ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Implementing Secure and Efficient Auditing Protocol for Cloud Storage

Prof. Anup S. Kunte[1], Sukhada S. Jadhav[2]

Assistant Professor, Dept. of Information Technology, KGCE, Mumbai, India[1].

M. E Student, Dept. of Computer Engineering, YTGOIFE College, Mumbai, India[2]

ABSTRACT: In cloud storage environment, data owners host their data on cloud servers and users can access the data from cloud servers. Due to the data outsourcing, this process of data hosting service introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Because, owner need to be convinced that the data are correctly stored in the cloud. Two-Party storage auditing system could not be guaranteed to provide proper auditing result thus Third-Party auditing is the better choice for the storage auditing in cloud computing. A Third-Party auditor is capable to do a more efficient work and convinces both the cloud service providers and the owner.

There are chances of data being lost or get misplaced in cloud storage environment. We calculate replication bytes and store them into secondary storage. Furthermore, divide the encrypted data file into fragments. With this work we combine best practices of both secure cloud storage and secure network coding in order to create more secure cloud storage architecture. We will also try to evaluate AES based encryption to make each fragment sufficiently encoded. It makes the auditor to receive only combined encrypted data instead of the original one as third party auditor be used to provide security services. The third party security service provider i.e. auditor would not store any data at its end, and its only confined to providing security service. Hence user will get the belief that his data is safely stored on the cloud and could retrieve data without any modification.

KEYWORDS: Storage, third-party auditing protocol, network coding, security

I. Introduction

Cloud storage refers to saving data to an off-site storage system which is maintained by the third party. The information is stored on computer's hard drive or other local storage device, and it is the saved to the remote database through Internet connection between your computer and the database. We need not to carry any physical storage device or use the same computer to save and retrieve your information. With the right storage system, we could even allow other people to access the data, turning a personal project into a collaborative effort.

Cloud storage is convenient and offers more flexibility. As Data Integrity is an essential in databases, similarly integrity of Data Storages is an essential in the cloud; it is a major factor affecting the performance of the cloud. It provides the validity of the data, assuring the consistency or regularity of the data. It is the complete mechanism of writing the data in a reliable manner to the persistent data storages which can be retrieved in the same format without any changes. Storing data at cloud data storages or data centres doesn’t ensure the integrity of data, but some mechanisms need to be implemented at each storage level to ensure the data integrity.

In traditional approach, owners can check the data integrity based on two-party storage auditing protocols. In cloud storage system, it is inappropriate to let the cloud or user to conduct such auditing, because they could not be guaranteed to provide auditing result. In this situation, third-party auditing is a natural choice for the storage auditing in cloud computing. A third party auditor has some capabilities to provide 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. The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds.

DOI: 10.15680/IJIRCCE.2017. 0501074

There are some existing remote integrity checking methods which can only serve for static archive data and therefore they cannot be applied to the auditing service because the data in the cloud can be dynamically updated. Thus, an efficient and secure auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. To verify whether the cloud lies to an audit query, the user needs to have some secret information on its side, which is computed according to a certain security level parameterising the probability of successful cheating. A secure cloud storage (SCS) protocol, a keyed protocol used for the user to generate data to be outsourced and subsequently query for auditing.

II. RELATED WORK

This section presents a summary of some existing review articles related to secure data sharing in the Cloud. These focus on main requirements that enable the secure data sharing in the cloud instead of focusing specifically on secure data sharing in cloud. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people.

A. DEFINITION OF A SYSTEM MODEL

Below Fig 2.1 shows the data hosting process. This process involves communication among three entities Cloud server, Owners and Auditor. The data verification is done by creating challenges and proofs for data integrity. The auditor can be a trusted organization managed by the government, which can provide unbiased auditing result for both data owners and cloud servers.

