ijecs
open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.18001-18004

Group User Revocation and Integrity Auditing Of Shared Data in Cloud Environment

P.Ayeesha Khan

PG Scholar Dept of CSE ,Madanapalle Institute of Technology and Science, Computer Science and Engineering,
Madanapalle, Chittoor district of Andhra Pradesh, India
ishakhan728@gmail.com

Abstract— ***So many investigations are made on safety issues and data integrity auditing for sharing the dynamic data. Cloud computing provides secure remote data auditing for storage purpose. But it does not provide secure from collision of cloud storage server and revoked and revoked group customers during user revocation in practical cloud storage system. In This paper, we determine the collusion attack within the existing plan and supply a competent public integrity auditing plan with secure group user revocation according to vector commitment and verifier-local revocation group signature. We design a concrete plan in line with the plan explanation. Finally, the safety and experimental analysis expose that, in comparison using its relevant schemes our plan can also be safe and effective.***

Index Terms— Public integrity auditings, dynamic dates, vector commitments, group signatures, cloud computing.

1 INTRODUCTION

Cloud computing motivates businesses and organizations to delegate their data to 3rd-party cloud providers (CSPs), that will insert to the storage control of resource compress local products [1]. Public integrity auditing plan with make safe group user's revocation according to vector commitment and verifier-local revocation group signature. Commitment is a fundamentals primitives in cryptographies and it plays an important role in security pro-tocols such as voting, identification, zero-knowledge proof, etc. It returns either valid or invalid. The latter response can indicate either that σ is not a valid signature, or that the users who produce it contain been revoked. Our plan utilizes bilinear group's safety beginning by the assumption of Strong Diffie-Hellman and also the Decision Straight line.

Our model in cloud helps make the remote data auditing schemes become infeasible, where just the data owner can update its data [2]. Particularly, the audience user uses the AGKA protocol to secure/decrypt the proportion database that will be certain that a person within the group will have the capacity to secure/decrypt a note from the other group patrons. We leverage the Uneven Asymmetric Group Key Agreement (AGKA) and group signatures to aid cipher text database update among group customers and efficient group user revocation correspondingly.

We designed an Asymmetric Group Key Agreement scheme (AGKA). The shared encryption key is negotiated in an AGKA protocol. The audience signature may prevent the collusion of cloud and revoked group customers, in which the data owner will play in the users revocation phase and also the cloud couldn't revoke the information that last modified through the revoked user. Our idea is to use vector commitment plan within the database. We presented related work in section 2. In section 3 present frameworks of cloud storages. In section 4 provides system model. In section 5 provides UML diagram. In section 6 provides Results and Discussions. In section 7 provides references. In section 8 provides Conclusion.

2. Related Work

Burns and Ateniese [3] introduce a model for provable data possessions .It allows users for storing the

DOI: 10.18535/ijecs/v5i9.36

data at an untrusted server to confirm that the server contains the original data.

Proofs of retrievability are discovering by **Juels and Kaliski [4]**. A POR scheme enable a archive or back-up services (prover) to produce a concise proof that a user (verifier) can retrieves a target files *F*, that is, the archived maintain and reliably transmits file data sufficient for the users to recover *F* in its total.

This scheme enable a backup services to produce a concise proof that a verifier can retrieves a target files F, **Erway and Kupcu[5]** discussed a provable data possession model providers the users preprocess the information and then send it to an untrusted server for storage.

Wang and Ren [6] discussed privacy-preserving public auditing for data storage security in Cloud computing.

3. Framework of Cloud Storages For Group User Revocation And Integrity Auditing Of Shared Data

The Strong Diffie-Hellman problem, the choice Straight line problem and also the Computational Diffie-Hellman problem. Commitment is really a fundamental primitive in cryptography also it plays a huge role in security methods for example voting, identification, zero-understanding proof, etc.. The safety from the plan is dependent around the Strong Diffie- Hellman assumption and also the Decision Straight line assumption. Within this section, we evaluate the definitions of bilinear groups and also the complexity assumption [7]. The hiding property of commitment mandates that it shouldn't representation information from the committed message, and also the binding property mandates that the carrying out mechanism shouldn't allow a sender to alter his/her mind concerning the committed message. We present the formal meaning of group signatures with verifier-local revocation. We think about the database DB as some tuple. Informally, an open integrity auditing plan with updates enables an origin-restricted client to delegate the storage of the large database to some remote server. We offer the formal meaning of our plan based on the definition. Then, we design the concrete plan according to our definition. Later, the customer can retrieve increase the database records kept in the server and openly audit the integrity from the up-to-date data. Based on previous researches, the suggested framework in our public integrity auditing for shared dynamic cloud information with secure group users revocation is offered. We offer a concrete plan from vector commitment and verifier-local revocation group signature. In cloud storage outsourcing atmosphere, the outsourced information is usually encoded database that is usually unconditionally assumed within the exiting academic research [8]. Some fundamental tools happen to be accustomed to construct our plan. Thus we think that the actual foundations feel at ease, including the vector commitment, group signature, and uneven group key agreement plan. Our plan is made to solve the safety and efficiency problems of public data integrity auditing with multi-user modification, in which the data needs to be encoded among an engaged group and then any group user can conduct secure and verifiable data update at the appropriate interval.

