International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Preserving Privacy and Integrity of Shared Data Stored on Cloud via Tpa.

Yogesh Lubal [1], V. S. Gaikwad[2]

[1]Computer Engineering Department RSSOER, JSPMNTC Savitribai Phule Pune University, Pune, India

[2]Assistant Professor, Computer Engineering Department RSSOER, JSPMNTC Savitribai Phule Pune University, Pune, India

Abstract: ***The Cloud computing is a latest technology which offers number of facilities via internet. The Cloud server allows user to store their information remotely on a cloud storage and allows to enjoy on-demand services and application from the configurable resources without worrying about accuracy & integrity of data. And also provide the access to data from any location at any time. In cloud computing, data owner host their data on cloud servers and users access that data from cloud server. Due to outsourcing of data on cloud number of security challenges occurs. The auditing protocol is required to check the data integrity on the cloud. Cloud also provides efficient solution for sharing resources among the group. In a group, every member is able to host their data and access data stored by another group member. Owner of data is able to add new users in the group. Identity of user preserved from third party auditor. There are many internal and external threats, which affect on cloud data storage. Every time it is not possible for a user to download all data and verify integrity, so in this paper we proposed system named Privacy Preserving And Verification Of Integrity Threat By Tpa Of Shared Data In Cloud.***

Keywords: Cloud Data Storage, Public Auditability, Data Auditing, Dynamic Data, Batch Auditing

1. Introduction

The constructing cloud and storing data on it has a incredible benefits. It ease the authenticated and authorized cloud users to access large resources that are outsourced and shared on the cloud. Whenever requisite the user can request and gain the access (only, if the users' credentials are validated [4]) to the resources in an easy way and at low cost, irrespective of the user location. Also, cloud computing takes away the expenses that are spent on installing all hardware and software at local site. Cloud computing paradigm allows users to rent out the resources based on their needs and pay them as per their usage. Despite of all these benefits, cloud computing still a undergoes broad range of challenges which forbid the successful implementation of the cloud. These include both the traditional as well as cloud security challenges. Specific to cloud computing, the issues are many, of which some are: identity management of cloud users, multi-tenancy support, securing the security of applications, preserving privacy of the users, attaining control over the life cycle of outsourced data, etc. Among which, the issues related to privacy preserving are alone looked in this paper.

Privacy preserving is used to provide an trusted service.ie sender does not reveal the key and the data that an trusted customer sends in response to an auditor that does not reveal the key. Security in cloud computing can be achieved in numerous ways such as authentication, integrity, confidentiality. Data reliability or data correctness is another security drawback that needs to be considered. Preserving the privacy of user, his identity and data in the cloud is very mandatory. With the rise in growth of cloud computing, the concerns about privacy preserving are also getting increased [3]. Several methods have been put forward to tackle this issue of privacy preserving. There are two very easy ways in which the user can ensure the data privacy and integrity, first is the user can download all the outsourced data and verify the integrity of the data.This solution is unrealistic as the I/O operations over network are expensive. Second way is that user can check the storage correctness of the data whenever that data is accessed but this solution does not give the assurity of data integrity of the data which is not accessed or is hardly ever accessed [3]. The confidentiality issue of outsourced data can be handled by using cryptographic technique but it is also very difficult to validate the integrity of the data without having the local copy of the data [9].As discussed above downloading the whole data for verifying its integrity is not an efficient way. So in this scenario, the alternative is using a third party auditor for auditing stored data in cloud computing. A third party auditor (TPA) that has expertise skills and capabilities and can more efficiently work and convince both cloud service providers and owners [1].

A. Challenges in the cloud data storage security are:

1) Snooping

Snooping is to steal a look into others private data. The efficient way to send and retrieve the data over a secure communication line.

2) Cloud Authentication

The clients can acquire's others authorization and may try to delete the data. So it is necessary to guard one's unique authorization. The unauthorized clients must not be loged in to others account and delete the data.

3) Key Management

The cryptographic keys has to be managed in the cloud environment but this key management must be user friendly.

4) Data Leakage

Data leakage takes place when data is transmitted between the user and the cloud server. The best way to protect is to encrypt the data from owner's side.

5) Performance

An resilient security approach is necessary for encrypting as well as decrypting the data to and from the cloud but it should keep the user's performance integral.

