International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

Cloud dynamic data Storage using group signature & public integrity auditing

M.Ramesh Babu[1]& Ms.B.Uma Maheswari [2]

[1]M-Tech,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

[2]Asst.Professor,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

Abstract:

The approach of the cloud computing makes stockpiling outsourcing turn into a rising pattern, whichadvances the safe remote data reviewing an interesting issue that showed up in the examination writing. As oflate some exploration consider the issue of secure and proficient public data trustworthiness inspecting forshared element data. On the other hand, these plans are still not secure against the intrigue of cloud storageserver and denied group users during user revocation in functional cloud storage framework. In this paper, wemake sense of the agreement assault in the leaving plan and give a proficient public trustworthiness reviewingplan with secure gathering client disavowal taking into account vector duty and verifier-neighborhoodrepudiation bunch signature. We plan a solid plan taking into account our plan definition. Our plan bolsterspeople in general checking and proficient client renouncement furthermore some decent properties, forexample, certainly, productivity, tally capacity and traceability of secure gathering client disavowal. At last, thesecurity and exploratory examination demonstrate that, contrasted and its pertinent plans our plan is likewisesecure and proficient.

Keywords: Cloud computing, dynamic data, group signature, public integrity auditing, victor commitment.

1. INTRODUCTION

The advancement of cloud computing persuades endeavors what's more, associations to outsource their data to outsider cloud service provider(CSPs), which will enhance the capacity impediment of asset oblige nearby gadgets. As of late, some business cloud storage services, for example, the basic stockpiling service(S3) on-line information reinforcement services of Amazon and some down to earth cloud based software Google Drive have been manufactured for cloud application. Since the cloud servers may give back an invalid result in some cases, for example, server hardware/software disappointment, human upkeep and pernicious assault [7],[8] new

structures of affirmation of information honesty and availability are required to ensure the security and protection of cloud client's information. For giving the respectability and accessibility of remote cloud store, a few arrangements [9], [10], [9] and their variations have been proposed. In these arrangements, when a plan bolsters information alteration, we call it element plan, generally static one (or restricted element plan, if a plan could just effectively bolster some predetermined operation, for example, affix). A plan is freely obvious implies that the information uprightness check can be performed by information proprietors, as well as by any outsider evaluator. Then again, the dynamic plans above spotlight on the situations where there is an information proprietor what's more, just the information proprietor could change the information. To apply vector commitment plan [10] over the database, at that point we influence the Asymmetric Group Key Agreement (AGKA) [8] and bunch marks [9] to bolster cipher text information base overhaul among bunch clients and effective gathering client denial separately. In particular, the gathering client utilizes the AGKA convention to encrypt/decrypt the offer database, which will promise that a client in the gathering will be capable to encrypt/decrypt a message from some other gathering clients. The gathering mark will keep the intrigue of cloud and denied bunch clients, where the information proprietor will join in the client disavowal stage and couldn't disavow the information that last altered by the revoked client.

2. RELATED WORK

Existing system

Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse. Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Data in a target VM could be stolen by instantiating another VM co-resident with the target one. Regarding availability of files, there are a series of cryptographic schemes which go as far as allowing a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owner’s anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality. A cryptographic solution, with proven security relied on number-theoretic assumptions is more desirable, whenever the user is not

perfectly happy with trusting the security of the VM or the honesty of the technical staff. These users are motivated to encrypt their data with their own keys before uploading them to the server.

Disadvantages of existing system

- Unexpected privilege escalation will expose all
- It is not efficient.
- Shared data will not be secure.

Proposed System

Providing the integrity and availability of remote cloud store, some solutions and their variants have been proposed. In these solutions, when a scheme supports data modification, we call it dynamic scheme, otherwise static one (or limited dynamic scheme, if a scheme could only efficiently support some specified operation, such as append). A scheme is publicly verifiable means that the data integrity check can be performed not only by data owners, but also by any Third-Party Auditor. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server.These software development environments, multiple users in a group need to share the source code, and they need to access, the shared source code at any time and place.The deficiency of above schemes motivates us to explore how to design an efficient and reliable scheme,while achieving secure group user revocation. To the end, we propose a construction which not only supports group data encryption and decryption during the data modification processing, but also realizes efficient and secure user revocation.

