RESEARCH ARTICLE OPEN ACCESS

Public Auditing for Shared Cloud Data with Group User Revocation

N.Gayathri[1], Dr.A.Nagarajan[2]
[1, 2](Dept. of Computer Applications, Alagappa University, and karaikudi)

Abstract:

In cloud computing data to be shared in cloud, in the process to be performed in sharing data to be secure manner in publically, revocation to be used for the purpose of existing user to revoked resign that the process of entering to the cloud then getting data and upload the information from the cloud. In this concept, we propose it is cloud audit the efficient by the revocation user. More proxy a signature by resign by the existing users, public auditing it is a shared data to be verifiable, it is no need without process of sharing data from cloud, in this mechanism batch auditing verify multiple auditing simultaneously, multiple it is the performance to be highly efficient in the asymmetric key algorithm to be used securely performed. It is the purpose of easily get the information from the cloud sequentially, experimentally results do that improve efficiency in user revocation.

Keywords — **Shared Data, Revocation, Public Auditing, Revoked Signature.**

1. INTRODUCTION

In cloud data services, it will be regular put to information to be not main saved in the cloud, as well as imparted crosswise over different clients.Cloud computing gives surroundings to asset offering framework, middleware's furthermore requisition improvement platforms Also business requisition. Those bases may be to the vast majority a feature provided for by a third party may be gotten on with those help about web.Cost will a chance to be diminished for a significant level previously, light of the truth that the individual's stronghold might be furnished to third party. Those cloud registering develops and endeavour outsider of the cloud service providers (CSP), it will be outsourcing of the data, it will enhance those stockpiling constraint from claiming asset hold numerous the nearby gadgets. Recently, a portion of the business cloud storages would give they need aid internet reinforcement administrations from claiming amazon Also exactly cloud based useful administrations starting with Google drive, Picasa and Mozilla they need fabricated for cloud provision. Some case, cloud servers may occur some errors, it causes from human maintenance or malicious attack, its rectify from new assurance to protect the security and privacy of cloud users data.

II.LITERATURE SURVEY

Title:Convergent Dispersal: Toward Storage-Efficient Security in a Cloud-of-Clouds.

Author:Mingqiang Liand Chuan Qin

Description:

Cloud of clouds storage avoids cloud storage vendors it's provided fault tolerance and avoid vendor. It's inherent the diversity property and keyless data security through dispersal algorithm. However, the keyless security of existing (dispersal algorithms relies on the embedded random information, which breaks data reduplication of the dispersed data. To at the same time enable keyless security and reduplication, we propose a novel dispersal approach called focalized dispersal, which replaces one of a kind sporadic information with deterministic cryptographic hash information that is gotten from the primary data however can't be inferred by attackers without knowing the whole data.

Title: Privacy-Preserving Public Auditing for Secure Cloud Storage.

Author:Cong Wang, Qian Wang

Description:

Cloud computing storage turns into a rising pattern, as of late some examination considers the issue of secure and proficient open information respectability inspecting for shared dynamic information. This advances the safe remote information inspecting an interesting issue that showed up in the examination writing. In any case, these plans are as yet not secure against the conspiracy of cloud store server and denied numerical gathering clients amid client repudiation in viable distributed storage framework. At long last, the security framework and exploratory examination appearance that contrasted and its applicable plans our plan is likewise secure and proficient.

Title: PCPOR: Public and Constant-Cost Proofs of Retrievability in Cloud.

Author:Jiawei Yuan and Shucheng Yu

Description:

For data storage outsourcing services, it is vital to enable clients to e-client and safely confirm that distributed storage servers store their information accurately. To address this issue, various Proof of Retrievability (POR) and Proof of Data Possession (PDP) plans have been proposed wherein servers must demonstrate to a verifier that information are put away effectively. While existing POR and PDP schemes over decent solutions addressing various practical issues, they either have non-trivial (linear or quadratic) communication and computational complexity, or only consider private verification. In this paper, we propose the _rst POR scheme with public variability, constant communication and computational costs on users. In our scheme, messages exchanged between cloud servers and users are composed of a constant number of group elements and random numbers; computational tasks required on users are also constant; batch auditing of multiple tasks is also anciently supported. We achieved these by a unique design based on our novel polynomial-based authenticators.

