Providing Security for storage and auditing of cloud data

Pooja Patil, Ram Joshi

Abstract— Cloud computing is gathering of existing system and advances, bundled inside another framework standard that offers enhanced adaptability, versatility, business skill, quicker startup time, decreased administration costs, and without a moment to spare accessibility of resources. Cloud computing is an Internet-based figuring and utilization of computer technology which gives access to resources as an administration, for example, storage, system, server and processors and so forth. By moving information into the cloud offers incredible straightforwardness to clients. By and large, server farm in cloud holds data that clients have put away on their machines. The security concerns emerge in light of the fact that the outsourced information is utilized by the client. Cloud computing is the developing field now a days. The stage gives help to decrease the expense and additionally make the powerful usage of the equipment and also programming. Information storage is the fundamental most alluring part of the cloud computing, however it accompanies some security challenges as well. The end clients store their information on cloud server are constantly in stress that either their information put away is secure or not? As the information put away is extensive enough so clients can not check its uprightness intermittently. Off and on again cloud administration suppliers may carry on unhonestly and erase clients information Or they neglect to roll out improvements on the information which is redesigned by the clients regularly. So to conquer these difficulties the Trusted Third Party Auditor assumes the crucial part in the interest of clients. As they guarantee to clients that the information facilitated on the server is secure. TPA gives more simpler and reasonable route for clients to their capacity accuracy in cloud, which likewise supportive for the cloud administration suppliers to enhance their cloud based administration stage. In other way we can say reviewing plan assume a critical part in foundation of secure cloud stage in clients personality and expand the cloud economy, where clients gets to the danger and apply their trust in the cloud to store information all the more accurately.

Index Terms— Cloud, Third party auditor, Privacy, Data storage, Public auditing, Security, User

1. INTRODUCTION

Cloud computing has been imagined as the next generation information technology (IT) construction modeling for undertakings, because of its long rundown of extraordinary focal points in the IT history: on-demand self-service, universal system access, location independent asset pooling, fast asset flexibility, utilization based evaluating and transference of danger. One key part of this ideal model moving is that information are being concentrated or outsourced to the cloud. From clients' point of view, including both people and IT undertakings, putting away information remotely to the cloud in an adaptable on-interest way brings engaging advantages: easing of the trouble for capacity administration, general information access with location independence and shirking of capital use on hardware, software, and personnel maintenances, etc.[3]. While cloud computing makes these focal points more attractive than at any time in the past, it additionally brings new and challenging security dangers to clients' outsourced information. Since cloud administration suppliers (CSP) are distinct administrative entities, information outsourcing is really giving up client's definitive control over the destiny of their information. Thus, the rightness of the information in the cloud is being put at danger because of the accompanying reasons. As a matter of first importance, despite the fact that the system under the cloud are a great deal more influential and solid than individualized computing gadgets, they are as yet confronting the broad range of both inward and outside threats for information reliability. Second, there do exist different inspirations for CSP to carry on unfaithfully at the cloud clients with respect to their outsourced information status. For illustrations, CSP may recover stockpiling for money related reasons via tossing information that have not been or are infrequently accessed, or even hide information disaster occurrences to keep up a reputation. To put it plainly, although outsourcing information to the cloud is financially appealing for long term expansive scale storage, it doesn't instantly offer any assurance on information trustworthiness and accessibility. This issue, if not legitimately addressed, may impede the success of cloud architecture.

To completely guarantee the information honesty and spare the cloud clients' processing assets and in addition online load, it is of basic vitality to empower open inspecting administration for cloud information stockpiling, with the goal that clients can ask to an autonomous outsider inspector (TPA) to review the outsourced information when required. The TPA, who has aptitude and capacities that clients don't, can

intermittently check the uprightness of all the information put away in the cloud for the clients, which gives a substantially more simple and moderate path for the clients to guarantee their capacity accuracy in the cloud. In addition, not withstanding help clients to assess the danger of their subscribed cloud information benefits, the review result from TPA would likewise be valuable for the cloud administration suppliers to enhance their cloud-based administration stage, and even fill for autonomous mediation needs.

