International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 3 | Mar-Apr 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Third Party Public Auditing Scheme for Security in Cloud Storage

Heeth Shah, Jill Shah, Ushma Desai

Department of Computer Engineering, Shah and Anchor Kutchhi Engineering College,
Chembur, Mumbai, Maharashtra, India

How to cite this paper: Heeth Shah | Jill Shah | Ushma Desai "Third Party Public Auditing Scheme for Security in Cloud Storage" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.179-184, URL: http://www.ijtsrd.com/papers/ijtsrd21687.pdf

IJTSRD21687

ABSTRACT

By means of cloud storage, users can distantly store their data and enjoy the on-demand high-quality applications and services from a shared group of configurable computing resources, without the burden of local data storage and maintenance. However, the information that users no longer have physical ownership of the outsourced data makes the data integrity protection in cloud computing a difficult task, particularly for users with constrained computing resources. Moreover, users should be able to just use the cloud storage space as if it is local, without worrying about the need to verify its integrity. Thus, to enable public auditability for cloud storage is of serious importance so that users can rely on a third-party auditor (TPA) to verify the integrity of outsourced data and be worry free. To securely introduce a well-organized TPA, the auditing process should bring in no new vulnerabilities to user data privacy, and introduce no additional online burden to user. However; we propose a secure cloud storage system supporting privacy-preserving public auditing and monitoring. We additional would extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently, also integrity of data in cloud. Extensive security and performance analysis show the future schemes are provably secure and highly well-organized. Our beginning tryouts would be conducted on Amazon EC2 instance additional demonstrating the fast performance of the design.

1. INTRODUCTION

An emerging computer concept where data and services exist in a massively scalable data centers in the cloud and can be accessed from any connected devices over the internet. Storage of data in the cloud has revolved out to be a tendency. An increasing number of clients store their important data in distant servers in the cloud, with not leaving a copy in their local computers. Sometimes the data stored in the cloud is most important that the clients must guarantee it is not lost or corrupted. While it is easy to check data integrity after entirely downloading the data to be checked, downloading large amounts of data just for checking data integrity is a throwaway of communication bandwidth. Therefore, a set of works have been done on designing distant data integrity checking protocols, which permit data integrity to be checked without entirely downloading the data. Distant data integrity checking is initial introduced in which independently propose RSA-based methods for solving this problem. After that propose a remote storage auditing method based on pre-computed challenge-response pairs and monitoring method for better visualization of cloud products. The objective of Cloud Audit is to provide cloud service providers with a method to make their performance and security data willingly obtainable for potential customers. The requirement provides a regular way to present and share detailed, programmed statistics regarding performance and security. Regular information makes comparisons between providers easier; reducing the resources required for collecting the documentation and analyzes the data. Cloud Audit is planned to provide benefits for cloud computing providers as well. For illustration, the cost of responding to a potential customer's compliance controls may be very small for a large vendor. However, a small vendor may find it troublesome to provide that information to multiple potential customers. With Cloud Audit, vendors can provide information once and only update when there are changes. With the Google Cloud Monitoring API (Application Program Interface), you can read monitoring data from the Google Cloud Platform. Using this data, you can drive visualizations and alerts in Google Cloud Monitoring that can help you better understand your usage of Google Cloud products and assist you in detecting and investigating issues.

WHAT MAKES CLOUD COMPUTING DIFFERENT?

- **Its MANAGED**

One basic principle of cloud computing is that you no longer need to worry how the service you're buying is provided: with Web-based services, you simply concentrate on whatever your job is and leave the problem of providing dependable computing to someone else.

- **Its ON-DEMAND**

Just like electricity, you can buy as much or as little of a cloud computing service as you need from one day to the next. That's great if your needs vary unpredictably it means you don't have to buy your own gigantic computer system and risks have it sitting there doing nothing.

- **ITS PUBLIC OR PRIVATE**

The world biggest online retailer, Amazon, became the world largest provider of public cloud computing in early 2006. When it found it was using only a fraction of its huge, global, computing power, it started renting out its spare capacity over the Net through a new entity called Amazon Web Services. Private cloud computing works in much the same way but you access the resources you use through secure network connections, much like an Intranet.

