International Journal of Computer Engineering and Information Technology

VOL. 8, NO. 9, September 2016, 179–183
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

Implementation of Privacy Preserving Model for Shared Data in the Cloud

Geetanjali Rokade[1] and Prof. Sambhaji Sarode[2]

[1, 2] Computer Department, MITCOE, Savitribai Phule Pune University, MS. 411030, India.

[1]srokadegitanjali@gmail.com, [2]sambhaji.sarode@mitcoe.edu.in

ABSTRACT

Cloud Computing gives storage services where user can remotely stores and access data. Cloud services can be used for different purposes such as data sharing in different domain, limiting the access rights to some groups, reduces the load of maintenance and security of data on intranet network. Currently, due to failure in system, maintain the integrity of cloud data is vulnerable. However, maintaining the integrity of shared data in to cloud using public auditing is a vital task. Therefore, proposed third party auditor solution to keep and maintain integrity of data and preserve privacy of shared data in the cloud. Hashing algorithms and confidentiality algorithm with addition of salt enhance the integrity of data. In addition to above, data anonymization technique is also used to keeping the secrecy of shared data. It enhances the data protection of existing and upcoming data. Therefore, proposed system will perform audit for some specific groups or multiple users efficiently

Keywords: *Cloud Computing, Public Auditing, Privacy Preserving, Data Storage.*

1. INTRODUCTION

In today's life everything is depends on internet, and cloud computing is the invention which usages progressive computational power and advance data storing and data sharing capabilities. Cloud computing could be a general term for the entire world that involves providing hosted facilities above the net. These facilities generally separated into 3 categories: (IaaS) that is Infrastructure-as-a-Service (PaaS) that is Platform-as-a-Service, and (SaaS) that is Software-as-a-Service. The cloud facilities has different characteristics which differentiate it from ancient hosting. IaaS provides physical resources like central processing unit, storage and network etc. PaaS offers a platform for implementation of different application. SaaS offers completely different types of application and net services to different clients. Cloud is nothing but the large group of interconnected computers, on which we can store large number of data and run different application. Cloud provides shared pool of configurable computing resources and on demand network access. Main benefit of cloud is that cost reduction; whereas disadvantage is nothing but the security. The cloud computing security has set of number of policies and technology which protect application, data, and related Infrastructure. Some privacy and security issues have to be considered. The only thing was that the cloud computing lacks regarding the issue of data integrity, data accessed by unauthorized user and data privacy [9]. Data integrity is nothing but the consistency of data, maintaining integrity of data in cloud is difficult task. And number of techniques has been proposed to protect integrity of data. Through this number of techniques the integrity can be checked and verify unauthorized change in original data without requesting original copy of data.[3]. The rest of the paper is divided into following sections. Section II Literature survey. Section III Implementation Details. IV Conclusion. Acknowledgment and References for the survey.

2. LITERATURE SURVEY

Qian W. et al. were used an easily adaptable distributed storage reliability auditing scheme in that they permitted users to audit data at low communication and low computation cost in cloud. It also allows very fast error localization but it again ensures strong accuracy guarantee [2]. Cong W. et al. proposed a scheme in that they used Homomorphic token with support of distributed verification to the erasure-coded data , this method is used for combinations about storage exactness and detecting of misbehaving servers.This scheme supports safe and proficient dynamic operations like delete, update and append [3]. Kan Yang etl. Implement auditing structure of a cloud data storage systems which propose an effective preserving privacy of auditing protocol. PoR method which is used to create an encoded result by using the Bilinearity property of some bilinear pairing. It means, in that the auditor can’t decode it but they can verify the surety of that proof. Without mask technique no need of any trusted organizer at the time of batch auditing for number of clouds. Besides, this method, they allow to the server to compute intermediate value of the verification that is the auditor easily use that value to evaluate the exactness of the proof [4]. Xuefeng L. et al. proposed that secure number of owner data distribution scheme. In cloud Sharing of data at multi-owner manner is the challenging issue at the time of preserving the privacy of data from an untrusted cloud so this scheme proposed as dynamic grouping in cloud, with the help of this and using group signature and also dynamic broadcast encoded method [5]. Bonyang Wang et al. Proposed that a novel Privacy Preserving Technique which support the shared data public auditing in the cloud. System uses Homomorphic Authenticator technique with ring signature to verify and compute the exactness of the stored data. Signature on each and every block of data is kept private from the TPA how verifies the data and also verify the data honesty (integrity) without access the whole data files. This is useful to do simultaneous number of auditing task instead of verify it one by one [9]