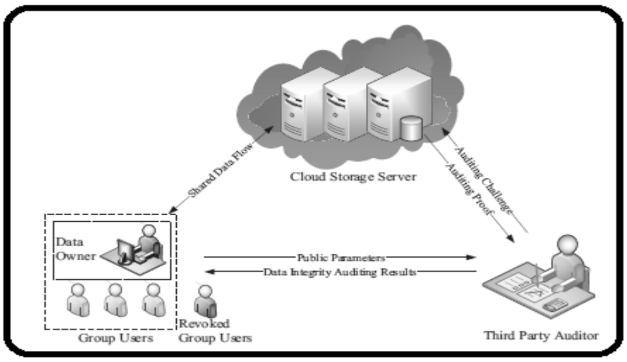

Fig.1.Framework of cloud storages

4. System Model

Group patrons contain an information holder and numerous customers who're approved to gain access to and customize the data through the data holder.

The cloud storage server is semi-reliable, who provides data storage services for that group customers. TPA might be any entity within the cloud that will have the ability to conduct the information integrity from the shared data kept in the cloud server. We first describe the cloud storage type of our bodies [9]. Then, we offer the threat model considered and security goals you want to complete. Within the cloud storage model, you will find three organizations, namely the cloud storage server, group customers along with a Third Part Auditors (TPA). Within our system, the information holder could secure and upload its data towards the remote cloud storage server. Our threat model views two kinds of attack:

i) An assailant outside the audience (range from the revoked group user cloud storage server) may obtain some understanding from the plaintext from the data. Really, this type of attacker needs to at least break the safety from the adopted group data file encryption plan.

ii) The cloud storage server colludes using the revoked group customers, and they would like to give an illegal data without having to be detected. Also, he/she shares the privilege for example access and modify (compile and execute if required) to numerous group customers. The TPA could efficiently verify the integrity from the data kept in the cloud storage server; the information is frequently up-to-date through the group customers.

5. REFERENCES

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

[2] X J. G. et al. (2006) the expanding digital universe: A forecast of worldwide information growth through 2010. IDC.[Online]. Available: Whitepaper.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *Proc. of ACM CCS*, Virginia, USA, Oct. 2007.

[4] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in *Proc. of ACM CCS*, Virginia, USA, Oct. 2007.

[5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. of ACM CCS*, Illinois, USA, Nov. 2009.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. of IEEE INFOCOM 2010*, CA, USA, Mar. 2010.

[7] Cloud9. (2011) your development environment, in the cloud. Cloud9. [Online].

[8] Codeanywhere. (2011) online code editor. Codeanywhere. [Online].

[9] D. Boneh and X. Boyen, "Collision-free accumulators and fail stop signature schemes without trees," in *Proc. of EUROCRYPT2004*, Interlaken, Switzerland, May 2004.

[10]"Bernd Bruegge, Alle H.Dutoit","Object-Oriented Software Engineering" using for UML 2nd edition.

6. CONCLUSION

We advised a plan to understand efficient and secures data integrity auditing for shared dynamic data with multi-users modifications. Also, the performance analysis implies that, in comparison using its relevant schemes, our plan can also be efficient in numerous phases.

We provide security analysis for data confidentiality among the group customers, which is also secure from the collusion attack in the cloud storage server and revoked group customers.

We provide framework in our public integrity auditing for shared dynamic cloud data with secure group user revocation is offered.

Author Profile

Author Photo

P.Ayeesha Khan received the B.Tech degrees in Computer Science and Engineering from Vignana Bharathi Institute of Technology in 2009 and 2013. She now M.Tech in Computer Science and Engineering in Madanapalle Institute of Technology and Science.