1.1. Objective

To design and use a Third Party Auditor in Cloud Storage to enhance security and maintain data integrity. The flexibility and ease of use of the Third Party Auditor(TPA) is the biggest positive point. Being highly flexible on-the-go, doesn't require very high software and hardware capabilities. Its cost efficient and requires a steady connection. A large amount of people uses cloud applications in Smart Mobile Devices, Tablets, PDAs so security and maintaining data integrity in cloud storage is required necessarily. It's very feasible and convenient to use.

1.2. Problem Statement

The first issue is data integrity. In computer security, data integrity can be defined as "the state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alterations or destruction". Integrity of data stored at the entrusted cloud server is not guaranteed.

The second issue is unfaithful cloud server providers (CSP). There are many reasons why CSPs are not always trustworthy like, for saving money and storage space, CSPs may discard the data that has not been accessed for long time (which belongs to ordinary client) or sometimes even hide data losses or corruptions to maintain a reputation. To ensure integrity of outsourced data, data owner delegate the auditing task to trusted third party auditor. The persona of TPA is listed as follows

- Reduces the owner burden in managing the data.
- Ensure the client that the data stored in the cloud is intact and data integrity is maintained.
- Aid in achieving high economies of scale through customer satisfaction.
- The TPA is an independent authority that has expertise and capabilities to monitor the integrity of cloud data outsourced by the following two fundamental requirements have to be met

1. TPA should be able to audit the cloud data storage efficiently without asking for the local copy of data thereby reducing the on-line burden of cloud users.
2. The third party auditor informs user about data corruption or loss, if any. To securely introduce an effective third party auditor (TPA), the auditing process should not affect user data privacy.

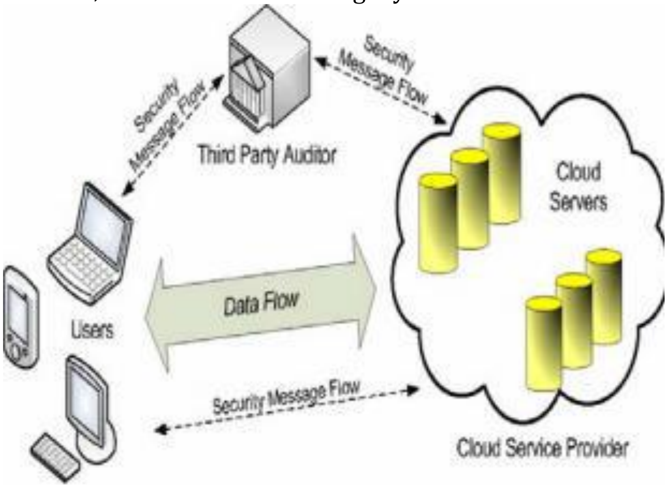
1.3. Methodology

The proposed scheme consists of three basic entities; they are data owner, cloud server storage and TPA. The data owner or the user is responsible for splitting the file into blocks, encrypting those using AES algorithm, generating a SHA-2 hash value for each, concatenating the hashes and generates a RSA signature on it. The cloud server is used to store the encrypted blocks of files. When the client or data owner request for data auditing to the TPA, it immediately requests for the encrypted data from the cloud server. After receiving the data, it generated the hash value for each block of encrypted files. It uses the same SHA-2 algorithm which was used by client. It later concatenates those hash values and generates a RSA signature for that file. In the Verification process, the signature generated by TPA and the one stored in the TPA which is provided by the data user are compared by the TPA. If they match with each other it means that the data is intact and data is not being tampered by any outsider or attacker. If it does not match, then it indicates that the data integrity has been affected or tampered. The result for the data integrity check is provided to the data owner.

Data owner is an important part of our proposed system. It performs most of the responsibility related to the data. In the proposed auditing scheme, the data owner first performs login and registration with cloud server and TPA. The new user has to firstly register itself by filling the registration form and be the active member of the system. A message for successful registration will be provided.

