RESEARCHERID
THOMSON REUTERS

[ICRTCET-2018]

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ENSURING PRIVACY OF OUTSOURCED DATA IN CLOUD STORAGE

Dr.T.Subha[*1] & Dr.S.Jayashri[2]
[*1]Associate Professor, Sri Sai Ram Engineering College, Chennai,
[2]Director-Research, Adhiparasakthi Engineering College, Melmaruvathur

ABSTRACT

The latest growing technology that can offer different services like storage, infrastructure, network and computing resources is termed as cloud computing. These services are can be offered via internet to the customers. This will pave a way for the client, individual users or the industries can store the data, applications to cloud vendor. Cloud server (CSP) takes the entire responsible for providing the service continuously and the customers need to pay for what they use. Users are fully relieved from the load of keeping the storage and data in house. It reduces their maintenance and capital cost. It brings out new challenging threats towards the integrity and privacy of data while the data is maintained in third party data center. The location of where the data gets stored is not known to the users and also they do not have control on their data. The auditor who is authorized and trusted can carry out the audit to ensure the data correctness on behalf of the client. This is known as public auditability. The data is not only in cloud storage and needs to be accessed or shared by many users. Users can update the shared data at any time and that is signed by the user belonging to that group. User's identity information should not be disclosed to auditor during auditing. Even though the auditor is trusted, he is curious and would like to learn the details about the shared data. We try to propose an algorithm for checking the shared data integrity and privacy in this paper. This algorithm utilizes ring signature algorithm with homomorphic authenticators to generate signatures on each block. This signature is further used as the verification Meta data by the auditor during integrity verification. The auditor (TTPA) selects random set of blocks specifying the block positions to be checked and send this as a query to the cloud storage server (CSS). CSS computes signatures for the blocks requested or challenged by the auditor. Then, auditor verifies the authenticity of signature and executes the algorithm to validate the proof. If the output passes, the data is intact and is stored correctly in cloud. Otherwise the integrity of data is not maintained by the CSS. The proposed scheme detects the misbehaving server with the probability of more than 95 percent.

Keywords: *Auditor, Cloud, CSS, Data, Integrity, Privacy, Security, Storage Server, TTPA.*

I. INTRODUCTION

National Institute of Standards and Technology [1, 8] defines cloud computing as, cloud is the ever present model that can provide access to networks based on demand and it is the convenient way for configuring the following resources (ex. networks, servers, applications, storage and services) which provides the flexibility to provision and release it quickly with minimal effort from service provider [1]. Cloud offers three types of deployment model. They are categorized into Private cloud, Hybrid cloud and Public cloud. The integration of public and private cloud combines the features of both clouds. Public cloud is accessible by anyone and user can utilize the services offered by that particular cloud [2]. Private cloud is the one which has been developed and maintained by the particular organization or industry. Authorized persons within that organization are allowed to use the cloud. Hybrid is the combination of these two clouds and offers additional benefits [2].

One of the major important service in cloud computing is cloud storage. It helps clients to relocate data from local storage systems to third party. Storage service offered by cloud is one of the major resources in maintaining clinical diagnosis data, banking details etc [18]. The datas and storage can be managed easily and it is cost efficient also. Drop box and Google docs are the storage examples [3].

The major concern in cloud storage is to provide security to the customer data and verifying integrity of data even if it provides major benefits to the customers [1-2]. It may lead to erroneous results in case of lack of

security. The data stored in cloud could be deleted easily because of software and hardware failures through malicious applications [4, 5]. Sometimes an adversary or active attackers

resides between service provider and auditor alters the data content without being noticed by third party [6]. These types of data errors are hidden from clients by the provider to maintain their reputation [7]. Hence it is highly essential to prove the data integrity and the accuracy of outsourced data in cloud.

There are different algorithms presented to verify integrity of stored data [1-8]. The communication overhead increases when the whole document/file is downloaded for the sake of verification. The mechanism of public auditing is a cryptographic method that checks the stored data integrity remotely. The advantage of a public auditing mechanism is the stored data integrity can be checked without the need to download the whole data during verification [3]. The overhead on computation and communication is decreased and the process of integrity checking becomes easier [7]. Therefore, public auditing can provide an efficient solution for verifying the data integrity.