B. Major goals of proposed schemes are.

1) The User needs to use best encryption method.
2) Secure key management.
3) Supple access right management.
4) Light weight integrity verification process for verifying the unauthorized change in the original data without need of local copy data.

2. System Architecture

The proposed scheme uses symmetric encryption which provides confidentiality, integrity, verification with low cost. It also provides enquiry for data owner and access control through which only authorized user can access the data. CSP may hide data loss or damage from users to maintain a reputation. To achieve security, we can handover our data to a third outsource party who will be assigned a task of identify the correctness and integrity of the cloud data. Hence Third party auditor (TPA) will check the data stored on the cloud based on the user's request.

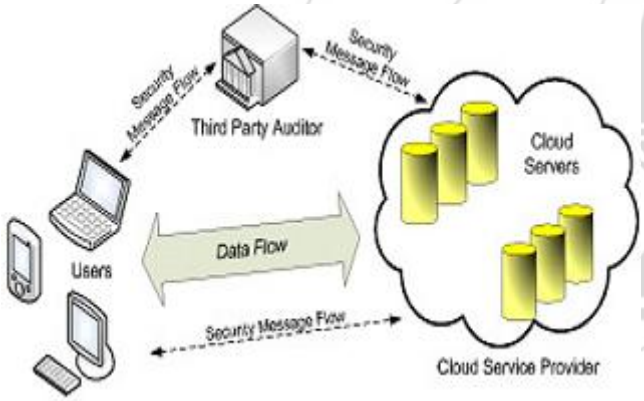

Figure 1: The framework of cloud data storage [1].

Fig.1.show the architecture of cloud storage where the cloud user (U), who has huge amount of data files to be stored on the cloud; the cloud server (CS), which is handled by cloud service provider (CSP) to provide data storage service and has considerable storage space and computation resources the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is authorized to assess the cloud storage service security on behalf of the user upon request.

We cannot achieve privacy; TPA can see the actual content stored on a cloud during the verifying phase. TPA itself may distribute the information stored in the cloud which violate security concept. To avoid the violation of security, Encryption technique is used where data is encrypted before storing it on the cloud. Hence using auditing with zero knowledge privacy technique where TPA will audit users data without seeing the contents. It uses existing public key based homomorphic linear authentication (HLA) [5] that allows TPA to perform auditing without requesting for user data. It reduces communication and computation overhead.

3. Literature Survey

a) MAC Based Solution

It is used to verify the data. In this, user uploads the data blocks along with their MAC to CS and provides its secret key SK to TPA. Afterward the TPA will randomly retrieve data blocks & Mac uses secret key to check correctness of stored data on the cloud. Various issues with this system are listed below as

1) It introduce an additional online burden to users due to limited use (i.e. Bounded usage) and stateful verification.
2) Communication & computation complexity
3) TPA requires familiarity of data blocks for verification
4) Restriction on data files to be audited as secret keys sk are limited
5) After usages of all possible secret keys, the user has to download all the data again and recomputed MACfor each data block & republish it on CS.
6) TPA should preserve & update states for TPA which is very difficult
7) It does not work with dynamic data ie it works only for static data

b) HLA Based Solution

It supports efficient public auditing without retrieve data block. It is aggregated and required stable bandwidth. It is possible to calculate an aggregate HLA which authenticates a linear combination of the individual data blocks.

c) Provable Data Possession

G. Ateniese et al., used a provable data possession with homomorphic verifiable tags [6]. It allows the verification of data without retrieving it from the original source. The model generates probabilistic proofs of possession by sampling random set of blocks of data from the server, which reduce the cost. The homomorphic verifiable tags computes multiple file blocks which can be combined to form a single file. The client pre-computes the tags and the tags are stored in the Third Party Auditor for verification. The modified file is stored in the server storage. The verification process is done in the requested style generated by the client.