3. IMPLEMENTATION

Cloud Storage Model

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.Cloud storage services may be accessed through a co-located cloud computer service, a web serviceapplication programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.who are authorized to access and modify the data by the data owner. The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA

could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access to a number of group users.

Data Group sharing:

In these software development environments, multiple users in a group need to share the source code, and they need to access the shared source code at any time and place who ever existing their Groups.

Public integrity auditing:

Public integrity auditing for shared dynamic data with group user revocation. Our contributions are three folds:We explore on the secure and efficient shareddata integrate auditing for multi-user operationfor cipher-text database.By incorporating the primitives of Asymmetric Group key agreement and Group Signature, we propose an efficient data auditing scheme. We provide the security and efficiency analysis of our scheme, and the analysis results show that our scheme is secure and efficient.

Revoked Group Users

The group signature will prevent the collusion of cloud and revoked group users, where the data owner will take part in the user revocation phase and the cloud not revoke the data that last modified by the revoked user. An attacker outside the group (include the revoked group user cloud storage server) may obtain some knowledge of the plaintext of the data. Actually, this kind of attacker has to at l break the security of the adopted group data encryption scheme. The cloud storage server colludes with the revoked group users, and they want to access the Cloud Data. Actually, in cloud environment, we assume that the cloud storage server is semi-trusted. Thus, it is reasonable that a revoked user will collude with the cloud server and share its secret group key to the cloud storage server. In this case, although the server group user revocation way brings much communication and computation cost saving, it will make the scheme insecure against a malicious cloud storage server who can get the secret key of revoked users during the user revocation phase. Thus, a malicious cloud server will be able to make data m, last modified by a user that needed to be revoked, into a malicious data m′. In the user revocation process, the cloud could make the malicious data m′ become valid. To overcome the problems above, A scheme is correct if for any database and for any updated data m by a valid group user, the output of the verification by an honest cloud storage server is always the value Data (m).

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

Group signature:

Group signature is introduced by Chaum and Heyst It provides anonymity for signers, where each group member has a private key that enables the user to sign messages. However, the resulting signature keeps the identity of the signer secret. Some systems support revocation where group membership can be disabled without affecting the signing ability of unrevoked users. Boneh and Shacham proposed an efficient group signature with verifier-local revocation. Also, the scheme is a short signature scheme where user revocation only requires sending revocation information to signature verifiers. Libert et al.proposed a new scalable revocation method for group signature based on the broadcast encryption framework. However, the scheme introduces important storage overhead at group user side. Later, Libert et al.designed a scheme to enhance the former scheme which could obtain private key of constant size. In their scheme, the unrevoked members still do not need to update their keys at each revocation.

