ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Secure Public Auditing Scheme for Cloud Data Share Supporting User Revocation

[1] .B.Renugadevi , [2] M.Senthil Kumar
[1] Final year PG CSE Student, [2] Assistant Professor/CSE
[1][2] Sree Sowdambika College Of Engineering, Aruppukottai,Tamilnadu,India

***Abstract* – Today, distributed storage winds up noticeably one of the basic administrations, since clients can without much of a stretch change and offer information with others in cloud. Be that as it may, the honesty of shared cloud information is helpless to unavoidable equipment deficiencies, programming disappointments or human mistakes. To guarantee the trustworthiness of the mutual information, a few plans have been intended to permit open verifiers (i.e., Third Party Auditors) to productively review information trustworthiness without recovering the whole client information from cloud. But this may reveal data owners personal information to TPA. Here we are using homomorphic authenticable group signatures which is designed to protect privacy. Here, the auditors can verify the integrity of shared information on behalf of group users. The group users may include Group Managers and ordinary members. Any of the GMs can add new members or they can revoke members from the group. Transmission of data will be encrypted and even the data is stolen, the corresponding key cannot be restored. User revocation is done by the group manager using a publicly available revocation list. Once revoked, they cannot access any of the files. The main issue with the cloud is data integrity which can be resolved using MD5 algorithm. During the process of verification, the signature generated by the auditors and the one which is provided by the client are compared. If it does not match with each other, then it indicates that the data has been changed.**

Keywords- Data Integrity; Homomorphic Verifiable; revocation.

INTRODUCTION

Due to the increasing range of applications of shared information, like iCloud, Google Docs, and so on, users will transfer their information to a cloud and share it with alternative peers as a bunch. Sadly, since cloud servers are susceptible to inevitable hardware faults, computer code failures or human errors, information kept within the cloud is also spoiled or lost. Within the worst cases, a cloud owner might even conceal information error accidents so as to preserve its name or avoid profit losses. Additionally, users who lose direct management over their information don't seem to be positive whether or not their cloud-stored information is undamaged or not. Therefore, integrity verification for the shared information within the cloud is a vital.

To ensure the integrity of knowledge hold on in cloud servers, variety of mechanisms supporting numerous techniques are projected. Specifically, so as to cut back the burden on users, a trusty third-party auditor (TPA) is engaged.

ON one hand, the identity of every signer is anonymous; and on the opposite hand, the group manager will trace a signer's real identity once a dispute occurs. Sadly, in all told existing public auditing schemes, the tracing method is accomplished by one entity. As a result, that entity has the privilege of tracing, which can cause abuse of single authority power. Moreover, a necessary authentication method is missing between the auditor and also the cloud in most existing public auditing schemes, therefore anyone will challenge the cloud for the auditing proofs. This downside can trigger network congestion and inessential waste of cloud resources. Though Liu et al. designed a licensed public auditing theme to unravel the problem, it's solely appropriate for one user, and can't be applied to group-shared knowledge. Since the malicious or false auditors/users may perpetually request cloud access for the auditing proof by utilizing TPA, unauthorized auditing is another necessary issue that ought to be self-addressed in integrity verification for shared cloud knowledge.

At present, all the prevailing public auditing schemes solely take into account single group manager when applied to shared knowledge with group users. However, in real-world applications, there may be multiple managers in an exceedingly group. For example, the shared knowledge of a project team is made by multiple managers together, whats more, any of them will maintain the shared knowledge. Another necessary sensible downside is that the group users ought to be ready to dynamically enroll and revoke the group, which is able to be managed by the group managers. And considerably, once tracing the identity of the signer, a such variety of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

managers will work along, that ensures the fairness of the tracing method.

II. PROPOSED SYSTEM

Our contributions can be summarized as follows.
Here the TPA are totally machine-controlled and can be able to properly monitor confidentiality and integrity of the information and unambiguously integrate it with random mask technique to realize a privacy-preserving public auditing system for cloud data storage security whereas keeping all higher needs in mind. We do ciphering of the data using AES algorithm. Transmission of knowledge are encrypted, though the data is purloined, there's no corresponding key that can't be rebuilt. Solely the user is aware of the key, the clouds don't understand the key. User's privacy is protected as a result of user's files area unit encrypted in cloud storage.
The most important issue with the cloud is information integrity, in this paper we have a tendency to use MD5 algorithmic program for maintain the integrity of knowledge. The input message (M) is created by the sender and the message digest is computed. Encrypted message digest is connected to the input message and also the whole message is distributed to receiver. On receiving side, the message is received and the encrypted message digest is extracted. Then the own message digest of the received message is computed.

III. PROBLEM STATEMENT

In this section, we are going to see about the system model and the threat model of this project, and we are going to mention the design objectives of our public auditing scheme.