It performs well and supports blockless verification. Its client/server computation is in O (1). Verification and communication takes time. It does not consider the privacy protection of the user's data against the external auditors

d) Dynamic Provable Data Possession

C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, Dynamic Provable Data Possession (DPDP) [7]. PDP is mostly applicable for static files. The DPDP is an updated version of the PDP where it supports the updates while storing the data. It can append, modify, or delete the existing blocks of files. This scheme uses rank information to organize the dictionary entities. It supports the verification of files for different users and does not need to download the whole file for verification. It also explains the security and blockless verification of DPDP. Its hashing schemes use ranks based RSA trees. The experimental results show that the block size minimizes the communication and computational overhead.

e) Proof-of-Retrievability System
In this paper A.Juels et al., defined the PORs [8] as using an archive or a backup to help the verifier retrieve the file in the target easily. The user can easily retrieve the file from the backup. The POR is viewed as a kind of cryptographic proof of knowledge (POK), which can support large files. POR protocol reduces the communication cost because it doesn't need to access the file from the server, it can easily be accessed from the archive. This PORs is an unusual security formulation.

The main goal of PORs is that they are used to check the file without downloading the files. It also provides quality of service. Here the pre-processing takes time i.e., encoding the file F is required before storing to the prover. At the time of encoding sentinels are randomly added in specific positions, to constitute the contents of a POR. These sentinels can also retrieved by using the PIR, and it can be reused. It does not consider the privacy of the data against the external auditors. It has computational overhead.

f) Compact Proofs of Retrievability System
Shacham and B. Waters [9], in a proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure — that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, we give the first proof-of-retrievability communication takes time. It does not consider the privacy protection of the user's data against the external auditors

4. Objectives of the Propose Work

There are following objectives & motivations of the proposed work

1) Public verification for storage correctness assurance
To There are following objectives & motivations of the proposed work allow anyone to perform auditing, not only for the clients that have originally stored the file on cloud servers. Public auditing capability allowed on demand for verification of the correctness of stored in cloud.

2) Dynamic data operation support
Clients can perform dynamic block level operations on the data files such as insert, delete, update, while maintaining correctness of data files in the cloud .The design of system should be as effective as possible for assure the consistent integration of public verifiability and dynamic data operation support.

3) Blockless verification
The challenged file blocks for data verification should not be retrieved by the verifier (e.g., TPA) during verification process for both efficiency and security concerns.

4) Stateless verification
Verifier should not maintain the state information during the auditing process. Stateless verification can remove the need for state information maintenance at the verifier side between audits throughout the long term of data storage.

5) Batch Auditing
Auditing can be carry out for the batch of users i.e Multi-User auditing can be supported by TPA in cloud environment.

5. Methodology of Proposed System

The public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, and VerifyProof). KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification metadata, which may consist of digital signatures. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof. Running a public auditing system consists of two phases, Setup and Audit:

1) **Setup Phase** The user initializes the public and secret parameters of the system by executing KeyGen, and preprocesses the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server. The user may alter the data file F by performing updates on the stored data in cloud.
2) **Audit Phase** The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will create a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response by cloud server via VerifyProof.