II. RELATED WORK

There had been many methods designed to prove the correctness of data in cloud storage [8-18]. Provable data possession [8] named as PDP and Proofs of retrievability named as PoR were the basic schemes designed to achieve data integrity in remote data centre. They were the one who had introduced public auditing scheme. Their scheme was implemented using homomorphic linear authenticators. RSA algorithms were used in this method. Ateniese et al [10] extended their scalable data possession scheme to dynamic version to support block level operations. They had achieved partial implementation of dynamic data operations except block level insertion. One of the limitation of their system is it supports limited number of challenges and responses.

In continuation with this the further development of dynamic version of public auditing was introduced by Erway [11] & Juels [9]. Their scheme also suffered from updation operation. Pseudo random based compacts proof of retrievability was proposed by Shacham and Waters [12] that utilize BLS based signature scheme to support public auditing. Public auditing method has been introduced for the verification of data by introducing trusted third party auditor (TTPA) in [13] by subha et al. Merkle hash tree (authentication structure) has been utilized to store the data values in leaf nodes.

Wang et al [14 – 15] introduced a scheme on preserving the privacy of users from the trusted auditors, to carry out auditing for updating blocks, deleting blocks and inserting blocks. In all the above mentioned schemes the data correctness is being achieved by third party auditor based on the request received from server.

B.Wang et. al [15] introduced a new method to resolve shared data privacy issue in cloud. They utilized ring structures, homomorphic authenticators technique and the signer identity of each block is kept secret. Their scheme supports batch auditing also. In [18] the author proposed certificateless public auditing method in wireless sensor networks for verifying the clinical data. It is essential to keep the identity and secret information of users from being accessed by public verifiers. Eventhough we assume TTPA is a trusted one, the auditor is curious enough to learn the data contents of user. It is necessary to protect the user privacy from verifiers [14 – 16].

Adversaries will try to listen to the interactive messages between the server and the auditor. Adversary may alter the proof that is being generated from server without the server noticing the malpractice. Auditor also is not able to identify the attacks properly. The protocol emits PASS during verification algorithm implies that the data is well maintained in cloud.

But the data have been corrupted actually [17]. Adversaries only need to understand how the data is altered. We utilize public auditing methodology in our system and a solution is suggested to preserve the user identity in

ISSN 2348 – 8034
Impact Factor- 5.070

shared data. The original scheme supports confidentiality, integrity of data and data availability. Finally the cloud server digitally signs the proof using digital signature algorithm during the auditing process.

III. PROBLEM STATEMENT

It is almost necessary to share the data among several users and this is one of the promising features that prompt the usage of storage server in cloud which is remotely maintained. It is very much necessary to check the shared data integrity out stored in to cloud is correct or not. The major problem that exists in existing mechanism lies in the leakage of private information (ex. identity) to the public verifiers [19].

The two users User A and User B are working together and file is shared between two users. Sharing of public data is shown in Fig.1. The file is divided in to blocks and individual blocks are signed by any one of the users. The user will sign a block newly using his private key, if the data in a particular block is modified. Different user's signs individual blocks involved in the group based on the modifications introduced by them. To check the entire data correctness, the verifier wants to access the public key of a particular block (ie, User A's Public key can be used to check the block signed by User A). Verifier can easily learn the identities of users based on the relationship between identity and the public key of a signer from the above concept.

