INTEGRITY CHECKING IN CLOUD STORAGE USING THIRD PARTY AUDITOR

P. Kaviya
Assistant Professor, Department of Information Technology
Kamaraj College of Engineering & Technology, K.Vellakulam, Madurai, Tamil Nadu, India

R. Vigneshwari, P. Rajasruthi and V. Kaviya @ Manisha Preethi
UG Scholars, Department of Information Technology
Kamaraj College of Engineering & Technology, K.Vellakulam, Madurai, Tamil Nadu, India

Abstract

Cloud computing is a modern technology which is growing rapidly throughout the world. The users make use of cloud storage to store data on the cloud and that can be accessed from anywhere and anytime. Users may not fully trust the cloud service providers (CSP) because it is difficult to determine whether the CSPs provides complete data security. Therefore it is critical to develop efficient auditing techniques to strengthen user's trust and confidence in cloud storage. Data integrity is verified by third-party-auditor (TPA), guarantees the efficiency of the data. In this paper, we propose an integrity checking scheme to verify the integrity of user's data through public auditing by TPA. Initially, Users store the encrypted data and HASH value on the cloud using homomorphic linear authenticator and SHA-2. TPA will check the integrity by comparing the HASH value which is calculated for the user's encrypted data using SHA-2 algorithm.

Keywords: *Cloud Storage, Cloud Security, Third Party Auditing, Homomorphic Linear Authenticator, SHA-2.*

Introduction

Cloud computing is a style of computing where anyone can easily obtain and access the computing resources anytime. It is a type of Internet based computing, where different amenities such as servers, storage and applications are distributed to an organization’s computers and devices connected to the internet. It is cheaper and simple to use and work with it. Cloud saves both user time and money. It can be defined as according to its five main characteristics: on-demand self-service, broad-based network access, resource pooling, rapid elasticity and measured service. Additionally, the user should be able to access the cloud from any device that can connect to a network. Resource pooling refers to a collection of IT resources such as servers. This collection of resources is outsourced to an organization needs to increase productivity, the resources will scale appropriately. Lastly, the pricing of the cloud is monitored and controlled in order to determine the cost.

Cloud has become increasingly popular among various business and enterprises due to its numerous advantages. Businesses can outsource their data to popular cloud service providers such as Amazon or Google. This can be very cost effective since the cloud offers a high storage capacity and increased data processing speed. Despite of the offered benefits, there are some privacy concerns in the services provided by the cloud. The cloud service provider can share the information with third parties, if necessary, which is permitted in their privacy policy of the stored data.

Cloud data storage service have three different entities: Cloud user, in which huge data files to be saved in the cloud; Third party auditor, which has information and facility that cloud users do not have and which have faith to access the cloud storage service consistency on behalf of the user request; Cloud server, which is handled by the cloud service provider and provide data service, large amount of storage space and computation resources.

User can encrypt their data before storing it in the cloud for to prevent unauthorized access. After storing the data, user wants to check the data integrity. So user sends request to the third party auditor. The third party auditor send request to the cloud for the data. When the request is received by the cloud it sends the data to TPA for integrity checking. The third party auditor checks the integrity and sends the status to the cloud user.

The rest of the paper is organized as follows. We discuss previous works on related topics in Section 2. Section 3 describes system architecture, an algorithm for user data encryption, and third party auditing (TPA) in detail. Section 4 provides the implementation of proposed system. Section 5 result and analysis of the proposed mechanism. Section 6 finally concludes the paper.

Related Works

Sutirtha Chakraborty, et al proposed an integrity checking using third party auditor in cloud storage. This scheme is to check the integrity of data store at remote location through a third party auditor using bilinear pairing. This auditing protocol successfully checks the integrity of stored user’s data without retrieving it from the cloud storage. It is secure against to the tamper attack.

Suneeta Mohanty, et al presented a confidentiality preserving auditing for cloud computing environment. In public auditing, cloud user verifies the data integrity by itself or with the help of third party auditor (TPA). TPA verifies the integrity of stored data and sends report to the cloud users based on their request. It checks the integrity of user's data along with TPA authentication and non-reputation.