2. LITERATURE SURVEY

In public auditability for storage security paper, authors have studied the issue of guaranteeing the trustworthiness of information stored in cloud computing rule mining. Ordonez et. It considers the assignment of permitting third party verifier, to confirm the honesty of data put away in the cloud. This paper accomplishes both open auditability and data dynamics operations. It first distinguishes direct extensions with fully dynamic data updates from prior works and then shows how to construct an elegant verification scheme for the seamless integration of these two features in protocol design. Later, privacy preserving data integrity checking paper has included information honesty while examining the cloud information where in proposed convention never reveals the information to verifier. This solution removes the trouble of check from the client, reduces both the clients and storage administrations fear of data leakage. This solution gives storage administration responsibility through independent, outsider evaluating and intervention. The protocol has three critical operations: Initialization, Audit and Extraction. This convention principally concentrates on audit and extraction. For audit, the auditor cooperates with the administration to watch that the put away information is in place. For extraction, the auditor interacts with the administration and client to watch that the information is in place and return it to the client [8]. Restriction of this technique is it doesn't help dynamism. To backing the same, technique PDP came into picture which is prior scheme of dynamic PDP where client preprocesses the information and after that it will be sent to cloud server for storage. While doing this, client will store some of metadata with them. This put away information will be checked by client by asking server to demonstrate that put away information has not been changed or erased without recovering the entire information for inspecting. However this plan is not considering data dynamics, It applies just to static information. Subsequently progressive dynamic PDP plan covers limit of normal PDP scheme by extending it with support to provable updates of stored data. It utilizes new version of authenticated dictionaries based on rank information. To help open auditability with protection, privacy preserving public auditing for data storage security in cloud computing paper have proposed a system for data storage security in cloud computing. It uses the homomorphic linear authenticator and random masking to ensure that the TPA would not realize any learning about the data content put away on the cloud server among the efficient inspecting methodology, which not just dispenses with the trouble of cloud client from the tedious and perhaps costly examining task, additionally dispels the clients hesitation of their outsourced information leakage. Considering TPA might simultaneously handle numerous review sessions from diverse clients for their outsourced information records. Likewise help security saving open evaluating convention into a multiuser setting, where the TPA can perform numerous inspecting tasks in a group way for better efficiency [1]. They have demonstrated the security and legitimize the execution of proposed plans through concrete experiments and comparisons with the state-of-the-art.

3. MATHEMATICAL MODEL

- Generation of Keys:

  INPUT: Two distinct Prime numbers x and y, ϕ (n)=(x-1)(y-1) and n=x*y and e such that1<e<ϕ(n) d ≡ e−1 (mod ϕ(n))

  OUTPUT: Public Key is (e,n) Private Key is (d,n)

- Encryption:

  INPUT : Private Key (d ; n), Public key (e; n) and Data to be signed D

  OUTPUT: S (signature of D)

  1) E = h(D) ;

  2) S =E^d mod n;

  3) Return (s)

- Verify Proof:

  INPUT: Signature S, public key of sender (e,n) OUTPUT:

  1) E′=S^e mod(n);

  2) E=h(D) (from the CSP)

  3) If E=E′ then file is original else modification is done.

4. SCHEME DISCRIPTION

As shown in below system architecture, proposed system comprise of three major components:

Client: User can be individual entity or association who will store their information in cloud and depend on cloud for information processing.

Cloud Service Provider: CSP has critical assets and ability in building and overseeing circulated distributed storage servers.

Third Party Auditor: TPA has capability and abilities that clients might not have. TPA is trusted to evaluate and uncover danger of distributed storage benefits for the benefit of client's solicitation.

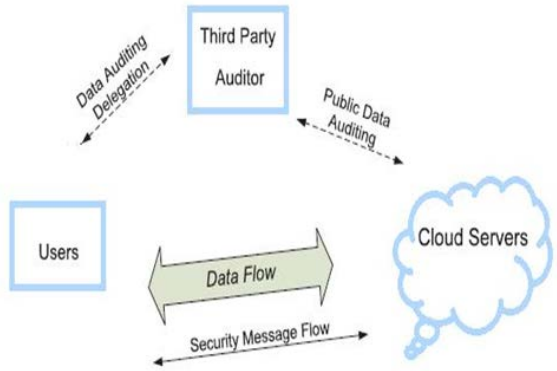

Fig.1: System Architecture

In the cloud standard, by putting the vast information documents on the remote servers, the customers can be relieved of the trouble of storage and processing. As customers no more have their information locally, it is of discriminating significance for the customers to guarantee that their information are in effect accurately put away and kept up. That is, customers must be equipped with certain security implies so they can occasionally confirm the accuracy of the remote information even without the presence of nearby duplicates. So,they can designate the observing assignment to a trusted TPA. In the proposed plan,TPA in possession of the public key can act as a verifier. We assume that TPA is unbiased while the server is untrusted. For application purposes, the clients may interact with the cloud servers via CSP to access or retrieve their pre-stored data. More importantly in practical scenarios, the client may frequently perform block-level operations on the data files. The most general forms of these operations we consider are modification, insertion and deletion.

There are 5 modules in proposed system as given below:

1. File Encryption

2. Distribution Of File

3. Public Verifiability with privacy

4. File Retrieval

4.1 File Encryption

Let the client U wishes to store the file F on cloud server. To start with, User will generate private and public key and then file will be encrypted using public key generated by RSA algorithm. Once file is encrypted, it will be uploaded on cloud server.