III. EXISTING SYSTEM

In existing system, every signature is connected to each block in information, that the information accuracy of the considerable signatures. Public verifier provides the verification services, who would like to utilize cloud data for third party auditor (TPA).

Disadvantages of Existing System

- Users are used limited amount of communication and resources, but straightforward method may costlier.
- Shared data will not be secure.
- Unexpected collisions destroyed the data.

IV. PROPOSED SYSTEM

In proposed system incorrectness of shared data to save reputation of its data services and avoid losing money of its data services. It's no collusion to be occurring in this task large number of users to share data in performance to handle multiple auditing tasks simultaneously with batch auditing.

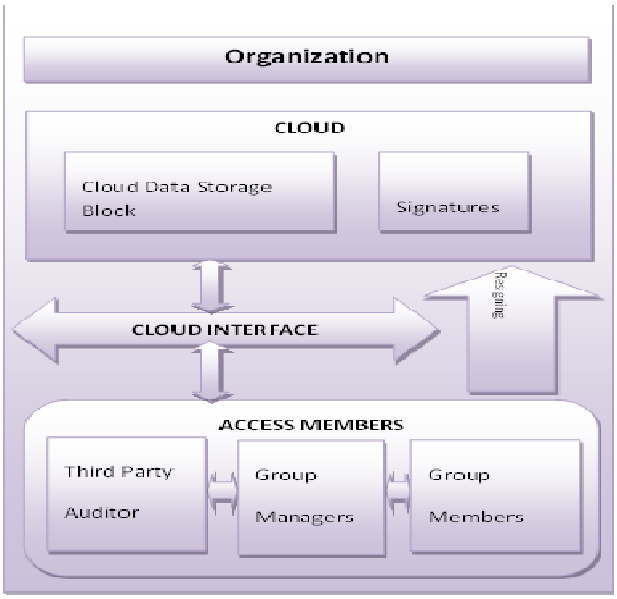
Advantages of proposed system

- Blocking user account.
- Security questions.
- Login with secret key in each time.
- Large number of task to auditing simultaneously and efficiently.

IV. SYSTEM ARCHITECTURE

Cloud Data Storage Block

Authorized person get the space from the cloud and stored data in this cloud it is secure and easy to get from this cloud.it is stored large number of data and may not be collusion. Users and requestors retrieve and upload from the separate cloud storage.



Signatures Block

Signature block it is unique from each user, asymmetric group key agreement (AGKA) it is highly secured in this task then the performance is high.it is the process of resigned and revocation users.

Cloud Interface

Cloud interface it is intermediate to cloud data storage block, access members, and resigning request.

Resigning Request

Enable the cloud to re-sign blocks for existing clients during client revocation, so that existing clients don't have to download and re-sign blocks independent from anyone else.

Access Members

Third party auditor, group managers and group members those are allocated by cloud storage

and intermediate to each other. It is the process reviews to be stored in database.

VI.TECHNIQUES USED FOR ALGORITHM

User Revocation - Basic Algorithm

- Share File
- Edit Share File

Batch Verify Algorithm

- Authentication

Key Generation Algorithm

- TPA send key to Users.

Asymmetric Group Key Agreement (AGKA)

Asymmetric Group Key Agreement (AGKA) and gathering signatures to cipher text data base update among group customers and successful group client revocation independently. Specially, in this cloud clients utilize the AGKA protocol to the process of encryption and decryption to share the database, it is a certification of the users in this gathering to encode and decode messages to some other group users. The group signature will keep the collusion of cloud and revoked group users, where the data proprietor will share in the client user revocation phase and the cloud couldn't revoke the data that last changed by the revoked users. Be that as it may, the plan presents imperative storage overhead at group user side.A plan to upgrade the previous plan which could acquire private key of constant size. In their plan, the unrevoked individuals still don't have to refresh their keys at every revocation.

A goal of GKA protocol its correctness to establish a confidential channel for group members. We use the goal its correctness of the GKA protocol the goal to perform that the approaches from GKA protocols.

- Accuracy
- Asymmetric group key agreement.
- Freshness.
- Secrecy of GKA.

Sign: The signature of any string s 2 {0, 1}_ under the public key pk is = XH(s)r.

Verify: Given a message-signature pair (s, _), the verification equation is e (_, g) e (H(s), R) = A.