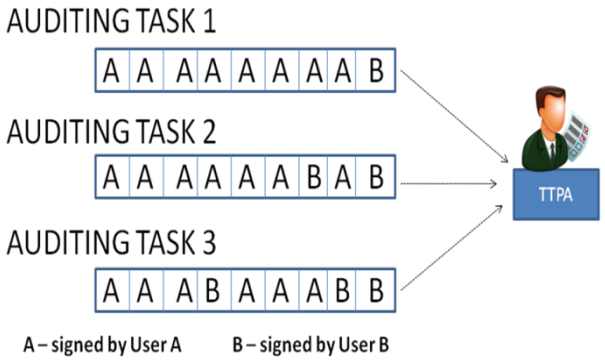

Fig.1 Public Auditing on Shared Data

This leads to disclosure of confidential information on shared data. Examples like

1. Which block is frequently accessed (this block may be the important target) and
2. which user is frequently updating the block (the role (or) importance of particular user)

From the above diagram we conclude that, User A has an important role than others and seventh block may have a higher value. It's because the block is more frequently updated by users. Hence, it becomes necessary to protect the confidential information and verifier's identity privacy during public auditing [19].

We recommend a new public auditing scheme to prove the shared data correctness on cloud. We introduce TTPA who can act as a public verifier, and he checks integrity of data in cloud. We use ring structures and homomorphic authenticators to generate signatures as verification meta data. Therefore, TTPA can able to prove the shared data integrity. It does not require downloading the entire file. The signer identity is also kept secret from the verifier.

3.1 Basic Terminologies

We describe the preliminaries and the basic algorithms used in our proposed system.

3.1.1 Bilinear maps

Our system uses BLS scheme as the basis to generate signature for verification [17].

3.2 System model

The major entities involved in the integrity verification process are named as Users (they work as a group), Server (CSP), and trusted third party auditor (TTPA). User's files are outsourced in to third party storage. There is some group of users in the cloud. A file is created by original user and shares it to others in a group. Data can be shared and accessed by each member in a group. Shared data with Meta data is used for verification and it is stored in the remote server. We assume the auditor in a system is a trusted person. Cloud storage is been offered as a service to the users by cloud provider. The architecture model of our scheme is represented in Fig.2.

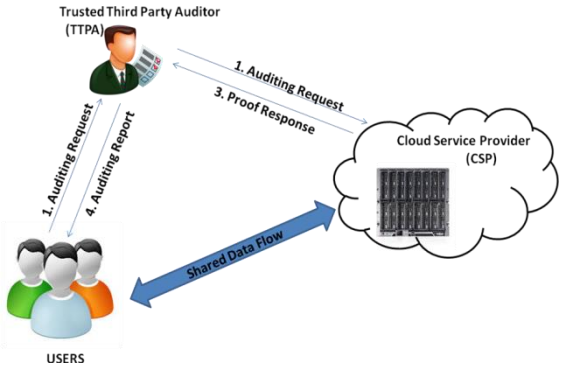

Fig.2 System Model

In case of integrity verification, after receiving the user request auditor initiates the process. The auditor sends the challenged blocks contains the index as a request to the prover by specifying the index and position of blocks for which the proof needs to be generated. Service provider in turn gives the result to the TTPA as a proof.

The result contains the signatures of the challenged blocks sent by TTPA. Then TTPA verifies whether the proof and produces the result of integrity verification by running the verification algorithm. It outputs TRUE if the integrity is maintained in verification step, otherwise it outputs FALSE. As the next step, auditor sends back the report to the user. Our verification scheme utilizes hybrid cloud is explained in [13].

Our earlier version of the paper describes the method of how the auditing process had been carried out using TTPA. The previous scheme did not focus on sharing of data in cloud. Our proposed scheme utilizes ring signature with homomorphic authenticators. The scheme is discussed in detail as below.

3.2.1 Ring Structure Algorithm

Ring structure algorithm is a kind of digital signature algorithm in which any member in a group can sign if they have keys. So, the signed message is validated by some group users.

The property of ring signature states that it is difficult to determine the signer and its identity [4, 5, 14-16]. Therefore, the signer's identity is kept secret and thus privacy is preserved.

3.2.2 Homomorphic Authenticators

In cloud storage, the entire data downloading is not possible just for the sake of integrity verification. It may incur high communication cost incase if the entire file is downloaded. So a sampling technique is introduced in which a random set of blocks are chosen for challenge. Random blocks from the entire file blocks are sent as challenge request to the cloud server [8 – 16]. Homomorphic authenticatable signature scheme is one type of tool that supports blockless verifiability. It combines the signature of random blocks in to a single one. So that the files are not needed to be downloaded.