Jagruti Patil, et al discussed a privacy preserving and dynamic audit service for secure cloud storage. They developed an audit service which holds privacy preserving, public auditing, data integrity. It supports batch auditing and dynamic data operations. It only verifies whether the stored data is altered or not and modifies the result to the data owner. They used Merkle Hash Tree for indexing of encrypted data which efficiently allows to the update data dynamically while preserving data integrity.

Priyanka Patel, et al focused an access control for cloud computing through secure OTP logging as services. They presented a secured authentication system based on secured OTP based logging system in cloud computing environment. The proposed algorithm is a combination of hash algorithm system and also it reduces the security risk over cloud based services. The derivates of interpolation is very complex in terms of guessing and predictability.

Sawan V.Baghel, et al presented a secure communication of cloud third party authenticator. The proposed system uses Kerberos as a TPA/ authenticator, RSA algorithm for secure communication and Message Digest (MD5) algorithm is used to verify data integrity. MD5 algorithm supports full dynamics operation of system as well as provide guarantee on system compatibility and system provide multilevel security to database.

Cong Wang, et al proposed a privacy-preserving auditing for secure cloud storage. They extended their work to enable the TPA to perform audits for multiple users simultaneously and efficiently. The experiment is conducted on Amazon EC2 instance to demonstrate the fast performance of the design. They discussed how to generalize the privacy-preserving public auditing scheme and it supports data dynamics.

Syed Rizvi, et al proposed a potential solution for securing a cloud environment by third party auditing (TPA). They developed an auditing method for CSUs/CSPs to ensure the integrity of the TPA and minimize the possibility of insider threats or malicious activities. The integrity of TPA will be verified using the time-released session keys and the service level agreement (SLA).

Wang, et al proposed a privacy-preserving public auditing for shared data in the cloud. They used ring signatures to compute verification metadata needed to audit the correctness of shared data. The identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. This mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

Chaudhari, et al discussed a third party auditing scheme for cloud storage. The main objective of the paper is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all the requirements. It verifies the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data.

Hui Tain, et al presented a novel public auditing scheme for secure cloud storage based on dynamic-hash-table (DHT) which is a new two dimensional data structure located at a third party auditor (TPA) to record the data property information for dynamic auditing. It supports privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA. Also batch auditing is achieved by employing the aggregate BLS signature technique.

Jain Liu, et al proposed privacy preserving public auditing for regenerating code based cloud storage. They designed a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys. They randomized the encode coefficients with a pseudorandom function to preserve data privacy. This system is highly efficient and can be feasibly integrated into the regenerating-code-based cloud storage.

System Model

The system model consists of three main components: data owner, cloud service provider (CSP), third party auditor (TPA).

Cloud Service Provider (CSP): This entity possesses the infrastructure and proficiency to host indefinite and extendable data storage and computational resources.

Data owner (Client): This entity utilizes cloud server to store huge volume of data and leaves IT operations on data to third party professionals and focuses on his/her business requirements.

Third Party Auditor (TPA): This entity possess more capabilities and expertise than cloud user and performs integrity check on data on behalf of client and then sends report to client regarding the status of data.

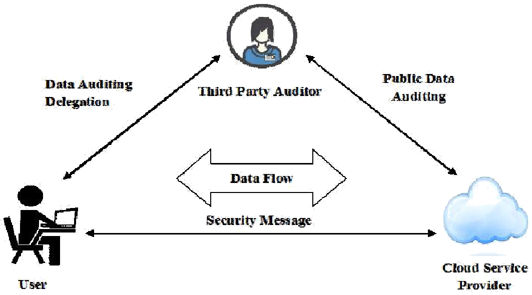


Fig.1 System Architecture

Using cloud storage, user outsources their data to CSP. Owner encrypts the file using homomorphic linear authenticator. In addition, a secret hash key is generated using SHA-2 for data integrity verification. Owner sends secret key to authorized users with whom the user wants to share the uploaded files and sends secret hash key to TPA for verifying cloud files integrity. Initially, the auditor challenges the CSP for initial verification of the entire data. The audit results are also send to the data owner of the file.