If the equation holds, yield 1 to speak to that purported signature is valid.

Else yield 0 and reject the purported signature.

Encryption: encryption for a plaintext m 2 GT, randomly select t 2 Z_ p and compute c1 = g t,

c2 = R t, c3 = m At.

Decryption: After receiving a cipher text (c1, c2, c3), anyone with a valid messAge-signature pair

(s, _) can extract:m = c3 e (_, c1) e (H(s), c2).

The correctness of the proposed a direct verification. Define by (R1, A1) (R2, A2) = (R1R2, A1A2) and _ by _1__2 = _1_2.

For security, we have the following claims in which Claim 2 follows from theDefinition of and _, and the security proof of Claim 3 can be found in the fullVersion of the paper.

VII. EXPERIMENTAL RESULTS

Implementation is the phase of the venture when the hypothetical plan is transformed out into a working framework. Therefore it can be thought to be the most basic stage in accomplishing a fruitful new framework and in giving the client, certainty that the new framework will work and be compelling. The execution organize includes planning, examination of the current framework and its requirements on usage, designing of methods to achieve changeover and assessment of changeover strategies. It is efficiency of the security for public data integrity auditing of the multi user modification, data can be encrypted among the dynamic group and group user can conduct and it is secure and vulnerable,and any group user can conduct secure and verifiable data update when necessary.