A. SYSTEM MODEL

As shown in Fig 1., the proposed system model contains four entities: cloud, TPA, trusty non-public key generator (PKG), and group users. The cloud has powerful data storing space and computing capability, and provides services (e.g., information storage, information sharing,etc.) for group users. The TPA will verify the integrity of the shared information on behalf of the group users. The PKG generates the system public parameters and group key try for group users. The group users embody 2 varieties of users: GMs (Group Managers) and standard members. In contrast to existing system models, the GMs contain multiple members who produce the shared information along and share them with the normal members through the cloud. Therefore, the GMs act because the common homeowners of the initial information, and their identities area unit equal. Meanwhile, any of the GMs will add new members or revoke members from the group. Additionally, either a GM or a normal member will access, download, and modify the shared information within the cloud. Note that multiple managers during a group is extremely common in practice. As an example, the shared information of a project team is formed by multiple managers along. Later, any of the GMs will maintain the shared information and manage the cluster users. once tracing the identity of the signer, a given variety of managers will get together to trace the identity, that ensures the fairness of the tracing method. Once a group user needs to see the integrity of the shared information, she/he 1st submits associate degree auditing request message to the TPA. Once receiving the request, the TPA challenges the cloud for associate degree auditing proof. Once the cloud receives the auditing challenge, it first of all authenticates the TPA.

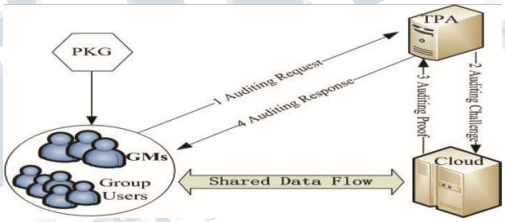

Fig. 1. The system model

B.DESIGN OBJECTIVES

To achieve integrity checking of the shared information within the cloud, our project is anticipated to supply the subsequent style objectives:

1)Public auditing:

Besides the group users, the TPA may properly check the integrity of the shared information within the cloud while not retrieving entire users' information from cloud.

2) Authorized auditing:

Only the TPA that has been licensed by the cluster users will challenge the cloud.

3) Identity privacy:

During the method of auditing, the TPA cannot learn the identity of the cluster user from the signatures of the information blocks

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

4)Traceability:
Under sure conditions, the cluster managers will reveal the signer's identity from the signatures and choose that cluster user has changed the information block.

5) Nonframeability:
Group managers will guarantee the fairness of tracing method, i.e., innocent cluster user won't be framed and therefore the misbehaved user won't be harbored by the cluster managers.

6) Support data traceability and recoverability:
Group users will simply trace information changes and recover the newest correct knowledge once current data is broken.

7) Support group dynamics:
Group dynamics embrace 2 aspects. One is that GMs will simply be part of or leave the cluster, the opposite is that new users may be simply other into the cluster and misbehaved users may be with efficiency excluded from the cluster

IV. PRELIMINARIES

In this section, we have a tendency to shortly introduce the cryptologic information applied within the project. The most important notations utilized in this paper are represented in.

A. Homomorphic Verifiable Tags
Homomorphic Verifiable Tags (HVTs) acting as the verification data of file blocks are wide utilized in integrity checking for information hold on within the cloud.

Definition 1 (Homomorphic verifiable signature). If an HVT based on group signatures can simultaneously agree to the following two properties, then the signature theme is a homomorphic verifiable signature theme. Assuming (pk,sk) are the public/private key pair of the signer, ó 1 and ó2 representing the tags of data block m1,m2 ∈Zq, respectively.

1).Blockless verification: A verifier can verify the correctness of all information through the linear combination of the data without having to retrieve it from the cloud. Specifically, given ó1, ó2 be the two random numbers y1,y2∈ Zp and data block m = y1m1+y2m2, a verifier can verify the correctness of m without having to know about m1, m2.

2) Non-malleability: Any Any entity without having the secret key cannot generates a brand new and valid tag through combining the identified tags. Specifically, given α1, α2 be the two random numbers y1, y2 ∈Zp and information block be m = y1m1 +y2m2, an entity which has no secret key cannot generate the valid tag α for m by combining α1 andα2.

V. THE PUBLIC AUDITING SCHEME

A. Overview
We assume that there's S group managers GMl(1< l≤S), and d users Ui(1 ≤i≤d)in the project. The shared knowledge M is split into w knowledge blocks, i.e. M = m1,m2,…. so as to support dynamic operations on the shared knowledge, we tend to index every knowledge block by using index hash table. Specifically, the project consists of eight algorithms: {Setup, Enroll, Revoke, Sign, Authorize, ProofGen, ProofVerify, Open}.