Initialization

Before uploading data files on cloud server the user has to encrypt the file and also generate the hash key. The steps are given as follows:

Before uploading data (file F) on cloud server, owner encrypts the data using homomorphic linear authenticator.

Generate hash value for the encrypted data using SHA-2.

Data owner uploads file F on the cloud server.

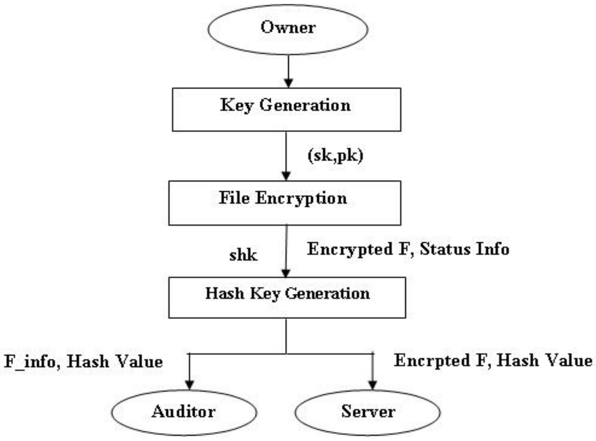


Fig. 2 Initialization Stage

The TPA performs integrity checking by calculating hash value for the encrypted file on cloud server using secret key.

If hash values are equal then the data contents are original, else modified.
TPA sends the auditing report to the data owner.

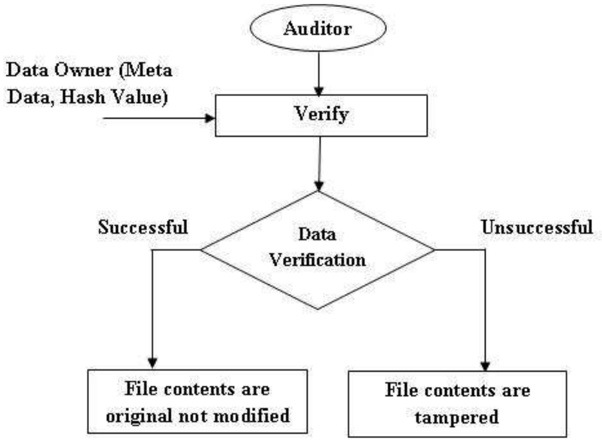

Auditor
Data Owner (Meta Data, Hash Value)
Verify
Successful
Data Verification
Unsuccessful
File contents are original not modified
File contents are tampered

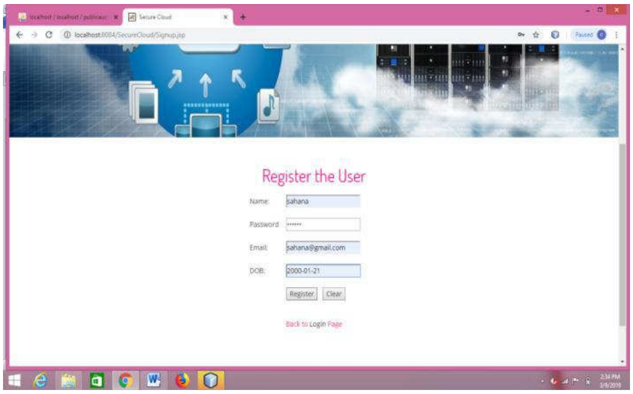
Fig.3 Data Verification

Implementation

The implemented system consists of four modules: User registration, File encryption and upload, TPA Verification Auditing, File decryption and download.

User Registration

The registration function allows users to create secure account. Here the user enters his/her necessary information like user's name, password, E-mail id, Date of Birth for signing up. The validations and required fields are effectively handled. Each user will be provided with own space on cloud.


localhost / localhost / publicau
Secure Cloud
localhost:8084/SecureCloud/Signup.jsp
Paused

Register the User

Name: sahana

Password: ••••••

Email: sahana@gmail.com

DOB: 2000-01-21

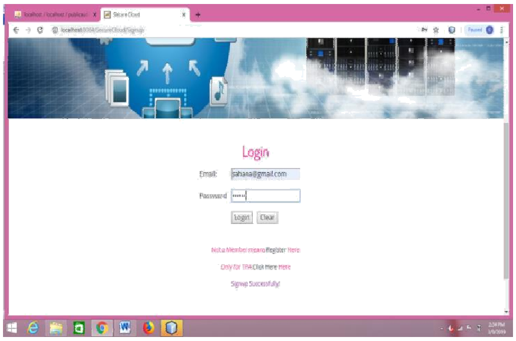
Register
Clear
Back to Login Page
2:34 PM
3/9/2019

Fig 4: User Registration

Data Verification

The TPA checks whether the user's data on cloud server is Fig. 4 Cloud User's Registration modified or not. The steps are given as follows:

The CSP stores the data files along with the hash value send by the owner.



