support public verification.
- **Data recovery**, which means that the scheme can recover the data in case of a failure. It can be achieved by introducing error correcting code or erasure code.
- **Provable security**. Generally, it is necessary to prove that the scheme is secure.
- **Data blocks access**, which refers to that how much data blocks the scheme needs to access.In addition, some applications may hope to have a third-party auditor to periodically verify the data and assist in returning the result to the users.

Remote data possession checking(RDPC) protocol to refer to any protocol (including PDP and POR).that aims to solve the integrity of remote data.

4.1 SECURITY ANALYSIS OF THE DYNAMIC RDPC PROTOCOL:

4.1.1 Definitions

We start with the definition of a provable data possession scheme and protocol, followed by the security definition that captures the data possession property. A PDP (Provable Data Possession Scheme)scheme is a collection of four polynomial-time algorithms (KeyGen, TagBlock, GenProof, CheckProof) such that: **KeyGen(1k)** → (pk, sk) is a probabilistic key generation algorithm that is run by the client to setup the scheme. It takes a security parameter k as input and returns a pair of matching public and secret keys (pk, sk). **TagBlock(pk, sk, b)** → Tb is a (possibly probabilistic) algorithm run by the client to generate the verification metadata. It takes as inputs a public key pk, a secret key sk, and a file block b, and returns the verification metadata Tb. **GenProof(pk, F, chal,_)** → V is run by the server in order to generate a proof of possession. It takes as inputs a public key pk, an ordered collection F of blocks, a challenge chal, and an ordered collection _ which is the verification metadata

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

corresponding to the blocks in F. It returns a proof of possession V for the blocks in F that are determined by the challenge chal. **CheckProof(pk, sk, chal, V)** → {"success", " f ailure"} is run by the client in order to validate a proof of possession. It takes as inputs a public key pk, a secret key sk, a challenge chal, and a proof of possession V. It returns whether V is a correct proof of possession for the blocks determined by here it construct a PDP protocol

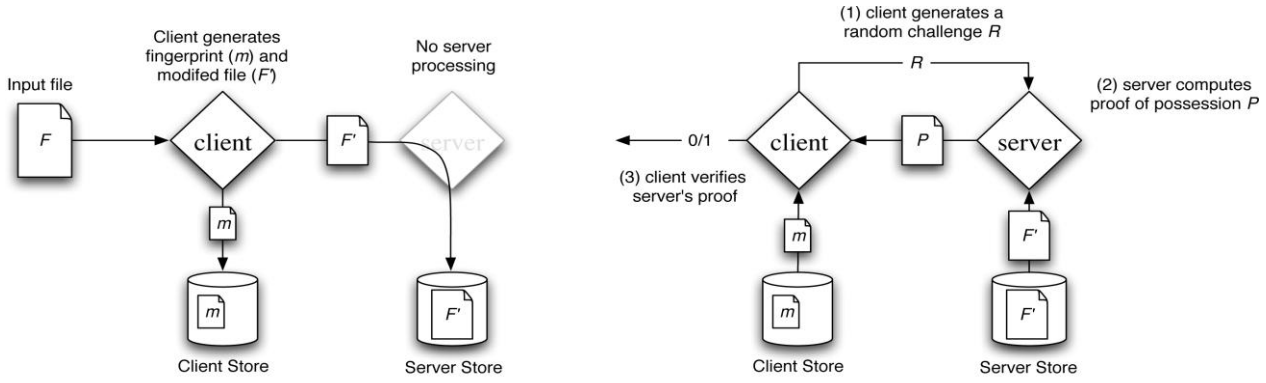
5. PROVABLE DATA POSSESSION

Provable data possession (PDP) that can be used for **remote data checking**: A client that has stored data at an untrusted server can verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which considerably reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking is lightweight and supports large data sets indistributed storage systems. Remote data checking (RDC) allows an auditor to challenge a server to provide a proof of data possession in order to validate that the server possesses the data that was originally stored by a client The challenge and the response are each slightly more than 1 Kilobit. also present a more efficient version of this scheme that proves data possession using a single modular exponentiation at the server. Concurrently with this work, another model for proofs of retrievability (PoRs) was proposed to perform remote data checking PDP scheme in two phases, Setup and Challenge.