Table 1: Liturature Survey

SR. NO .	TITLE	METHODS	PROS	CONS
1	Privacy Preserving Public Auditing for Secure Cloud Storage.2013[1]	Homomorphic Linear Authenticator , Random Masking	This method allow Safe public data auditing.	Privacy of data cannot preserve.
2	Towards Secure and Dependable Storage Services in Cloud Computing. [2]	Homomorphic Token along with Distributed Erasure-Coded Data	Audit cloud data with lightweight communication and computation cost	System is safe but some user files where not encoded so data confidentiality is violated.
3	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. sep. 2013.[4]	Proof of Retriviability with bilinearity property of bilinear paring	Low communication and computation cost	This scheme does not support the efficient preserving privacy for public data auditing of store (shared) data.
4	Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. May 2011. [6]	Message Authenticated code	It provide secure auditing of shared data	High communication and computation complexity.
5	Oruta: Privacy Preserving Public Auditing for shared Data in the cloud. January-March 2014.[8]	Homomorphic Authenticator along with ring signature	Perform multiple document verification simultaneously rather than one by one	1. Traceability and data freshness could not check while preserving the identity privacy. 2. Data re-computation
6	Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud. January/February 2015 [9]	Homomorphic Authenticator with proxy re-signature	Preserve identity privacy And also audit data efficiently.	Achieving blockless verifiability of two level signature and verify them together in public auditing technique.

3. IMPLEMENTATION DETAILS

Here is the discussion of proposed system architecture, its flow structure and then the modules of the system.
In previous system data was stored in the cloud but for maintaining the privacy and integrity of users original data they used the Homomorphic Ring Authenticator and proxy re-signature. Using this methods, data can be analyzed and privacy of the shared data can be maintained.

3.1 Proposed system

Proposed system consist of one servers which is the main server where user information is stored along with documents to share. And the admin is used to analyze the data. Propose system is a good and useful distributed theme along with particular dynamic data support which make certain correctness of user and user's knowledge within cloud. System have tendency to produce guarantee and redundancies of the information irresponsibleness. System objective is nothing but to make up a warehouse to facilitate information and share across cloud in conjunction with preservation of knowledge privacy. For that system is uses a good coding technique to produce data security on data storage.

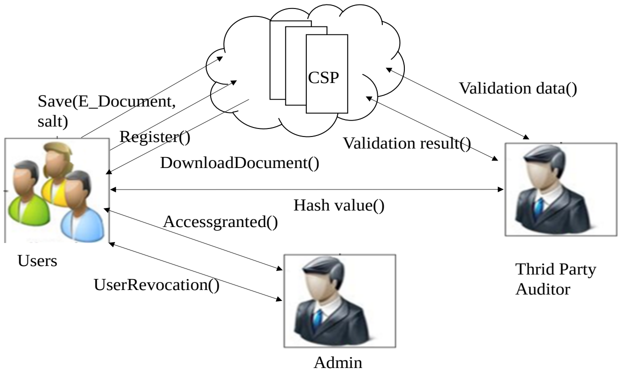


Fig. 1. System Architecture

As above Figure 1 shows that, encrypting the information before storing in cloud will handle the confidentiality issue and to make assured accuracy of users data in cloud system have a tendency to used TPA, thus planned system offers effective and economical users information exactness with minimum communication, computation and storage overhead. In past, cloud computing has huge growth within the company business, particularly because the technology caters to media ability and accessibility. System objective is to build a security services that can be supplied with a sure third party, and would result in providing solely security services. Main aim to be bringing home the salt is providing security to knowledge publically cloud by specializing in a pair of necessary issues:

1) Integrity
2) Privacy
Detailing it an additional.

1. To construct internet services system might offer data integrity verification, and encryption/decryption of the buyer information.
2. Process access list for sharing information firmly with particular band of people.
3. To create thin consumer application which might be decision of those internet service such as before uploading/downloading that knowledge to and from the cloud.