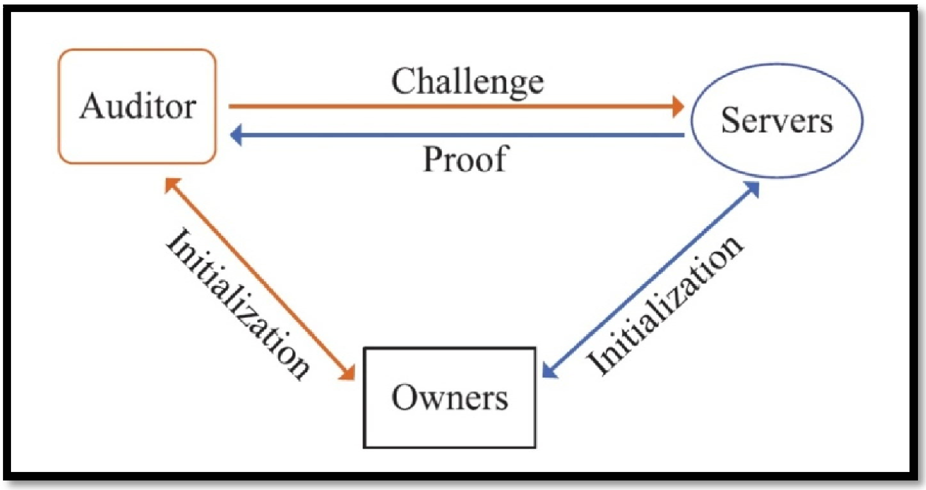

Fig.1. System model of the data storage auditing [2]

B. REVIEW OF EXISTING SYSTEM

In recent paper Chen, Xiang, et al [2], have designed a general construction of secure cloud storage protocol based on any secure network coding protocol. Chen and Zhao [8] outline the requirements for achieving privacy and security in the Cloud and the requirements for secure data sharing in the Cloud.

There are many examples [6] of insider attacks such as Google Docs containing a flaw that inadvertently shared user documents, MediaMax going out of business in 2008 after losing 45 % of stored client data due to administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on a number of occasions. It's clear from many of the reviews, that the Cloud is very susceptible to privacy and security attacks and currently there is on-going research that aims to prevent and/or reduce the likelihood of such attacks. The importance of data sharing and the need to ensure privacy and security is discussed in a number of existing articles.

III. PROPOSED ALGORITHM

This section presents the system model of storage auditing protocol which gives the solution for data integrity checking and security model for a storage auditing system. In this application, Owner will upload his data and it is securely stored at server using AES encryption. In this scenario there are chances of data loss due to system crashes or any disaster. In such situation owner's data should be protected from this and should be kept safely on the cloud server. For this purpose we divide the encrypted data file into fragments each of equal size (i.e. size of 3 bytes) and store the fragmented data over the cloud. Every fragment is having random coefficient *ei* as per network coding.

Auditor gets email of list of combined data which is then requested by the system. There is verification of each fragment id and its coefficient for combined data, which is entered by auditor. If all fragments are valid then status valid will be displayed to both auditor and owner. Invalid status will be displayed to auditor and owner when any one fragment is invalid.

To download the data, there is checking of fragments in main storage. If fragments are available in main storage then data will be downloaded from main storage. Otherwise, data will be downloaded from secondary storage. Owner will be download data through AES key, which is received by him earlier.

Hence user will get the belief that his data is safely stored on the cloud and could retrieve data without any modification. So that owner would remain unaware about any data loss situations and get his original data. Thus it helps to achieve data integrity.

IV. PSEUDO CODE

```
Step 1:  Generate AES key and transmitted to owner upon file uploading.
Step 2:  Generate a random byte ‘b’ value for each user and calculate replication bytes = encrypted bytes (Ex-OR b)
Step 3:  Store replication byte in secondary storage.
Step 4:  Divide encrypted data into fragments and calculate random co-efficient ei for each fragment.
Step 5: Auditor will get combined data (fragment id + ei) where each fragment id and its co-efficient will be verified.
Step 6:  If all fragments are valid then display valid status to auditor and owner; else display them invalid status.
Step 7: Check all fragments in main storage; if fragments are not available then retrieve the data from secondary storage else retrieve fragments from main storage.

Step 8: Owner will download data using AES key received earlier.
Step 9: End.
```

V. SIMULATION RESULTS

Before uploading the data to the cloud server, owner encrypts his data with AES symmetric encryption algorithm. Since RSA algorithm could not encrypt the data more than 8GB, we will require to create huge amount of small data chunks; thus causes the slow encryption. Because in cloud storage system, numerous data is being uploaded dynamically we will try to use AES encryption algorithm. Since, it is faster, more efficient, and superior in terms of time consumption and throughput under the scenario of data transfer and also used to achieve faster performance and low computational overhead.In our case symmetric key is used and it delegates the burden of key management to the third party auditor. With the use of symmetric key encryption the master key or private key usage which would be stored in security cloud provider per user gives the client the advantage like, freedom from remembering any key. Therefore, it would be better to use AES scheme in encryption of data stored at other end and need to decrypt multiple time.