Once successfully login, the data owner will select the file he or she want to store on the cloud server. The file selected by him will be split into number of blocks. In order to carry out the splitting of the required file into blocks a File Splitter algorithm is used. In this algorithm, we check if the file exists or not. If exist, then the file is split in specific size based upon the file size.

Advanced Encryption Standard algorithm (AES) to provide confidentiality to the data. The blocks which are split are now encrypted using AES algorithm by the data owner. Each blocks of file will be encrypted and stored on the client. It encrypts data blocks of 128 bits using symmetric keys of size 128 bits. After encrypting the blocks, now a hash value for the blocks are generated separately. For this purpose, a hashing algorithm SHA-2 is being used. After the hashes are generated, the hashes for each blocks are concatenated and RSA digital signature is performed on it. Digital signatures are used to authenticate the source of messages. Later this signature is sent to the TPA, where it uses this signature to check the integrity of data stored in the cloud server storage is maintained or not. In the proposed scheme, to perform the task of data auditing a TPA is been used for this purpose. TPA performs data auditing either periodically or on demand by the client. On receiving the auditing request from user or data owner, the TPA starts its auditing process. TPA also stores the signature which has been generated by data owner. The TPA follows the same process performed by data owner such as generating hash for encrypted blocks of data files, concatenating them and generating signature on it. Later it compares the two signature in verification process. If it matches, then it means the integrity of data is maintained.



2. Literature Survey

In 2014 Mrs. Niyamat Ujloomwale et al. introduced Cloud computing is worthy of consideration and try to build business systems as a way for businesses in this way can undoubtly bring about lower costs, higher profits and more choice; for large scale industry, Data security has become the most important issue of cloud computing security. Though many solutions have been proposed, many of them only considers one side of security ;this paper proposes the cloud data security must be considered to analyze the data security risk, the data security requirements, deployment of security functions and the data security process through encryption. Distribution of file is done on cloud servers with token generation. The security architecture of the system is designed using encoding algorithms, which eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced. The system is acceptably secure, but that the level of encoding has to be stepped up as computing power increases. Results in order to be secured the system the communication between modules is encoded. Since the customer does not have control over data the cloud provider should assure the customer that data is not modified. In this paper a data correctness scheme is proposed in which a cloud service provider assures the user that the data is stored in the cloud is safe. This scheme also achieves the integration of storage correctness insurance and data error localization i.e., the identification of misbehaving server.

In 2015 Mrs. Swapnali Morea et al. proposed a secure and efficient privacy preserving public auditing scheme. It achieves privacy preserving and public auditing for cloud by using a Third Party Auditor (TPA). The data owner or the user is responsible for splitting the file into blocks, encrypting those using AES algorithm, generating a SHA-2 hash value for each, concatenating the hashes and generates a RSA signature on it. In the Verification process, the signature generated by TPA and the one stored in the TPA which is provided by the data user are compared by the TPA. If both matches, then data is intact and if mismatch occurs then it indicates that the data integrity has been affected or tampered.

In 2010 Mr. Wang et al. proposed another protocol that supports both public auditing and data dynamics by using BLS based HLA along with Merkle Hash Tree (MHT). It achieves the integrity of data but fails to provide confidentiality to the data stored on the cloud. Wang et al. has also proposed a design to detect the modified blocks easily using homomorphic token pre-computation and later erasure coded technique is used to acquire the desired blocks from different servers. Solomon et al. proposed protocol uses the same security level as Wang et al. but with better efficiency. It generates a signature set which is an ordered collection of signatures on each file block, thus incurring computation and communication overhead. Meenakshi et al. has proposed a protocol which uses TPA to audit the data of the users using Merkle Hash Tree algorithm. It supports data dynamics but fails to provide confidentiality to the data stored in the cloud.

In 2013 Mrs. Tejaswani et al. has achieved integrity of data using a Merkle hash tree by TPA and the confidentiality of data is achieved using RSA based cryptography algorithm whereas Jadhav et al. have introduced an attacking module which continuously keeps track on data alteration in the cloud. The attacking module is a small code which resides on cloud server. Confidentiality of stored data is achieved by encrypting the data using AES algorithm. Arasu et al. has proposed a method that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to enhance the security of TPA. It is a technique for verifying the integrity of a data transmitted between two parties that agree on a shared secret key. HMAC's are based on a key that is shared between the two parties, if either party's key is compromised, it will be possible for an attacker to create fraud messages.