In Setup part, the PKG sets parameters for the complete system, distributes the group key pair and a shared public/private key pair used to authorize every GMl, and initializes the membership data Ω . Then, any GM generates a user signing communication key uski, a (public) user membership key upki, and a user revocation key rvki for Ui. GM additionally shares the authorization key pair with Ui within the enrol procedure. Once a grouo user is revoked, GM invokes the Revoke algorithmic rule to update Ω. The group user will figure the signatures of the shared knowledge block from the issued keys within the Sign method. With the Authorize algorithmic rule, the group authorizes TPA to get approved auditing challenges, so the valid TPA will check the integrity of the shared knowledge on behalf of the cluster user. Once the cloud receives a challenge from TPA, the cloud verifies whether or not the challenge has been approved and decides whether or not to get the audit proof via ProofGen. The correctness of the proof is checked by TPA via ProofVerify.

B. Support Data Traceability and Recoverability
Since the identity of every data block will be represented by the index hash table, i.e., idj={vj,rj}, wherever vj is denoted because the virtual index of block mj, and rj could be a random variety generated by a collision-resistant hash perform, each cluster user will simply perform dynamic operations on the shared knowledge, the main points of which might be found in. However, if the information block has been modified maliciously, the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

cluster user cannot trace the changes and recover the correct knowledge. To support knowledge tracing and recovery, we've designed an extra organisation supporting binary tree for the cloud server to record each modification of knowledge block. Through the records, group users will simply trace knowledge changes. Once the change has been found, group users will recover the correct knowledge by the records. Because the cluster users will verify the older blocks one by one till discover the most recent correct block.

C. Using One Time Signatures

A one-time signature is predicated on a group of public commitments to secrets that the signer indiscriminately generates. The random key are generated for every file and this can be entered so as to access and use the file.Hence if the user isn't valid he/she isn't ready to access the file since the indiscriminately generated secret is essential for the file access. However, every set of such committed secrets are often wont to sign only 1 (or a few) messages.

The user can get a mail confirmation message that may well be a random key generated on an individual basis for every file and this can be entered so as to access and use the file from the cloud. Thus if the user isn't valid he/she isn't ready to access the file since the indiscriminately generated secret is essential for the file access. Once the accessing of file is completed by the user, they will with efficiency use the file as per would like. This may be restricted inside a gaggle of persons still. During a company or organizations say as an example, the users are often restricted since there could also be confidential knowledge gift inside the organization. Thus it's pretty much essential to own random key that is exclusive for a file.

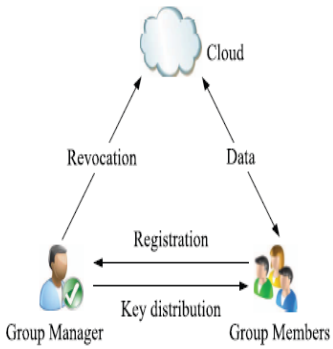

Fig 2: System model for User Revocation

D. Construction of the model

Here, we have a tendency to describe the main points of the eight algorithms enclosed. To safeguard information privacy, the information may be encrypted by the means of symmetrical cryptography technology and attribute-based cryptography technology before shared data is outsourced to the cloud; but, this can be outside the scope of our paper.

Setup Phase

The user initializes the general public and secret parameters of the system by executing KeyGen, and pre-processes the info file F by the help of SigGen to get the verification data. The user then stores the information file F and therefore the verification data at the cloud server. The user could alter the information file F by activity updates on the keep data in cloud.

Audit Phase

Auditors sends audit message to the cloud server to create positive verification to check that the cloud server has maintained the data file F properly at the time of the auditing. A response message is created by the cloud server by executing Genproof using file F and its verification information as input. The response by cloud server will be verified by the TPA using Verify Proof.

A owner may be a one who will access resources from the cloud. The owner would initially register to the interface to urge the services with the valid username and password. Thus to properly check the integrity of the whole information, a public verifier has to opt for the acceptable public key for every block. Then they will request for the file to the cloud service provider. There will be a 3rd party auditor who performs the integrity checking of the knowledge before providing it to the owner or the clients. The owner has the option of downloading the verified file and conjointly uploads new files. When encrypting the blocks, currently a hash value for the blocks are generated on an individual basis. For this purpose a hashing algorithmic rule MD5 is being employed. A good hashing operate should give a 1 method hash operate. In this, it's simple to reason on the input file however troublesome to revert it back to traditional input. It should even be collision resistant. During this options it's troublesome to search out hashes with same output for various inputs.MD5 algorithmic rule supports each the property of 1 way hash operation and collision resistant hash operation. So MD5 is employed for hashing within the planned system. MD5 is more practical and secure. The information owner build use of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

cloud storage to store the encrypted sort of data. There's no further computing burden on cloud server. This can be one amongst the advantage of the planned system. As a result of as mentioned earlier most of the present theme involve cloud server for computing still as storage purpose too. Because the information is keep in encrypted type, that the cloud server has zero information concerning the information. Still as if the cloud server turns into malicious server or is attacked by any outside aggressor, the information won't be retrieved simply because it is within the encrypted type and it's not aware of it.