In below screenshot we can see how efficiently file is getting encrypted and decrypted upon its uploading and downloading.The third party auditor can only view the encryption and decryption of uploaded file by using ‘Graph Encryption’ and ‘Graph Decryption’ menues respectively.

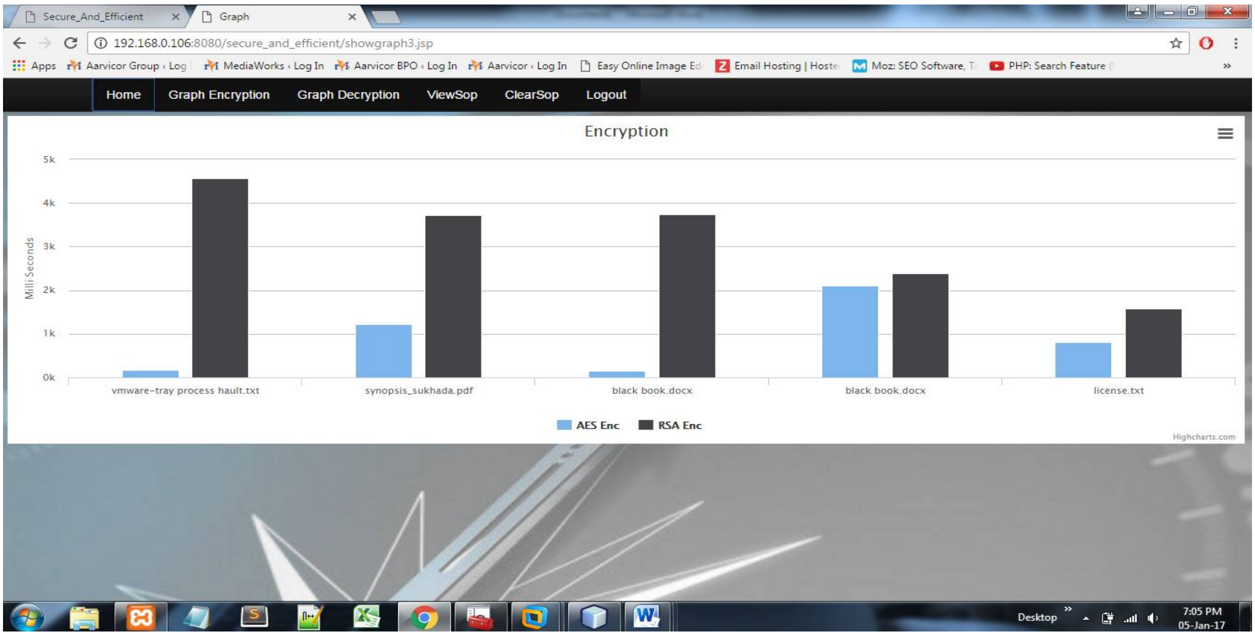

Fig. 2. Difference while encrypting uploaded file

Fig.2.shows the graphical representation of the result i.e. encryption performed on uploaded file using AES encryption algorithm and it is then compared with encryption performed using RSA encryption algorithm for testing the response time.

Fig.3. Represents the output for decryption performed using AES algorithm and compared with the output for the same by applying RSA algorithm.