4.2 Distribution Of File

It will distribute clients data on distinctive servers with help of Rotated reed solomon technique [6]. which (m+k; k) R. Reed- Solomon erasure correcting codes [6] is used to create (k) redundancy parity vectors from (m) data vectors in such a way that , the original (m) data vectors can be reconstructed from any (m) out of the (m + k) data and parity vectors. By placing each of the (m + k) vectors on a different server, the original data file can survive the failure of any (k) of the (m+k) servers without any data loss. For support of efficient sequential I/O to the original file, this file layout is systematic, i.e., the unmodified (m) data file vectors together with (k) parity vectors is distributed across (m + k) different servers.

4.3 Public Verifiability With Privacy

As, clients are putting away their imperative information on cloud, they are constantly in stress whether there information is in place or not. Consequently information honesty checking gets to be challenging issue. As frequently cloud administration suppliers may carry on unhonestly and can erase clients information or they neglect to roll out improvements on the information which upgraded by the clients every now and again. So to defeat these difficulties the Trusted Third Party Auditor assumes the basic part in the interest of clients. As they guarantee to clients that the information facilitated on the server is secure. While checking trustworthiness of clients information on cloud, outsider auditor should not realize any learning about the data put away on the cloud server. Henceforth security ought to be kept up while publically examining the information.

4.4 File Retrieval

When user wants to retrieve the file from cloud server, user select the file and click on download button. Once file is downloaded, user will select the private key and by using this private key, file will be encrypted and user can view his original file.

5. EXPERIMENTAL RESULT

Below are the actual results of File selection, File Encryption, File Distribution and verification of file.