ISSN 2348 – 8034
Impact Factor- 5.070

3.3 Steps in Ring signature-Homomorphic Authenticator Signature Scheme (RSHASS):

Our scheme combines Ring signature scheme with homomorphic authenticable signature method. This scheme includes three algorithms called

1. Key Generation algorithm
2. Ring Signature Algorithm and
3. Ring Verification Algorithm.

3.3.1 Key Generation algorithm

A particular user Ua in a group selects a private key as x_a. From this, public key of a user is calculated as follows.

PK = {Wa = g_2^{xa}} and SK= x_a ---------- (1)

3.3.2 Ring Signature Algorithm

There are n members in a group. The users' public keys in a group is denoted as

(PK_1, PK_2,…, PK_n = W_1, W_2,… W_n) ---------- (2)

Given a block m, identifier of a user ID, and user U_s choose random value a_i , i∈ [1, n] members of the group. Then the signature is calculated as,

$\Omega i = g_1^{a_i}$ ---------- (3)

$\Re = H_1(ID) g_1^{m}$ ---------- (4)

$$\Omega s = \left(\frac{\Re}{\prod w_i a_i} \right) 1/X_s \quad \text{----------(5)}$$

Finally, the ring signature of block m is given as

Ω = (Ω$_1$, …… , Ω$_n$)

3.3.3 Ring Verification Algorithm

Given a group of n users public keys **(PK_1, PK_2,……, PK_n = W_1, W_2,…… W_n),** block m, block ring signature for m is **Ω = (Ω$_1$, …… , Ω$_n$),** the TTPA computes **ℜ** value and checks whether one of the n users in the group signs the block by checking the equation no 6.

e(ℜ , g2) =? $\prod_{i=1}^{d}$ e(Ω$_i$, W$_i$) ---------- **(6)**

Otherwise it is not signed by the users in the group.

3.4 Public auditability of data based on RSHASS scheme

Our auditing scheme on the client side consists of three important phases. They are divided in to initialization, key Generation and followed by tag Generation phase:

3.4.1 Initialization phase:

In this phase the file to be sent to cloud is preprocessed first as a first step. Then the signatures generated are added to the result based on the corresponding file blocks. The original file, tag contains the file name to identify a particular file and set of signatures calculated for each block are moved to the cloud server. After this the file is deleted from local storage. The Meta data that needs to verify integrity is also shared with the auditor (TTPA) that can be used to perform the integrity checking.

Step1: The original file can be divided into n small blocks.

3.4.2 Key Generation phase:

Step2: The key pairs used to sign (Private key - sk and Public key - pk) are generated by the users in a group. The confidentiality can be given by encrypting the data using a secret key (sk) before outsourcing it into data centre. This feature helps us to provide confidentiality. User U_i chooses a random element x and calculates public key (PK) as $\mathbf{W_i = g_2^{xi}}$ **and SK=** x_i. The user also chooses random elements ($r_1, r_2, \ldots . r_k$) and denotes this as aggregate key.

3.4.3 Signature Generation (or) tag generation phase

Step3: Tag is attached for each file in order to find a file. File tag is used to represent the name of the file. Given a group of n users public keys
(PK1,PK2,……, PKn = W1, W2,…… Wn), block mi where i ϵ [1..n], user identifier IDi, Private key SKu for some u. user Uu calculates ring signature as follows.

Aggregated signatures for the block m_i is given as,

$$R = H_1(ID_i)^{r_k m_j} \quad \text{----------} \quad \mathbf{(7)}$$

$$\Omega s = \left(\frac{\Re}{\prod_{i \neq u} w_i a_j} \right) 1 / X_s \quad \text{----------(8)}$$

The ring signature for the block m_i is given by $\mathbf{\Omega\ i = (\Omega_1, \ldots\ldots\ldots\ldots , \Omega_n)}$

3.5 Data verification process:

The auditing process is carried out by third party auditor (TTPA) for checking the data integrity in cloud storage. Challenge request as a message is generated by the auditor to the cloud server by giving the parameters for which proof needs to be generated. Then it proves the integrity by verifying the proof using the corresponding algorithm. The two important phases of the scheme is given below.