Login

Email: sahana@gmail.com

Password ••••••

Not a Member means Register Here

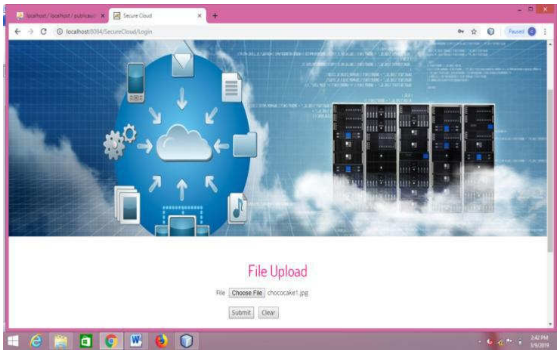
Only for TPA Click Here Here

Signup Successfully!

Fig 5: Cloud User's Login Page

File Encryption and Upload

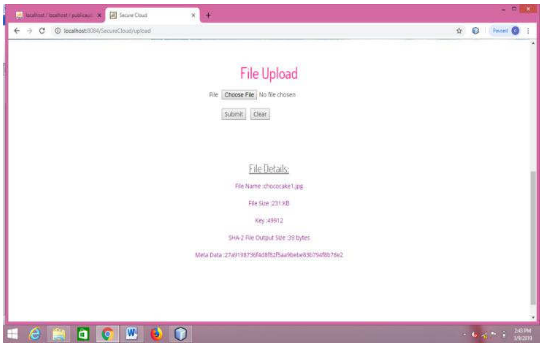
If registration is successfully completed, the user may login into the system. Every user is provided space on cloud where they can upload their files. Homomorphic linear authenticator encryption will encrypt the data files for users before storing them on cloud storage. The owner will generate secrete hash key using SHA-2 which is stored along with file for integrity checking by TPA.



File Upload

File Choose File chococake1.jpg

Fig 6: File Upload



localhost:8084/SecureCloud/upload

File Upload

File Choose File No file chosen

File Details:

File Name :chococake1.jpg

File Size :231 KB

Key :49912

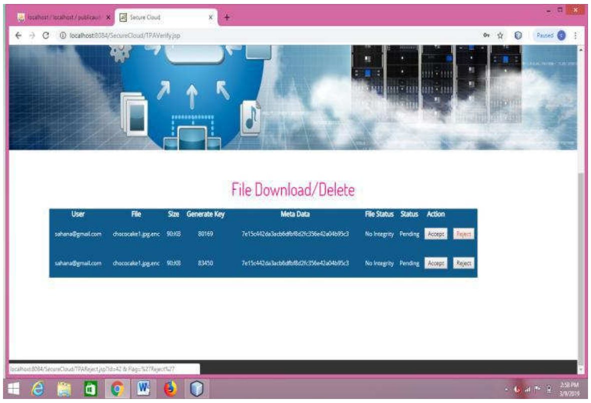
SHA-2 File Output Size :39 bytes

Meta Data :27a9198736f4d8f82f5aa9bebe83b794f8b78e2

Fig 7: File Encryption and Upload

TPA Verification Auditing

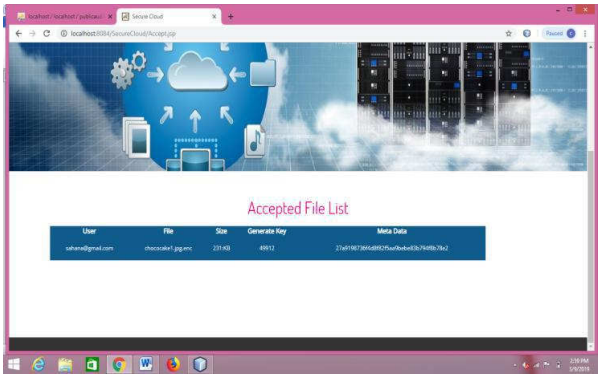
In order to authenticate the integrity of the user's uploaded data, the TPA is granted access to the system. The TPA validates the integrity of the cloud data files on behalf of cloud user. TPA verifies the legitimacy of data by calculating the hash value for the user's encrypted file on cloud server. If the hash key matches with hash key in the cloud server, the verification proves that the data files has not been modified. In case, the verification is unsuccessful, data file has been tampered. TPA sends auditing report to the data owner.



File Download/Delete

User	File	Size	Generate Key	Meta Data	File Status	Status	Action	
sahana@gmail.com	chococake1.jpg.enc	90:KB	80169	7e15c442da3acb6dfbf8d2fc356e42a04b95c3	No Integrity	Pending	Accept	Reject
sahana@gmail.com	chococake1.jpg.enc	90:KB	83450	7e15c442da3acb6dfbf8d2fc356e42a04b95c3	No Integrity	Pending	Accept	Reject

Fig 8: TPA Auditing



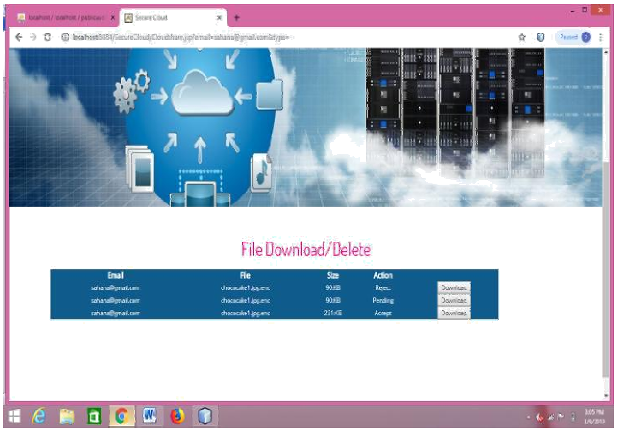
Accepted File List

User	File	Size	Generate Key	Meta Data
sahana@gmail.com	chococake1.jpg.enc	231:KB	49912	27a9198736f4d8f82f5aa9bebe83b794f8b78e2

Fig 9: TPA Auditing and Verification

File decryption and download

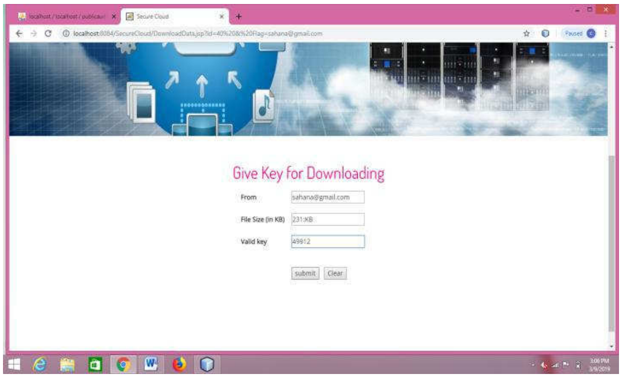
Since the data files stored on cloud server are in encrypted form, decryption must be performed before downloading the file. Initially, the system validates whether the legitimate user is requesting to download the file by demanding the secret key from the user. Data decryption is performed using algorithm and downloads the data using secret key send by the cloud user.



File Download/Delete

Email	File	Size	Action	
sahana@gmail.com	chococake1.jpg.enc	90:KB	Reject	Download
sahana@gmail.com	chococake1.jpg.enc	90:KB	Pending	Download
sahana@gmail.com	chococake1.jpg.enc	231:KB	Accept	Download

Fig. 10: File Download



Give Key for Downloading

From: sahana@gmail.com

File Size (in KB): 231:KB

Valid key: 49912

Fig 11: File Decryprtion and Download

Result and Discussion

Fig. 12 represents the time required encryption and decryption respectively on different sizes.