In 2011 Mr. Ezhil Arasu et al. has proposed a method that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to enhance the security of TPA. It is a technique for verifying the integrity of a data transmitted between two parties that agree on a shared secret key. HMAC's are based on a key that is shared between the two parties, if either party's key is compromised, it will be possible for an attacker to create fraud messages.

3. System Requirements

3.1. Functional Requirements

The Data stored will be secured using AES Algorithm. It will maintain the Integrity Check Mechanism between Client and CSP. There will be Integrity check mechanism between client and third party auditor to ensure that the TPA cannot derive user's data content from the information collected during the auditing process. As our auditor is trusted Third Party Auditor, the privacy of data is preserved to protect the data from unauthorized access and to ensure that our data are intact.

The TPA will be able to properly monitor confidentiality and integrity of the data to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. The use of RSA algorithm and MD5 algorithm for encryption, cloud computing can be applied to the data transmission security. Proposed system mainly consists of four modules which are listed below:

- Login Module
- Third Party Auditor
- Cryptography
- Privacy-preserving

A. Login Module
In this module, there is multiple login

- User Login
- CSP login
- TPA login

The role of User, CSP and TPA are as follows:

- USER

Can register him or her with specific information. Then user can simply store data, file or application on cloud and received original decrypted data from cloud.

- TPA

Should encrypt and decrypt all users' data and save encrypted data on cloud. Also data integrity validation is done through challenge and challenge verification. TPA has privileges to see user's original data as well as encrypted data.

- CSP (Cloud Service Provider)

Provide space for storing data on cloud and response to challenge. But CSP doesn't have any privilege to see the original content of users file or data. So that privacy is preserved.

B. Third Party Auditor (TPA)
In this module, Auditor (TPA) views all List of Files Uploaded by User. Auditor directly views all user data without key. TPA has privileges to encrypt the user's data and save it on cloud. Also auditor can view data which is uploaded by various users. TPA can encrypt data and send it to Cloud service provider (CSP) for storage and auditor can view encrypted data of every user.

C. Cryptography
The art of protecting information by transforming it(encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. In our scheme, we had used RSA Algorithm to perform encryption and decryption on user's data. Due to encryption privacy is preserved as no one can see the data.

D. Privacy-Preserving
To ensure that the TPA cannot derive users' data content from the information collected during the auditing process. As our auditor is trusted Third Party Auditor, privacy is preserved. There is privilege for user to see only the files uploaded by that user only and not by other user. Privacy is preserved by both user and cloud service provider (CSP) as they don't have right to view the content of file