3.5.1 Auditing Challenge request phase:

Step1: In this phase, auditor selects randomly selected blocks as the challenge request. It is sent as a challenge query to the CSP. Auditor specifies the position with index for verification by server. It chooses the c element (the number of challenged blocks) from S = {S1 ≤ ….≤ Sc} of set [1, n] randomly. Auditor selects a random value y_j.. and the challenge message is sent from TTPA to the server.

Challenge msg= {(S,yj)} S1 ≤ i ≤ Sc --------- (9)

Step2: After receiving the challenge request from auditor, storage server takes a challenge query, input file F, and a signature set S. Proof has been generated by server and given back to the auditor for verification.

Server aggregates the signature as a single one and sends the data proof as follows.

$$\mathbf{\eta_l = \sum_{j \epsilon S}\ y_j\, m_j\, , l} \quad \text{----------} \quad \mathbf{(10)}$$

$$\mathbf{\sigma_i = \prod_{j \epsilon S} \Omega^{y}_{\ j\ ,i}} \quad \text{----------} \quad \mathbf{(11)}$$

3.5.2 Auditing Challenge Proof Phase:

Step3: After receiving the proof, auditor checks the integrity. The signature is computed newly and compared with stored signature to ensure the data is intact.

Step4: If both signatures match the output is TRUE, otherwise FAIL.

Step5: Finally the data owner receives the result from auditor.

ISSN 2348 – 8034
Impact Factor- 5.070

IV. RESULTS AND DISCUSSIONS

We carried out our experiment on Eucalyptus software. Eucalyptus faststart 3.4.1 has been used to setup a private cloud with 8 GB RAM. The results of our experiment are shown below.

Fig.3 depicts the computational cost incurred in our system. It is plotted between no of challenged blocks and the overhead by it. The overhead is linearly increasing with the increasing no of blocks. The performance of auditing time is shown in Fig.4. Auditing time is represented in seconds. When the group size increases, the auditing time also increases linearly.

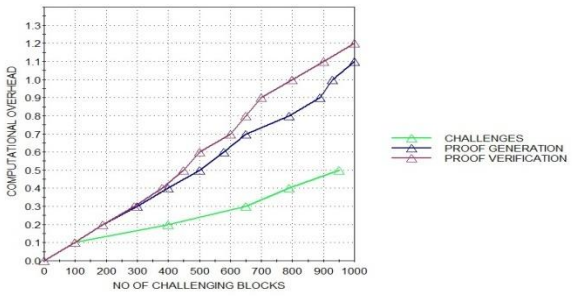

Fig .3 Computational Cost

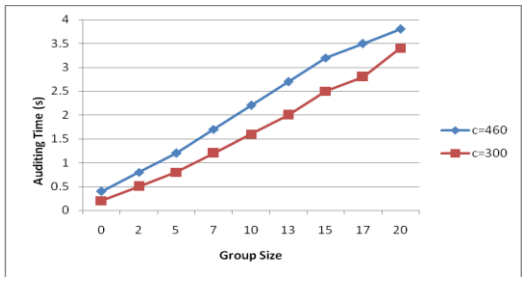

Fig. 4 Auditing Time Performance

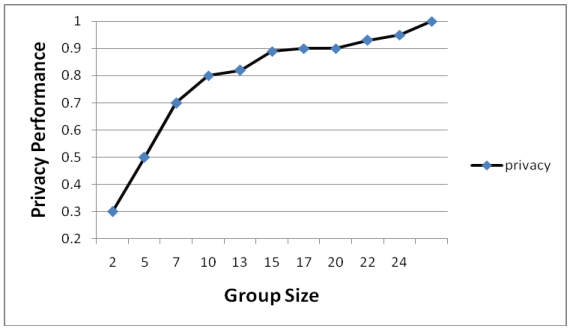

Fig.5 Impact of Privacy Performance

Fig.5 shows the privacy performance of our scheme. This scheme proposes a better efficiency even though the group size is larger.