Table 1 Comparative Time for Encryption & Decryption

File Size (KB)	Encryption Time (ms)	Decryption Time (ms)
10	1000	3520
235	3000	3110
776	3000	3990
858	5000	5580
1425	4000	4300
25360	44000	49690

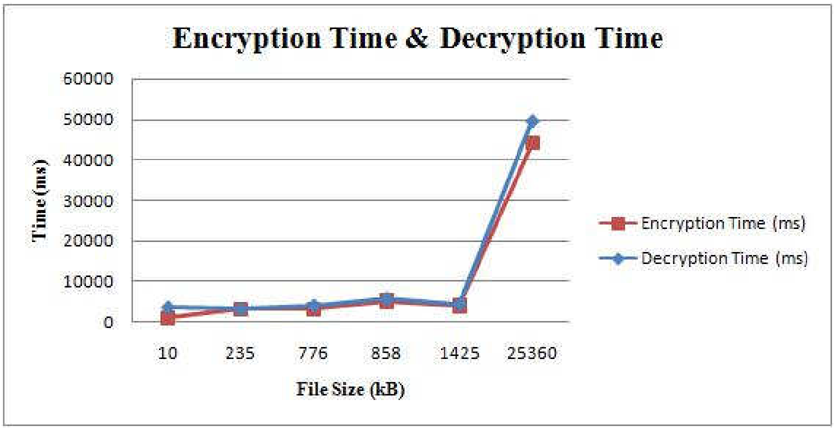


Fig. 12 Encryption and Decryption Time

Conclusion

Thus the proposed system uses public auditing scheme for data storage security on cloud while protecting the confidentiality of the user's data. Homomorphic linear authenticator along with SHA-2 hash algorithm are used to make sure that the TPA should not get access to the outsourced data on the cloud server while performing integrity check thereby increasing the effectiveness of the auditing process. This eliminates the overhead of performing auditing task from the client and also lessens the cloud user's concern that their uploaded data may be accessed by an untrusted organization or individual.

References

1. Sutirtha Chakraborty, Shubam Singh, Surmila Thokchom “Integrity Checking Using Third Party Auditor in Cloud Storage” Eleventh Conference On Contemporary Computing 2018.
2. Suneeta Mohanty, Prasant Kumar Pattnaik, Raghvendra Kumar “Confidentiality Preserving Auditing for Cloud Computing Environment” IEEE 2018.
3. Jagruti Patil, Sangita Chaudhari “Privacy Preserving and Dynamic Audit Service for Secure Cloud Storage” International Conference on Smart city and Engineering Technology 2018.
4. Hui Tain, Yuxiang Chen, Chin- Chen Chang, Hong Jiang, Yongfeng Huang, Yonghong Chen, Jin Liu “public auditing scheme for secure cloud storage based on dynamic-hash-table (DHT)” IEEE transactions on service computing, VOL 10, NO.5, 2017.
5. Priyanka Patel, Nirmal Gaud “Access Control for Cloud computing Through Secure OTP Logging as Services” International Journal of Computer Application VOL. 141 2016.
6. Swapnali, Chaudhari “third party auditing scheme for cloud storage” 7th International Conference on Communication, Computing, Virtualization 2016.
7. Sawan V. Bagel, Deepti. Theng “A Survey for Secure Communication of Cloud Third Party Authenticator” IEEE SPONSORED SECOND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEMS 2015.

8. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian “Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage” IEEE TRENSCATIONS ON INFORMATION FOENSICS AND SECURITY, VOL. 10, NO. 7, 2015.
9. Syed Rizvi and Katie Cover, Abdul Razaque “Third-Party Auditior (TPA): A Potential Solution for Securing a Cloud Environment” IEEE 2nd International Conference on Cyber Security and Cloud Computing 2015.
10. Boyang Wang, Baochun Li, Hui Li “privacy- preserving public auditing for shared data in the cloud” IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.
11. Cong Wang, Sherman S.M Chow, Qian Wang, Kui Ren, Wenjing Lou “Privacy-Preserving Public Auditing for Secure Cloud Storage” IEEE TRENSCATIONS ON COMPUTERS, VOL. 62, NO. 2, 2013.