Fig:-1the cloud storage model

4. EXPERIMENTAL RESULTS

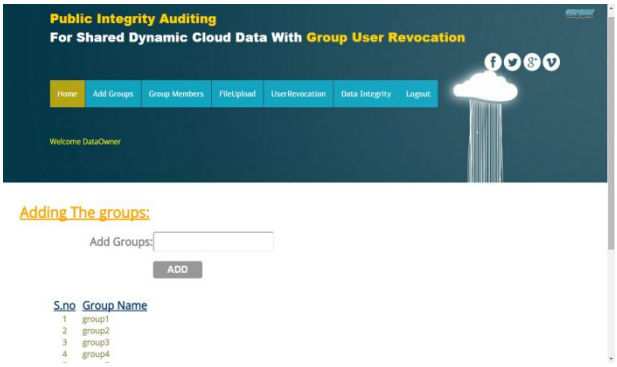

Fig:-2Adding Groups

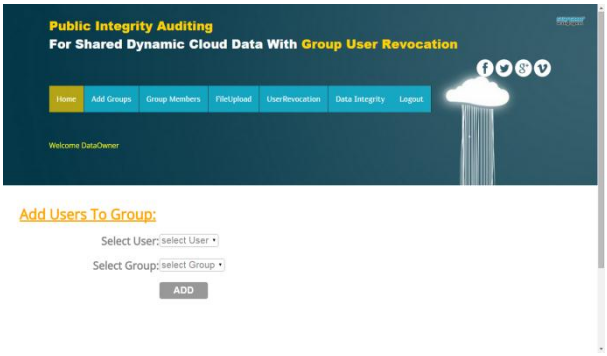

Fig:-3 Adding Users to group

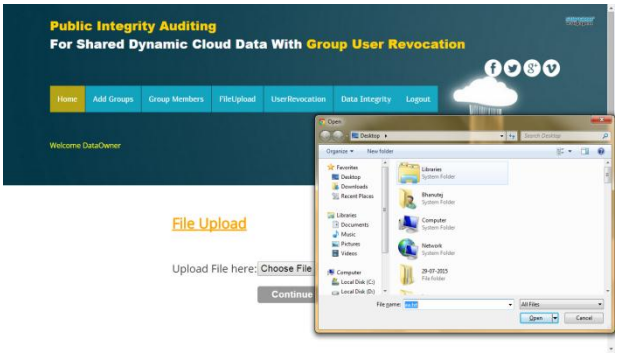

Fig:-4 Data Uploading

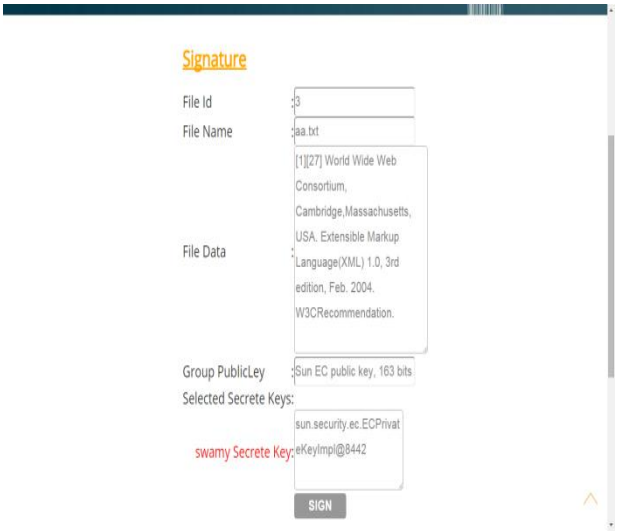

Fig:-5 Signature with user public key

Fig:-6 Auditor Results

5. CONCLUSION

The primitive of unquestionable database with proficient upgrades is a critical approach to take care of the issue of obvious outsourcing of capacity. We propose a plan to acknowledge proficient and secure data integrity reviewing for offer dynamic data with multi-client alteration. The plan vector responsibility, Asymmetric Gathering Key Agreement (AGKA) and group signatures with client denial are receive to accomplish the data honesty examining of remote data. Adjacent to people in general data examining, the joining of the three primitive empower our plan to outsource ciphertext database to remote cloud and bolster secure gathering clients denial to shared dynamic data. We give security examination of our plan, and it demonstrates that our plan give data privacy to gathering clients, furthermore, it is additionally secure against the conspiracy assault from the cloud storage server and disavowed group clients. Likewise, the execution examination demonstrates that, looked at with its pertinent plans, our plan is additionally productive in distinctive stages.

6. REFERENCES

[1]. Amazon. (2007) Amazon simple storage service (amazon s3).Amazon.[Online]. Available:http://aws.amazon.com/s3/

[2]. Google. (2005) Google drive. Google.[Online].Available:http://drive.google.com/

[3]. Dropbox. (2007) A file-storage and sharing service.Dropbox.[Online]. Available: http://www.dropbox.com/

[4]. Mozy. (2007) An online, data, and computer backup software.EMC. [Online]. Available: http://www.dropbox.com/

[5]. Bitcasa. (2011) Inifinite storage.Bitcasa.[Online].Available:http://www.bitcasa.com/

[6]. Memopal. (2007) Online backup. Memopal. [Online].Available: http://www.memopal.com/

[7]. M. A. et al., "Above the clouds: A berkeley view of cloudcomputing," Tech. Rep. UCBEECS, vol. 28, pp. 1–23, Feb.2009.

[8]. M. Rabin, "Efficient dispersal of information for security," Journal of the ACM (JACM), vol. 36(2), pp. 335–348,Apr. 1989.

[9]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable data possession atuntrusted stores," in Proc. of ACM CCS, Virginia, USA, Oct. 2007, pp. 598–609.

[10]. A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of ACM CCS, Virginia, USA, Oct.2007, pp. 584–597.