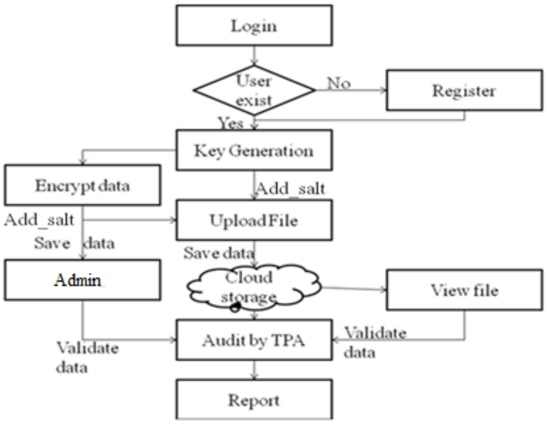


Fig. 2. Flow Diagram

3.2 Implementation details

1) Module I: In this the data store in cloud and enjoy the high end services from any cloud service provider like as Amazon, Google, IBM, Microsoft etc. on pay-as-you-go basis. In this, number of data owners and group users shared their data on the cloud then generation of public key and private key for every individual user, for this key generation we use RSA (pukey, skey) for registered user and registered data will get stored on main cloud.

2) Module II: Cloud service provider like a iCloud , Drop box and Google Drive provides the storage services for user and manage the stored data in cloud. While uploading any document system will encrypt the document first and then generate the digital signature for that document with the help of pukey and store it on both main server and proxy server. Digital signature is generated using SHA with RSA.

3) Module III: The Third Party Auditor (TPA) is an object which performed verification of stored data in cloud. This module is all about ensuring data confidentiality, TPA will generate its own digital signature using users data and public key and verify it with old generated digital signature, if signature verified then data is not violated else the data is violated.

4 . MATHEMATICAL MODEL

Mathematical model is nothing but the mathematical explanation of the system. The proposed system is represented using set theory. Let S be the proposed system. Let S = {D, E, S, PK, SK, Tds}

Ui= Users {U1, U2, U3, U4 …}

D- Shared Data {D1, D2, D3 …}

E-Encryption

S- Salt

C-Cloud

Pukey - User Public Key (PK)

Skey- Secret key (SK)

Tds - (TPA's) Third Party Auditor

Upload

Plain text doc (D)+random number(salt/S) => E

SK+E =>Tds =>Hi

PK+Di=>C

Download

Ui=>Ski+E'=> Tds=>H'I

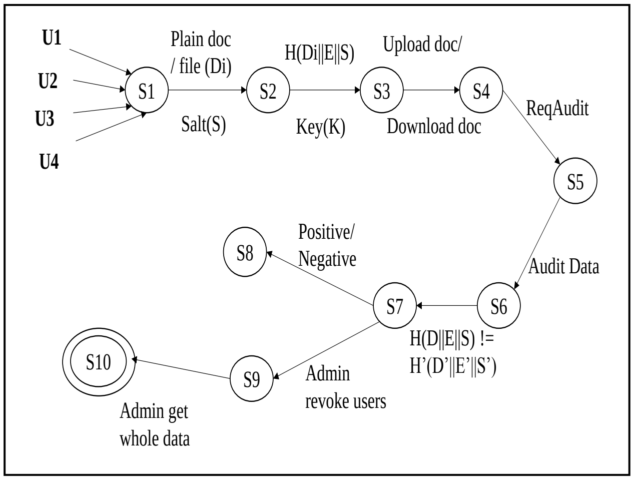
Pk'+D'i=> C

Verify :

Hi(D || S) = Hi'(D|| S) => positive

Hi(D || S) != Hi'(D|| S) =>Negative

State Transition Diagram



5 .EXPERIMENTAL RESULT

The result shows that the Encryption time, Checksum/Hash Calculation time and the Decryption time that all are depends on the size of the file. As the size of file is more it takes more time for encryption and decryption and also for addition of salt in that document.

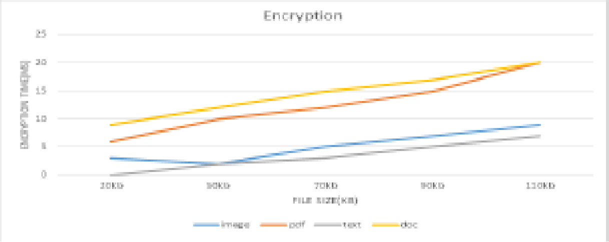


Figure 13.1: Encryption time

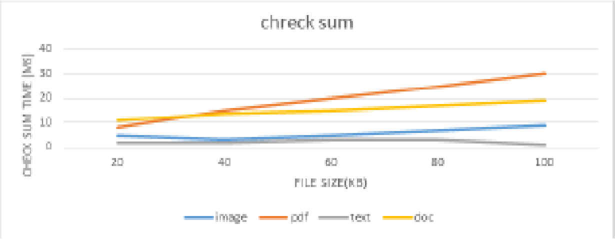


Figure 13.2: Hash calculation time

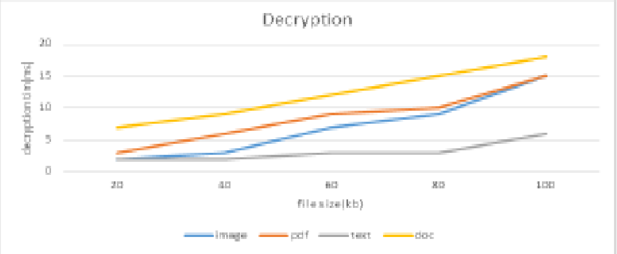


Figure 13.3: Decryption time

This graph shows the revocation time is depends on the downloading speed of the data.