There are 2 styles of threats connected to shared knowledge integrity. One is that external hackers would possibly corrupt the shared knowledge within the cloud, so cluster users will no longer access the proper knowledge. The opposite is that the cloud might corrupt or delete the shared knowledge because of the hardware/software breakdown or human made mistakes. What's worse, the cloud might repair the fact of knowledge harm from users so as to keep up self interest and service name.

E.User Revocation

GMs maintain a users-list, that consists of every user's key and expiration time. The deed users not solely ought to be prevented from accessing these outsourced knowledge that were antecedently accessible for them, however additionally cannot access these after outsourced knowledge, although their attributes satisfy the corresponding access policies. The group manager performs user revocation with the help of a public out there revocation list. Supporting that cluster members will cipher their knowledge files and make sure the confidentiality against the revoked users. During this case, any group manager will invoke Revoke algorithm and also the membership information are going to be updated. The users who are revoked by the group managers will no longer be able to access the files in the group. If they want to access the files, they have to register and they should get authenticated.

VI PERFORMANCE ANALYSIS

Computation Cost

During auditing, the TPA 1st generates some random values to construct the auditing message, that solely introduces a tiny low cost in computation. Then, when receiving the auditing message, the cloud server must generate a proof .Next to computation cost we are going to see the one which is concerning about communication cost, that is especially introduced by 2 factors.

Communication Cost

The communication cost is especially introduced by 2 factors: the auditing message and also the auditing proof. For every auditing message , the communication cost will be c(|q| + |n|) bits, wherever |q| is that the length of a component of Zq associated |n| is that the length of an index.

mpk is used to denote shared group public key mskl is used to denote the secret key ofGMl fspk,sskg is used to denote the public/private key pair
uski is used to denote the user signing key
upki is used to denote the user membership key

rvki is used to denote the user revocation key

(Vj1; Vj2) is used to denote the signature of the blockmj

VII. CONCLUSION

A secure and efficient privacy conserving public auditing theme has been proposed. It achieves privacy-preserving and public auditing for cloud by employing a TPA (Third Party Auditor), who will do the auditing process without having to retrieve the information copy, therefore privacy is preserved. The information is kept within the encrypted format within the cloud storage, thus maintaining the confidentiality of information. The information integrity is verified by TPA for the asking of the clients by verifying the signatures. It solely check whether or not the kept in knowledge is tampered or not and informs regarding it to the user. The cloud server is employed solely to store the encrypted kind of knowledge and so providing no on-line computing burden on that.

ACKNOWLEDGMENT

This paper was supported by Sree Sowdambika College of Engineering, Final Year PG Computer Science student Ms.B.Renugadevi (Reg.no:921816405011) guided by Asst.Prof of Computer Science Mr. M.Senthil Kumar. The authors thank to their colleagues for their help and support at different stages of the system development. Finally, we would like to thank the anonymous reviewers for their helpful comments.

REFERENCES

[1] D. Fernandes, L. Soares, J. Gomes, et al, "Security issues in cloud environments: a survey," International Journal of Information Security.

[2] W. Hsien, C. Yang, and M. Hwang, "A survey of public auditing for secure data storage in cloud computing," International Journal of Network Security, vol.18, no.1, pp. 133-142, 2016.

[3] J. Yu, K. Ren, C. Wang, et al, "Enabling Cloud Storage Auditing with Key-Exposure Resistance," IEEE Transactions on Information Forensics and Security, vol.10, no.6, pp. 1167-1179, 2015.

[4] Q. Wang, C. Wang, K. Ren, et al, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[5] S. Yu, "Big privacy: challenges and opportunities of privacy study in the age of big data," IEEE Access, vol. 4, no. 6, pp. 2751-2763, 2016.

[6] C. Wang, Q. Wang, K. Ren, et al, "Privacy-preserving public auditing for data storage security in cloud computing," Proceedings of IEEEINFOCOM, pp. 1-9, 2010.

[7] B. Wang, B. Li, and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," IEEE Transactions on Cloud Computing, vol.2, no.1, pp.43-56, 2014.

[8] B. Wang, B. Li, and H. Li, "Knox: privacy-preserving auditing for shared data with large groups in the cloud," Applied Cryptography and Network Security. Springer Berlin Heidelberg, pp. 507-525, 2012.