6. Screen Shots

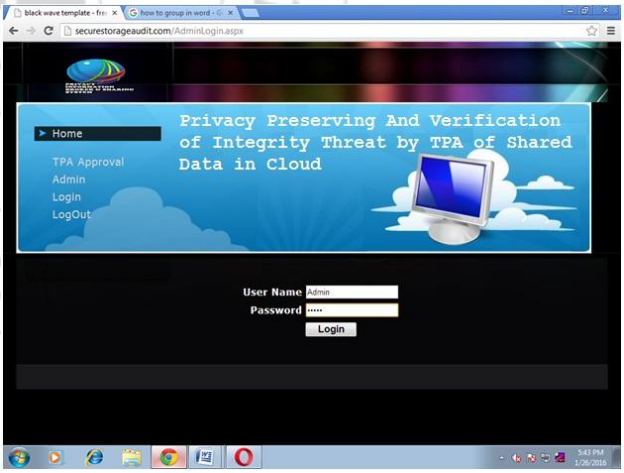

Figure: User Login Form

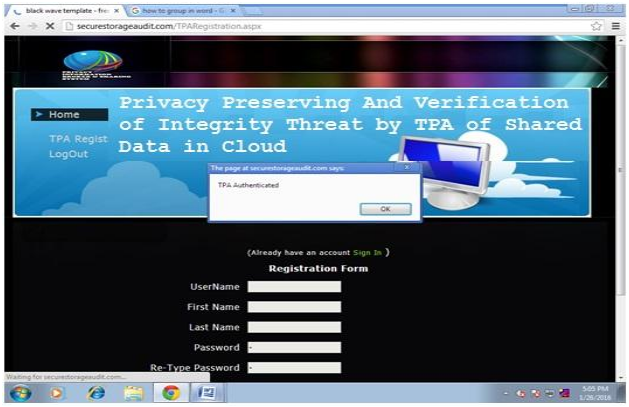

Figure: User registration form

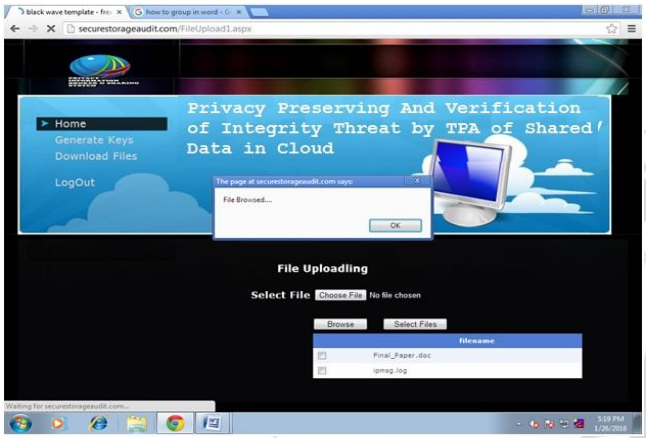

Figure: File Uploading Form

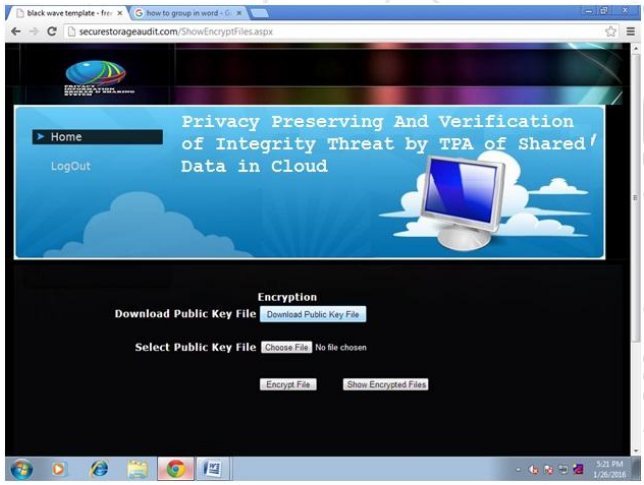

Figure: File Encryption Form.

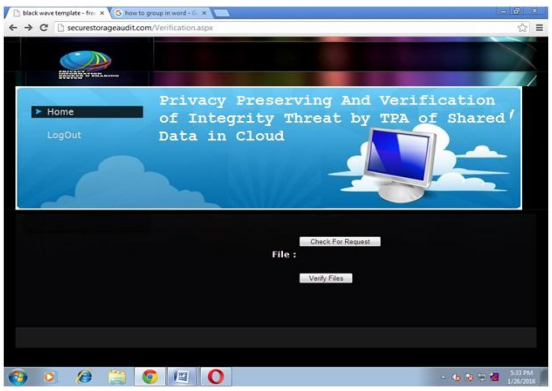

Figure: Integrity Verification Form

7. Experimental Result

We recognize that user s privacy always remains integral despite of various attacks launched by number of malicious users. For-eg if an professional hacker is able to attack the data during the transmission (downloading, uploading) or at the storage location it doesn t affects the privacy of data since before departure of data from the client slide it gets encrypted and remains same throughout the entire process even when it is stored or processed at cloud storage. When intruder get entry, they are not able to alter or get any meaningful data just rather than the cipher text and if an attacker violates the integrity at physical cloud storage, it is instantly identified during the auditing phase and data is recovered back to its previous state from the backup storage. Likewise when, TPA admin wants to extract the private key of client, attacker might not be able to decrypt it as it is encrypted. Though if attacker gets the private key, attacker might not be able to decrypt the client s data, since for decryption, system should perform the decrypt process and this job can only be initialized by the client after successfully login with required testimonial. The above said encryption and decryption algorithm are compared for different file size with algorithm such as DES and RSA as shown in graph-2&3.Performance of those algorithm is analyzed by considering the Time taken by these algorithm for both encryption and decryption and it is seen that time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm. The above said hashing algorithms is compared on the basis of time parameter with MD 5 and SHA-512 hashing algorithm. In this paper we are comparing three algorithms like SHA-1, MD 5 AND SHA-512. The SHA-1 is giving the better result.