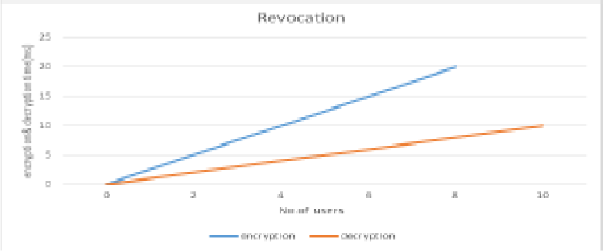


Figure 13.5: Revocation time

Graph shows the auditing efficiency of proposed system it shows that the auditing time is directly proportional to the number of users that is as the number of user's increases auditing time also increases.

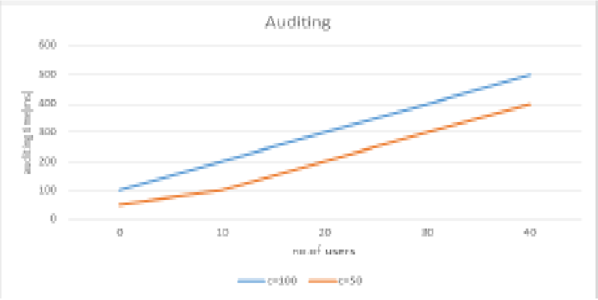


Figure 13.6: Auditing time

6. CONCLUSIONS

In many organizations the main issues is maintaining the security and privacy of confidential data. Cloud store different types of data for example documents, digital media object, data sheets and it is necessary to give guarantee about data confidentiality. Data privacy, integrity and auditing are the terms which examines all stored data to maintain privacy and integrity of data and give data confidentiality. Proposed system will preserve the secrecy of shared data which is store in cloud.

7. ACKNOWLEDGMENTS

I enormously thanks to Prof. Sambhaji Sarode, Computer Engineering Department MIT COE for their valuable guidance, continue inspiration and motivation at every stage of my project work during the semester. And I even thankful to all staff how directly or indirectly support me. To be obligated an inordinate deal of love to my family for their sanctifications and constant moral support.

REFERENCES

[1] The template C. Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou," Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions On Computers, Vol. 62, No. 2, February 2013

[2] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, "Towards Secure and Dependable Storage Services in Cloud Computing"

[3] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology Email: {cwang, qwang, kren}@ece.iit.edu "Ensuring Data Storage Security in Cloud Computing".

[4] Kan Yang "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactions OnParalleland Distributed Systems, VOL. 24, NO. 9, SEPTEMBER 2013

[5] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[6] Qian Wang, IEEE, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011.

[7] S. Ashli, B. Gowrie, S. Acanthi, "Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm", in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013.

[8] B. Wang, Student Member, IEEE , B. Li, Senior Member, IEEE, and Hui Li, Member , IEEE "Oruta: Privacy Preserving Public Auditing " IEEE Transaction On Cloud Computing Vol.2, No.1, January-March 2014.

[9] B. Wang, Student Member , IEEE, B. Li, Senior Member, IEEE and Hui Li, Member, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud ", IEEE Transaction On Services Computing, Vol.8, No.1, January/February 2015

[10] Jachak K. B. and GagareG.J."Homomorphic Authentication with Random Masking Technique Ensuring Privacy and Security in Cloud Computing" , Bioinformatics Security Information ,vol.2,no.2,pp.49-52,ISSN.2249-9423,12 April2012

[11] B. Wang, B. Li and H. Li, " Public Auditing for Shared Data with Efficient User Revocation in the Cloud ", Proc.IEEE INFOCOM, pp.2904-2912, 2013.

[12] Bin Zhou, Jian Pei , "A Brief Survey on Anonymization Techniques for Privacy Preserving Publishing of Social network data".

[13] Shivani Gambhir, Ajay Rawat ," Cloud Auditing :Privacy Preserving using Fully Homomorphic Encryption in TPA" . IJCA(0975-8887) .vol 80-No 14,October 2013.