V. CONCLUSION

Securing the privacy of a user's confidential data from adversaries has been discussed in this paper. Ring signature with homomorphic authenticator algorithm has been used to generate signatures. A secure channel is being established between TTPA and server for message communication. It helps us for securing data from external adversary. The user identity and the privacy content is not leaked to the TTPA while auditing with the help of ring signature. The scheme is capable to prove the data integrity by sending random set of blocks. This sampling is achieved through homomorphic authenticators. Our scheme supports public auditability of data stored in cloud.

REFERENCES

1. *P.Mell and T.Grance, "The NIST Definition of Cloud Computing", NIST Special Publication - 800145,2011; http://csrc.nist.gov/publication/nistpubs/800-145.*
2. *M.Lillibridge, S.Elnikety, A.Birrell, M.Burrows and M.Isard, "A Cooperative Internet Backup Scheme," proc. USENIX Ann.Technical Conf., pp.29-41, 2003.*
3. *Lee Cheng-Chi, Lai Yan-Ming, Hsiao Chin-Sung, Cryptanalysis of a simple key assignment for access control based on polynomial. J Inf Secur Appl 2013; 18(4):215-8.*
4. *Li H, Dai Y, Tian L, Yang H, " Identity-based authentication for cloud computing, Lecture Notes of Computer Science (LNCS), vol. 5931; 2009, p.157-166.*
5. *Yuan Zhang, Chunxiang Xu, Jining Zhao, Xiaojun Zhang, Junwei Wen, "Cryptanalysis of an Integrity checking scheme for cloud data sharing", Journal of Information Security and applications (2015), I-6.*
6. *Dolev Danny, Yao Andrew C, "On the security of public key protocols. Inf Theory, IEEE Trans Inf Theory March, 1983; 29(2):198-208.*
7. *G.Ateniese, R.Burns, R.Curtmola, J.Herring, L.Kissner, Z.Peterson, and D.Song, "Provable data possession at untrusted stores,"in Proc.of CCS'07. Newyork, NY, USA: ACM, 2007, pp.598-609.*
8. *A.Juels and B.S.Kaliski, Jr.,"Pors: proofs of retrievability for large files," in Proc.of CCS'07. Newyork, NY, USA: ACM, 2007, pp.584-597.*
9. *G.Ateniese, R.D.Pietro, L.V.Mancini, G.Tsudik, "Scalable and efficient provable Data possession," in: Proc. of SecureComm 2008, pp. 1-10.*
10. *C.C.Erway, A.Kupcu, C.Papamanthou, R.Tamassia, "Dynamic provable data possession," Proc. of CCS 2009, pp.213-222.*
11. *H.Shacham and B.Waters, "Compact proofs of retrievability," in Proc. of ASIACRYPT'08. Melbourne,Australia: Springer-Verlag, 2008, pp.90-107.*
12. *B.Wang, B.Li, H.Li, "Oruta: privacy preserving public auditing for shared data in the cloud," in: IEEE International Conference on Cloud Computing, 2012, pp.293-302.*
13. *B.Wang, B.Li, H.Li, "Knox: privacy preserving auditing for shared data with large groups in the cloud," in: Proc. of ACNS 2012, pp.507-525.*
14. *Jianbing Ni, Yong Yu, Yi Mu, Qi Xia, "on the security of an efficient dynamic auditing protocol in cloud storage," IEEE Trans on Parallel and Distributed Systems, Vol.25, No.10, October 2014.*
15. *Debiao He, Sherali Zeadally and Libing Wu, "Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks", IEEE SYSTEMS JOURNAL Digital Object Identifier 10.1109/JSYST.2015.2428620, pp.1-10.*
16. *B.Wang, B.Li, and H.Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc.IEEE Fifth International Conference on Cloud Computing, pp.295-302, 2012.*