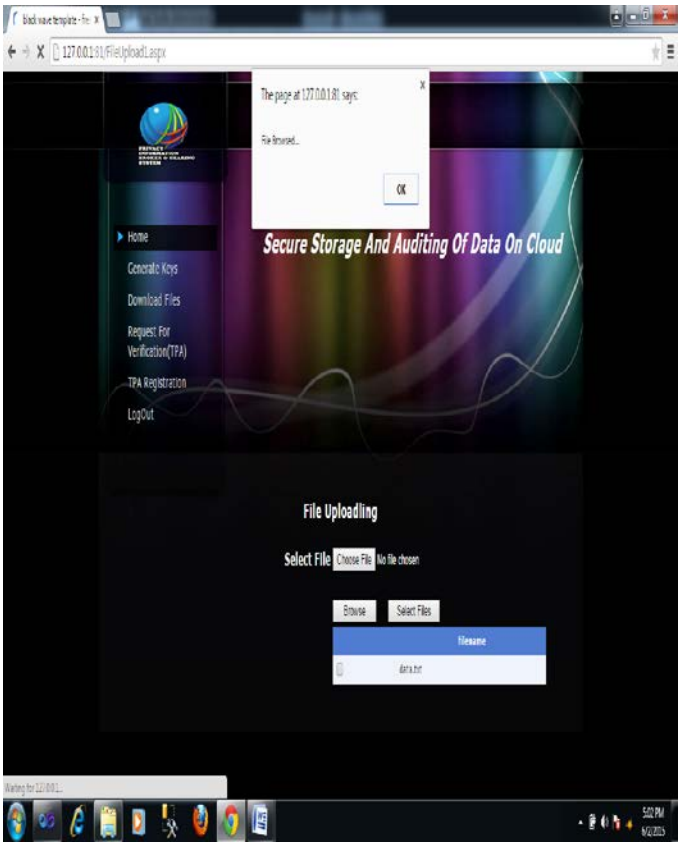

Fig 2: File Selection

Fig 3: File Encryption

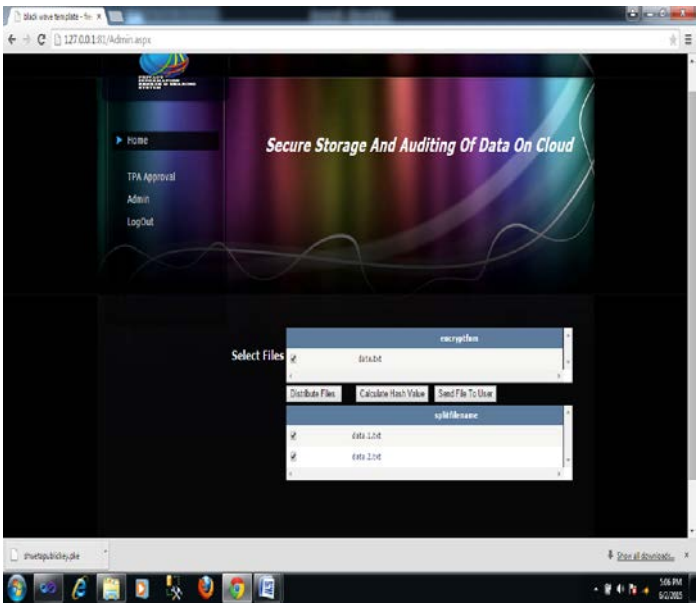

Fig 4:File Distribution

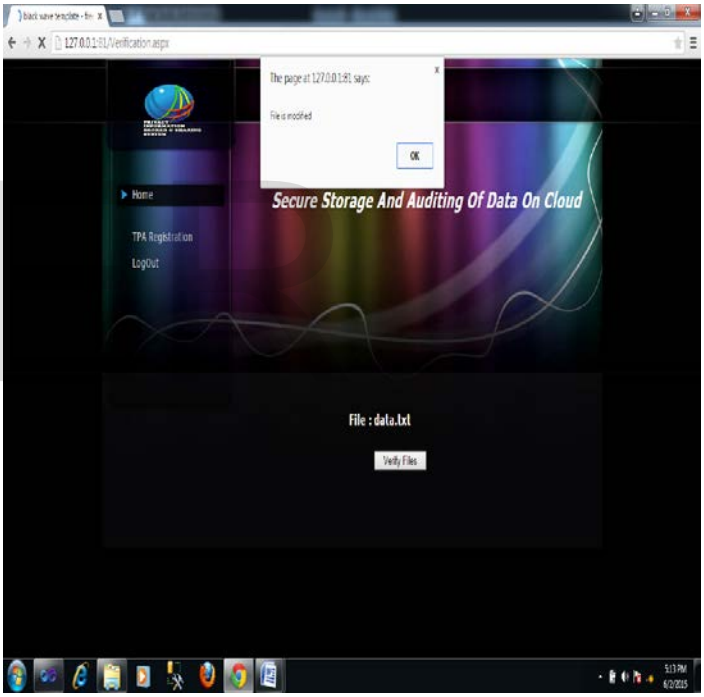

Fig 4: File Verification by TPA

6. CONCLUSION AND FUTURE WORK

Cloud computing is a web based registering which empowers offering of administrations and numerous clients put their information in the cloud. Be that as it may, clients are constantly in stress whether their information is secure or not. Along these lines, information honesty is challenging issue. To beat this, at first clients were downloading the complete information for examining which is really not practical as far as transmission cost and correspondence overhead. Henceforth we public auditing where one dedicated party audit the data from cloud on behalf of users request. while auditing the data one critical perspective is that our system is keeping up protection such that TPA

would not learn clients information. By utilizing Reed Solomon strategy, clients file will be distributed among distinctive server to accomplish information recovery to recover the lost information. Additionally it relinquishes additional load on one server. Also, our system supports data dynamics where user can perform modify, delete and insert operation on data which is stored on cloud. In future, data dynamics will demonstrate what alteration is carried out in the customer document by server to the customer and both present and past variants of the information record and relating metadata will be reviewed on interest.

7. ACKNOWLEDGMENTS

We take this opportunity to thank Prof. Ram Joshi for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this paper. We are also thankful to all the staff members of the Department of Computer Engineering for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, 2013 Privacy-Preserving Public Auditing for Storage Security in Cloud Computing.

[2] K.D. Bowers, A. Juels, and A.Oprea,, 2009 Proofs of Retrievability:Theory and Implementation", Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ,Mar 2010 Enabling PublicAuditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Trans. Parallel and Distributed Systems

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song,, 2007 Provable Data Possession at Untrusted Stores", Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609.

[5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, 2009 Dynamic Provable Data Possession", Proc. ACM Conf. Computer and Comm. Security (CCS '09),

[6] Osama Khan, Randal Burns,James Plank, William Pierce,Cheng Huang Rethinking Erasure Codes for Cloud File Systems:Minimizing I/O for Recovery and Degraded Reads

[7] A.L.Ferrara, M.Green, S. Hohenberger, and M. Pedersen, 2009 Practical Short Signature Batch Verification Proc. Cryptographers Track at the RSA Conf. 2009 on Topics in Cryptology (CT-RSA), pp. 309-324

[8] Z Hao, S Zhong, and N Yu, 2011 A privacy-preserving remote data integrity checking protocol with datadynamics and public verifiability, IEEE Transactions on Knowledge and DataEngineering, vol. 99

[9] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik,,2088 Scalable and Efficient Provable Data Possession", Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10

[10]] C. Wang, K. Ren, W. Lou, and J. Li, July/Aug 2010 Towards Publicly Auditable Secure Cloud Data Storage Services, IEEE Trans. Service Computing, vol. 5, no. 2, 220-232