Setup. The client C is in possession of the file F and runs KeyGen(1k) → (pk, sk),
followed by TagBlock(pk, sk, bi) → Tbi , for all $1 \le i \le f$. C stores the pair (sk, pk). C then sends pk, F, and _ = (Tb1, . . . , Tb f) to S for storage and may delete F

Challenge. C generates a challenge chal that, among other things, indicates the specific blocks for which C wants a proof of possession. C then sends chal to S. S runs GenProof(pk, F, chal,_) → V and sends to C the proof of possession V. Finally, C can check the validity of the proof V by running CheckProof(pk, sk, chal, V)

In the Setup phase, C computes tags for each file block and stores them together with the file at S. In the Challenge phase, C requests proof of possession for a subset of the blocks in F. This phase can be executed an unlimited number of times in order to ascertain whether S still possesses the selected blocks. We note that GenProof and CheckProof may receive different input values for chal, as these algorithms are run by S and C, respectively.



(a) Pre-process and store (b) Verify file possession by server

Fig. 2. Protocol For Provable Data Possession

6. PROOF OF RETRIEVABILITY

The notion of proof of retrievability (POR) and proposed a formal POR protocol definition and accompanying security definitions [12]. Their scheme use disguised blocks, called sentinels, hidden among regular file blocks that the server cannot differentiate from encrypted blocks In addition, the scheme can only be applied to encrypted files and can handle a limited number of challenges,because each challenge consumes some sentinel blocks. s two POR schemes. The first one, built from BLS (the abbreviation of three names: Boneh, Lynn and Shacham) signatures and secure in the random oracle model, has the shortest query and response with public verifiability. ,In [4]Curtmola et al. Research on Remote Data Possession Checking the key performance and security requirements for integrating FECs into PDP and describe an encoding scheme and file organization for RDPC . The scheme supports dynamic operations on data blocks, including data update, delete and append. In [9], they consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the
integrity of the dynamic data stored in the cloud. To achieve efficient data dynamics, they improve the POR model by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. In [6], they also consider introducing a TPA to audit the cloud data storage. They utilize public-key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy preserving public auditing

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

system. To support multiple auditing tasks, they explore the technique of bilinear aggregate signature to extend the scheme into a multi-user setting. However, all the data possession schemes are based on public-key cryptography and they don't consider data recovery

7. AUDITING PROCESS

Audit service based on TPA.This also provides a background for the description of our audit service outsourcing as follows: • First, the client (data owner) uses the secret key sk to preprocesses the file, which consists of a collection of n blocks, generates a set of public verification information that is stored in TPA, transmits the file and some verification tags to CSP, and may delete its local copy; • At a later time, using a protocol of proof of retrievability, TPA (as an audit agent of clients) issues a challenge to audit (or check) the integrity and availability of the outsourced data in terms of the public verification information. FIG 2.architecture is known as the audit service outsourcing due to data integrity verification can be implemented by TPA without help of data owner. the data owner and granted clients need to dynamically interact with CSP to access or update their data for various application purposes. However, we neither assume that CSP is trust to guarantee the security of stored data, nor assume that the data owner has the ability to collect the evidences of CSP's fault after errors occur. Hence, TPA, as a trust third party (TTP), is used to ensure the storage security of their outsourced data. We assume the TPA is reliable and independent, and thus has no incentive to collude with either the CSP or the clients during the auditing process:

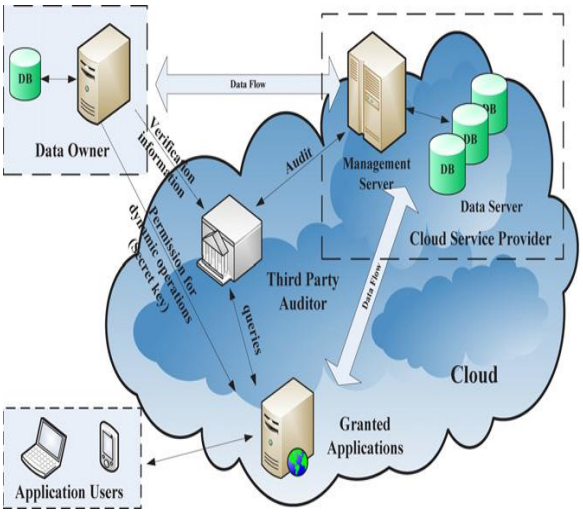


Fig.3. Audit System Architecture For Cloud Computing

• TPA should be able to make regular checks on the integrity and availability of these delegated data at appropriate intervals;

To enable privacy-preserving public auditing for cloud data storage under this architecture, our protocol design should achieve following security and performance guarantees:

- **Public verifiability**: to allow TPA to verify the correctness of cloud data on demand without retrieving the entire data or without introducing additional online burden to the cloud users.
- **Storage correctness**: to ensure that any server can pass TPA's verification only if it keeps user's data intact.
- **Privacy preserving**: to assure that no data content is leaked to TPA during the auditing process.
- **Batch auditing**: to enable TPA to cope with multiple auditing delegations from possibly many users concurrently in secure and manner.
- efficient **Blockless verification**: no challenged file blocks should be retrieved by TPA during the auditing process both for efficiency and security reasons.

7.1. System model

Our public auditing scheme comprises three different entities (parties) with well defined interactions among them, as

- **Cloud server** (for brevity, referred to server from here on), which is owned by CSP, has the infrastructure and expertise to host outsourced storage, and provides efficient mechanisms for its users to create, store, update and request for retrievability.
- **User** (client), who has data to be stored on the cloud, leaves information technology (IT) operations on data to professionals and concentrate on his/her core businesses.
- **Third party auditor**, another entity who has better expertise and capabilities than the user, is trusted to measure the cloud storage reliability and validity on behalf of users when needed. Users can put huge data on the cloud to make themselves free from the burden of storage and maintenance. As in [7] assume that the CSP is semi-trusted, which means it follows the normal flow of the protocol in the system. However, it might not be trusted with the actual data contents and its integrity,

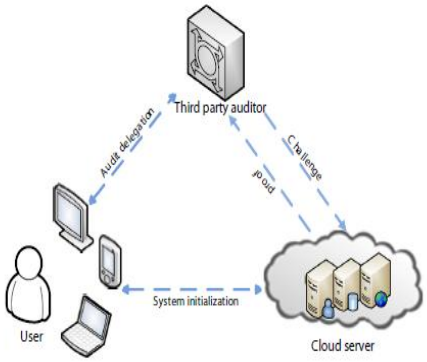


Fig 4.Cloud Data Storage ServicE

7.3 ISSUES ON PUBLIC AUDITING SCHEMES

Remote data storages are used to share data and services in the cloud environment. Data provider uploads the shared data into the data centers. Public auditing methods are used to verify the data integrity in remote data storages. Third-party auditor (TPA) is used to check the integrity of

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 11, November 2014

outsourced data. Privacy preserving public auditing mechanism is used to verify the data integrity with privacy. TPA supports auditing for multiple users simultaneously. Batch auditing
mechanism is used for multi user environment. Homomorphic linear authenticator and random masking techniques are used to protect the data from TPA. The following drawbacks are identified in the existing system.

- Data dynamism is not tuned for batch auditing scheme
- Commercial cloud operations are not supported by the system
- Data dynamism is not adapted for privacy preserved auditing mechanism
- Privacy is provided for single user verification process

8.MERKLE HASH TREE.

The existing schemes do not support dynamic data operation.This is because the construction of the tags is involved with the file information i.Merkle Hash Tree (MHT): is an authentication structure [15], which is constructed as a binary tree where the leaves in the MHT are the hashes of authentic data values.In this paper, it employ MHT to authenticate both the values and the positions of data blocks. We treat the leaf nodes as the left-to-right sequence.