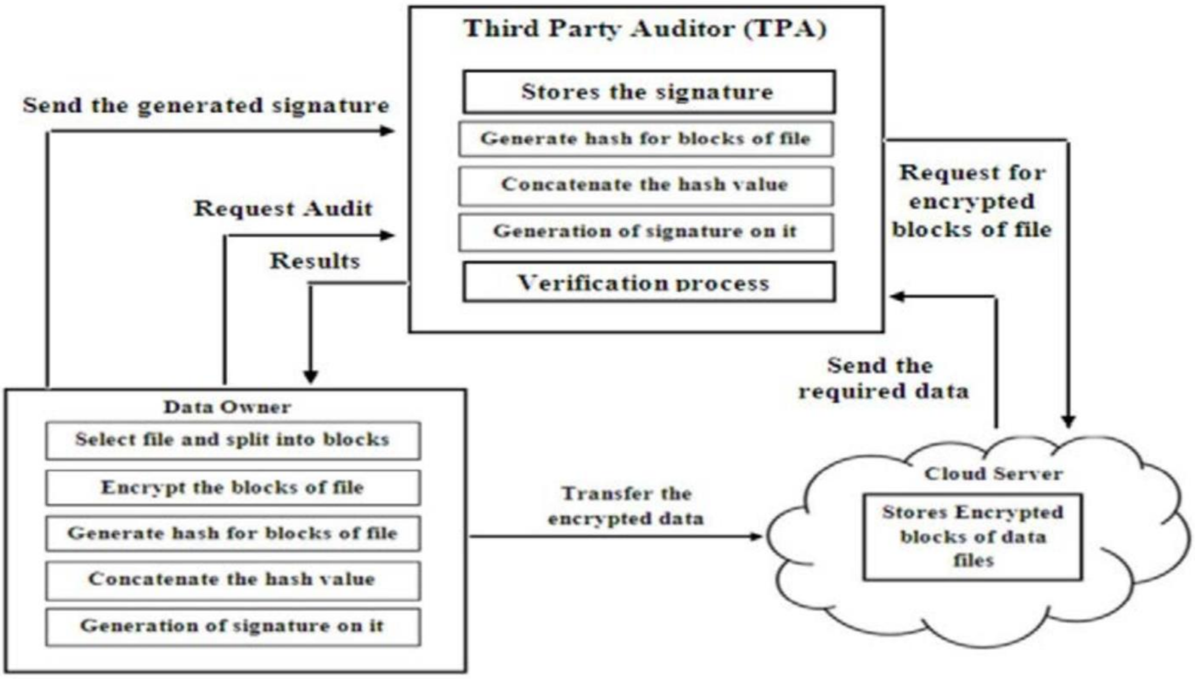
3.2. Hardware and Software Requirements
Hardware Requirements:

TYPE OF HARDWARE	HARDWARE REQUIREMENTS
Hardware	I3 Pentium Processor 32-bit system or 64-bit system 1.8 GHz processor
Disk Space	256 GB free disk space
RAM	4 GB RAM(recommended)

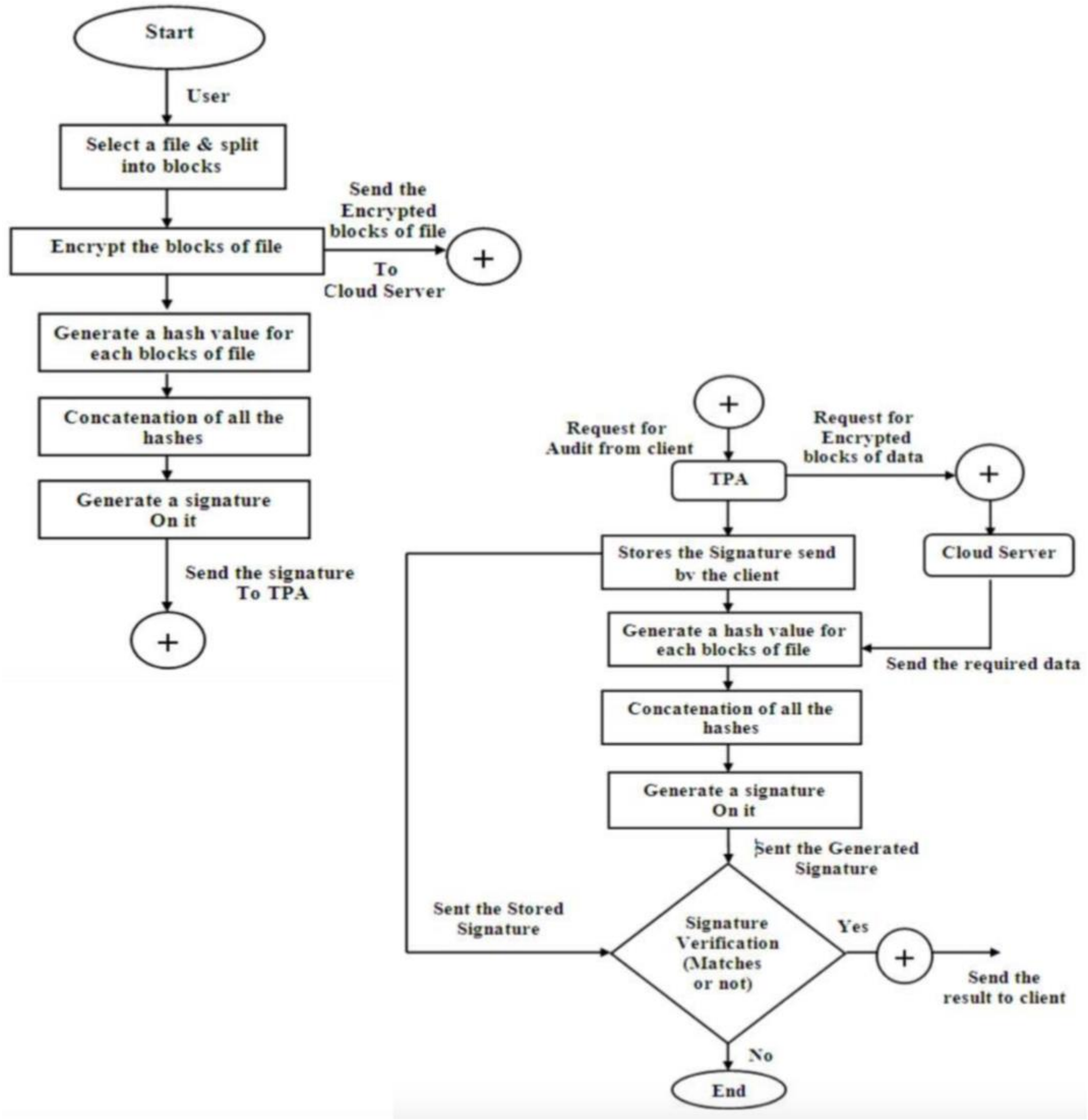
Software Requirements:

Operating System	Windows 7, 8, 10
Web browser	Google Chrome
Software Used	SQL server 2012 Visual Studio 2013 .Net Framework Amazon EC2/Local Server

4. System Block Diagram: -


Third Party Auditor (TPA)
Stores the signature
Generate hash for blocks of file
Concatenate the hash value
Generation of signature on it
Verification process
Send the generated signature
Request Audit
Results
Request for encrypted blocks of file
Send the required data
Data Owner
Select file and split into blocks
Encrypt the blocks of file
Generate hash for blocks of file
Concatenate the hash value
Generation of signature on it
Transfer the encrypted data
Cloud Server
Stores Encrypted blocks of data files

Working / Algorithm


Start
User
Select a file & split into blocks
Encrypt the blocks of file
Send the Encrypted blocks of file
To Cloud Server
+
Generate a hash value for each blocks of file
Concatenation of all the hashes
Generate a signature On it
Send the signature To TPA
+
+
Request for Audit from client
TPA
Request for Encrypted blocks of data
+
Cloud Server
Stores the Signature send by the client
Generate a hash value for each blocks of file
Send the required data
Concatenation of all the hashes
Generate a signature On it
Sent the Generated Signature
Sent the Stored Signature
Signature Verification (Matches or not)
Yes
+
Send the result to client
No
End

5. References

[1] Mrs. Niyamat Ujloomwale and Mrs. Ranjana Badre," Data storage security in Cloud", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. III (Nov – Dec. 2014), PP 50-56.

[2] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Wenjing Lou "Privacy-Preserving Public Auditing for Secure Cloud Storage.," Member, IEEE.

[3] "Monitoring Data Integrity while using TPA in Cloud Environment," ISSN: 2278 –1323, International Journal of Advanced Research in Computer Engineering &amp; Technology (IJARCET), Volume 2, Issue 7, July 2013.

[4] "Privacy-Preserving Public Auditing &amp; Data Integrity for Secure Cloud Storage," International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV100.

[5] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop on Hot Topics in Operating Systems (HOTOS '07), pp. 1–6, 2007.

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

[7] Jaspreet Kaur and Jasmeet Singh," Monitoring Data Integrity while using TPA in Cloud Environment," International Journal of Advanced Research in Computer Engineering &amp; Technology (IJARCET), Volume 2, Issue 7, ISSN: 2278 – 1323, July 2013.

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