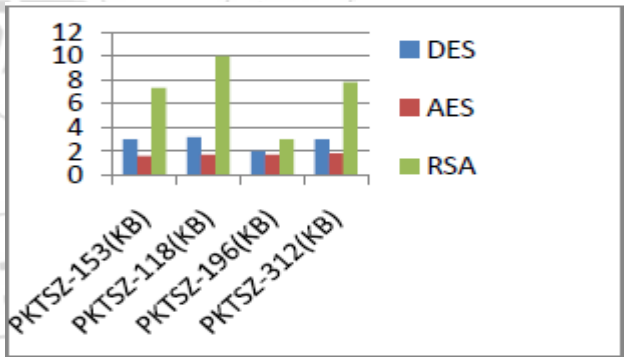

Figure 1: Comparative Analysis of Encryption Time among DES, AES and

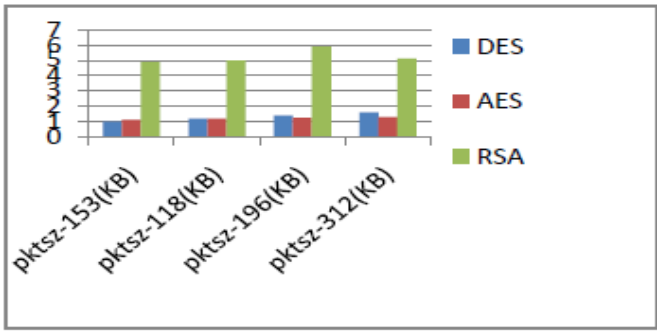

Figure 2: Comparative Analysis of Decryption Time among DES, AES and RSA

8. Acknowledgment

We express our sincere thanks to all the authors, whose papers in the area of cloud computing security and auditability aspect which are published in various conference proceedings and journals.

9. Conclusion

A system of privacy preserving public auditing not only provides security for stored on data cloud storage but also checks the accuracy of data. The cloud storage is advantageous than former traditional storage system. Our system uses AES encryption algorithm for encrypting of data prior storing it on cloud storage. In order to authenticate storage correctness we need to check integrity of data. Hence we are using SHA-1 algorithm for checking integrity of data stored. Therefore data will be secured on cloud storage. The cloud user can verify integrity of their data stored on cloud server using TPA.TPA will quickly notify the client regarding status of the client data and hence security and data integrity is properly achieved.TPA might not learn any knowledge regarding the data content while auditing the data i.e. Zero Knowledge Public Auditing which not only reduces the burden of cloud user from the complex and possibly expensive auditing task but also eliminates the users worry regarding their outsourced data leakage. Cloud data security is an essential aspect for the cloud user while using various cloud services.TPA is used to ensure security and integrity of data stored on cloud. As user is encrypting data prior to storing it on cloud server, to protect the data from any illegal user. The job of allowing a third party auditor,on behalf of the cloud user to validate integrity and privacy of the data will free up the user from the job of auditing task so resulted method is secure and has less communication overhead.

References

[1] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, ―Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.
[2] C. Wang, Q. Wang, K. Ren, and W. Lou, ―Privacy-Preserving Public auditing for storage security in cloud computing," in Proc.of IEEE INFOCOM'10, March 2010.
[3] Xiao Z, and Xiao Y. Security and Privacy in Cloud 14. Computing, IEEE Communications Surveys & Tutorials, vol PP(99), 1–17.
[4] Takabi H (2010). Security and Privacy Challenges in Cloud 13. Computing Environments, IEEE Security & Privacy, vol 8(6), 24–31.
[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik ―Scalable and efficient provable data possession," in Proc. Of SecureComm'08, 2008,
[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), 2007.
[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, ―Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), 2009.
[8] A. Juels and J. Burton, S. Kaliski, ―POR: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), Oct. 2007.
[9] H. Shacham and B. Waters, ―Compact Proofs of Retrievability," Theory and Application of Cryptology and Information Security: Advances in Cryptology Dec. 2008.
[10] C. Wang, K. Ren, W. Lou, and J. Li, ―Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[11] Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li ―Enabling Public Audatability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 – 859,2011.