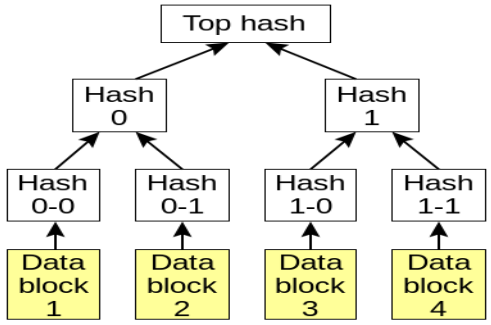


Fig 5. Creating Top Hash

The ith leaf node of the MHT stores a pointer which points to data block mi. Cloud user generates a U array. Each item ui represents the times of updates of the corresponding block mi. Cloud user computes a tag ti and a signature si for each block mi,and maintains the pointer among the MHT, blocks, tags, signature array and U array. The correspondence is shown in Figure 2, which also depicts an example of authentication for m6. The prover provides the verifier with the authentication path information (API).

9. CONCLUSION

In this paper, a dynamic data possession checking scheme is proposed Data dynamics provide the flexibility to the user ,after storing their data at the remote server.,can dynamically update the data at any times.designing RDPC schemes homomorphic hash functions that support public auditing and privacy preserving such that anyone can check the integrity of the outsourced data without learning any knowledge of user's data.another interesting research directions is to integrate some advanced cryptographic techniques,such as identity -based cryptography,attribute-based cryptography.in addition,exploring novel approaches to support data dynamic operations in RDPC protocols.and exploiting practical technology to locate the corrupted blocks in RDPC protocols are also noteworthy and vital.

REFERENCE

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. Computer and Comm. Security (CCS' 07), pp. 598-609, 2007.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson and D. Song, "Remote data checking using provable daa possession", ACM Transcations on Information and System Security, Vol. 14, No. 1, Article 12, May 2011

[3] F. Sebe, J.F. Domingo, A.B. Martinez, Y. Deswarte, J. Quisquater, Efficient remote data possession checking in critical information infrastructures, IEEETransactions on Knowledge and Data Engineering (2007) 1034–1038.

[4] R. Curtmola, O. Khan, R. Burns, G. Ateniese, MR-PDP: multiple-replica provable data possession, in: Proc. ofICDCS'08, 2008, pp. 411–420.

[5] H. Liu, P. Zhang and J. Liu, "Public data integrityverification for secure cloud storage", Journal of networks,vol.8, No. 2, pp. 373-380, 2013

[6]. Erway, C.C.,Küpçü, A., Papamanthou, C., Tamassia, R.:Dynamic provable data possession. In: Proceedings of the 16thACMconference on computer and communications security (CCS'09), pp. 213–222. ACM (2009)

[9] K. D. Bowers, A. Juels and A. Oprea, "HAIL: a highavailability and integrity layer for cloud storage", Proc. ofACM-CCS'09, pp. 187-198, 2009.

[10] M. A. Shah, R. Swaminathan, and M. Baker, "Privacypreserving audit and extraction of digital contents", Report 2008/186, Cryptology ePrint Archive, 2008.

[7] Xiao Da, Shu Jiwu, Chen Kang, Zheng Weimin, "A Practical Data Possession Checking Schemefor Networked Archival Storage", Journal of Computer Research and Development, 46(10):1660-1668, 2009[8] Q. Wang, C. Wang, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,"IEEE Trans. Parallel andDistributed Systems, vol. 22, no. 5, pp. 847-859, May 2011

[11]. Zhu,Y.,Hu, H.,Ahn, G.,Yu, M.: Cooperative provable data possession for integrity verification in multi-cloud storage. IEEE Trans. Parallel Distrib. Syst. 23(12) 2231–2244 (2012)

[12] 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), 2009.

[13] Yevgeniy Dodis, Salil Vadhan, Daniel Wichs, "Proofs of retrievability via hardness amplification", In: Proc. of TCC '09, pp.109--127, 2009.