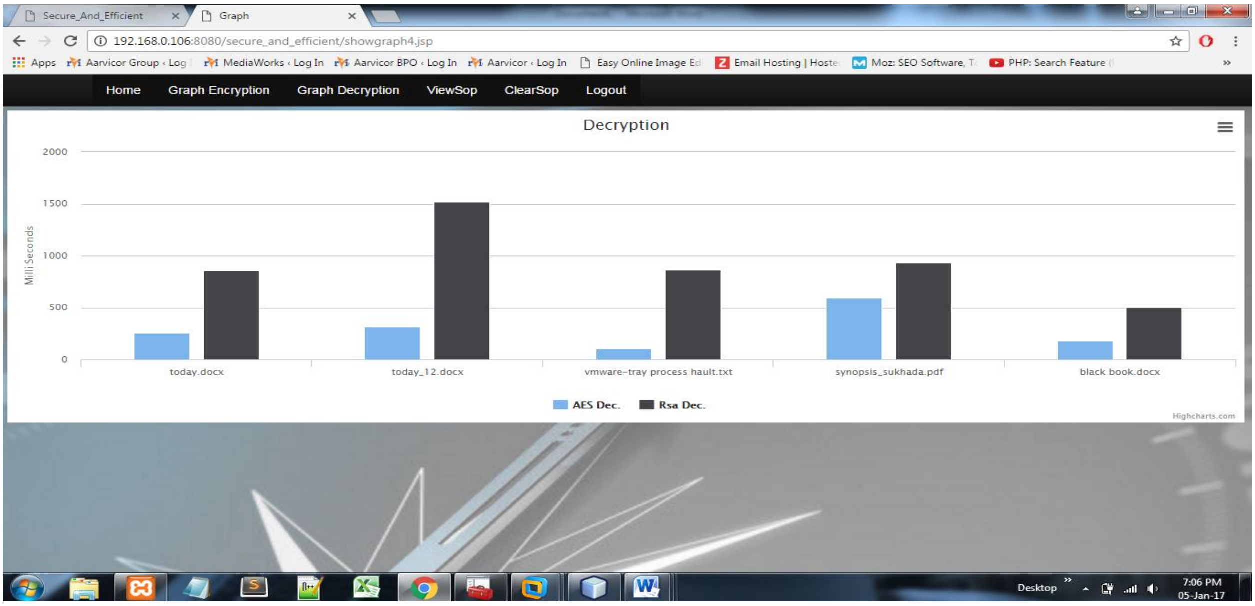

Fig. 3. Difference while decrypting uploaded file

VI. Conclusion and Future Work

With this project work, we proposed an efficient and secure storage auditing protocol. It protects the data privacy against the various security concerns. It also assures the data integrity as we are taking back up of this data into secondary storage server. As most of computation is processed on auditing server, the load on cloud server gets reduced. The fragmentation ensured that no significant information was obtainable by an adversary in case of a successful attack. Thus it helps to achieve data integrity, data availability as well its confidentiality. We have seen how delegation of responsibility of third party auditor which provides security services to secure user data. It reliefs the user from maintaining any kind of key information. It allows the user to verify the integrity of the data stored on own load or retrieval of its own stored data in cloud. The client can share the data securely without any overhead of key distribution.It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The future work will save the time and resources utilized in downloading, updating, and uploading the file again.

References

1. Fei Chen,Tao Xiang,Yuanyuan Yang,Sherman S. M. Chow : Secure Cloud Storage Meets with Secure Network Coding, IEEE INFOCOM 2014 - IEEE Conference on Computer Communications.
2. K. Yang and X. Jia, : An efficient and secure dynamic auditing protocol for data storage in cloud computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013.
3. Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo : Secure Data Sharing in the Cloud", DOI: 10.1007/978-3-642-38586-5_2,©Springer-Verlag Berlin Heidelberg 2014.
4. A. Juels and B. Kaliski Jr : Pors: Proofs of retrievability for large files,” in ACM Conference on Computer and Communications Security (SP), 2007, pp. 584–597.
5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in ACM Conference on Computer and Communications Security (CCS), 2007, pp. 598–609.
6. Huang R, Gui X, Yu S, ZhuangW (2011) Research on privacy-preserving cloud storage framework supporting cipher text retrieval. International conference on network computing and information security 2011:93–97.
7. Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun Surveys Tutorials 99:1–17.
8. Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. International conference on computer science and electronics, engineering, pp 647–651.
9. Oza N, Karppinen K, Savola R (2010) User experience and security in the cloud-An empirical study in the finnish cloud consortium. IEEE second international conference on cloud computing technology and science (CloudCom) 2010:621–628.
10. Sarathy R, Muralidhar K (2006) Secure and useful data sharing. Decis Support Syst 204–220.
11. Butler D Data sharing threatens privacy, vol 449(7163).Nature Publishing, Group, pp 644–645.
12. Feldman L, Patel D, Ortmann L, Robinson K, Popovic T (2012) Educating for the future: another important benefit of data sharing. Lancet 1877–1878.

BIOGRAPHY

Sukhada Suryakant Jadhav received bachelor’s degree from University of Mumbai in 2013. Now a P.G student in YTGOIFE College, University of Mumbai, India. Research interest in Cloud Security.