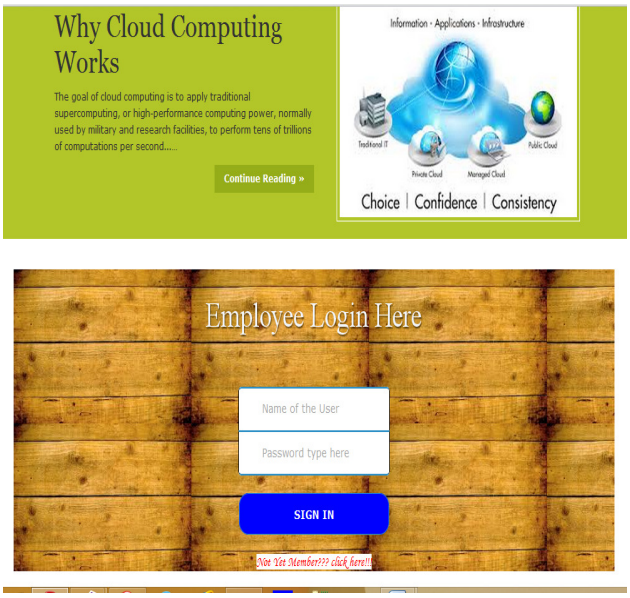


Fig 1: LOGIN PAGE

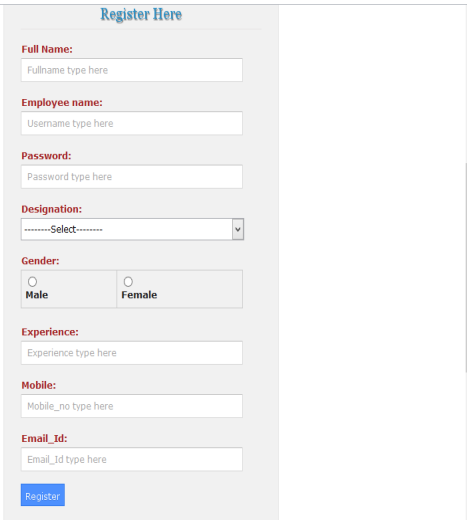


Fig 2: REGISTRATION PAGE

Fig 3: USER HOME

Fig 4: ADMIN LOGIN

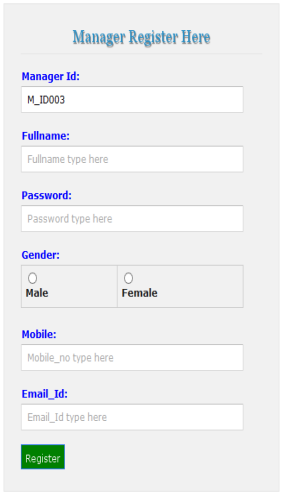


Fig 5: REGISTRATION PAGE

Fig 6: GROUP MEMBER

Fig 7: SIGN GENERATION

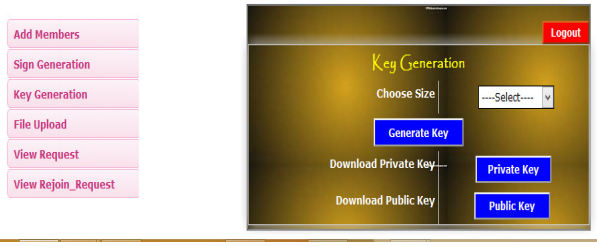


Fig 8: KEY GENERATION

Fig 9: FILE UPLOAD WITH KEY

Fig 10: KEY REQUEST

Fig 11: GET KEY AND FILE

Fig 12: VERIFY USER KEY

Fig 13: ACCESS CLOUD FILE

Fig 14: REVOCATION REQUEST

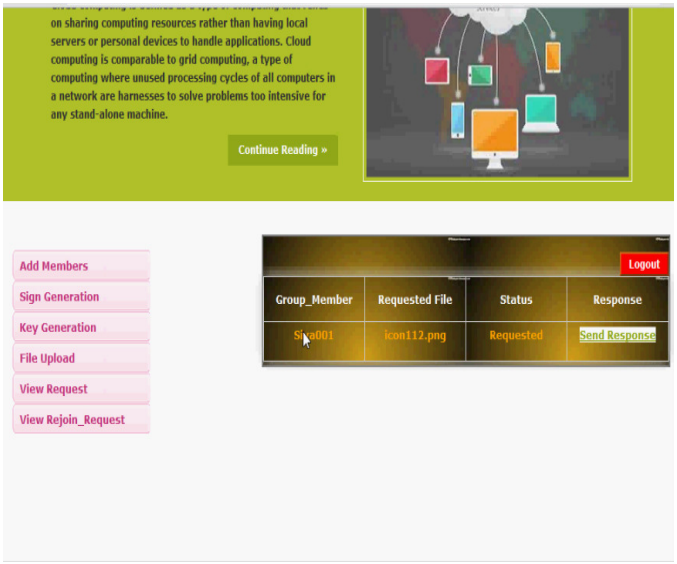


Fig 15: SEND RESPONSE

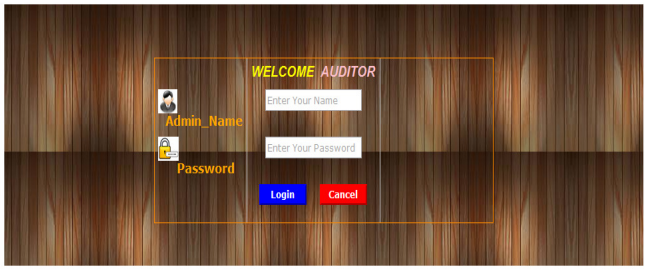


Fig 16: AUDITOR LOGIN

Fig 17: REPEAL USER DETAILS

VIII. CONCLUSION

We proposed a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. Secure data for share dynamic data with multi user modification. Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data. The public data auditing consists of the three primitive contain of our scheme to cipher text database to remote cloud and secure group users revocation to shared dynamic data. It give security analysis of our plan, and it demonstrates that our plan give data confidentiality to group users, and it is likewise secure against the collusion attack from the cloud storage server and revoke group users.

ACKNOWLEDGMENT

I would like to thank Dr.A.Nagarajan for his guidance and support and I also would like to thank Head of Department Dr.v.palanisamy for preparing this paper.

REFERENCES

[1] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, —Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud‖, IEEE Transactions on Service Computing No: 99 Vol: Pp Year 2014.

[2] B. Wang, B. Li, and H. Li, —Public Auditing for Shared Data with Efficient User Revocation in the Cloud,‖ in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, —A View of Cloud Computing,‖ Communications of the ACM, vol. 53, no. 4, pp. 50–58, April 2010.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, —Provable Data Possession at Untrusted Stores,‖ in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

[5] H. Shacham and B. Waters, —Compact Proofs of Retrievability,‖ in the Proceedings of ASIACRYPT 2008. Springer-Verlag, 2008, pp. 90–107.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, —Ensuring Data Storage Security in Cloud Computing,‖ in the Proceedings of ACM/IEEE IW QoS 2009, 2009, pp. 1–9.