IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 6, June 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106066 |

User Revocation in Identity-Based Cloud Storage using Third Party Auditor

Apoorva Shrivastav[1], Prof. Ashish Gupta[2]

Research Scholar, Department of Computer Science & Engineering, NITM, Gwalior, India[1]

Assistant Professor, Department of Computer Science & Engineering, NITM, Gwalior, India[2]

ABSTRACT: As cloud provides various services number of user stores their data on cloud. Integrity of cloud data is important as number of user shared data on cloud. User revocation is common in such schemes, as user's membership changes for variety of purpose. Previously, user revocation overhead in such schemes was related with the overall different file blocks occupied by a revoked user. Remote information integrity checking permits an information storage server, says a cloud server, to control a character that it's really storing owner's data honestly. Up till now, various Remote information integrity checking protocols are planned, however most of the concept suffer from the difficulty of a fancy key organization, that is, they rely on the expensive public key infrastructure which could hamper the preparation of Remote information integrity checking in observe. This project, have a tendency to propose a replacement construction of identity-based (ID-based) Remote information integrity checking protocol by creating use of key- homomorphic cryptanalytic primitive to remove the system complexness and also the value for establishing and managing the general public key authentication framework

KEYWORDS: Cloud computing; cloud storage auditing; identity based cryptography, user revocation;

I. INTRODUCTION

Data sharing is the important service in the cloud. In data sharing service user share the data with group of user. User does not have physical control when the data is in cloud. Any mistake can cause loss of data. To check integrity of data some scheme is used, when user cheat or leaves the group, the user should be revoked from group. Therefore user revocation is important in cloud storage. The cloud data owner uses his private key to generate signature for file blocks. When user is removed the user private key should also be removed .In previous scheme all signatures generated should get transfer to non-revoked user. In such case the non-revoked user download all revoked user block resign and upload new one. This cause lots of computation of resources. Once user is removed from group, there is lots of burden of user revocation for large cloud. The situation will be more difficult when membership changes frequently. Therefore to design efficient user revocation is important

II. INTRODUCTION OF GENERAL TERMS

1. **Group user:** There are multiple cluster users in an exceedingly cluster. every cluster user will share informationwith others through the cloud storage. cluster users will be a part of or leave the cluster. The legal cluster users area unit honest and can not leak any non-public info to others.

2. **Group manager:** The group manager may be a powerful entity. It is viewed as Associate in Nursing administrator of the group. once a user leaves the cluster, the manager is to blame of revoking this user. The revoked user cannot transfer information to the cloud any longer.

3. **Cloud:** The cloud provides huge storage space and computing resources for group users. Through the cloud storage, group users will get pleasure from the info sharing service.

4. **TPA:** The TPA is responsible for auditing the integrity of cloud information on behalf of group users. once the TPA needs to audit the info integrity, it'll send an auditing challenge to the cloud. once receiving the auditing challenge, the

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106066 |

cloud can reply to the TPA with an indication of information possession. Finally, the TPA can verify the info integrity by checking the correctness of the proof. The TPA may be a powerful party and it's honest.

III. GOALS AND OBJECTIVES

1. Correctness and Soundness:

Cloud should be able to pass the challenge from TPA and cloud, user and manger should be honest. If it cannot pass the data securely means it does not store data securely.

2. Securely revoking User:

User revocation should be done securely. The removed user should not be able to upload data.

IV. RESEARCH METHODOLOGY

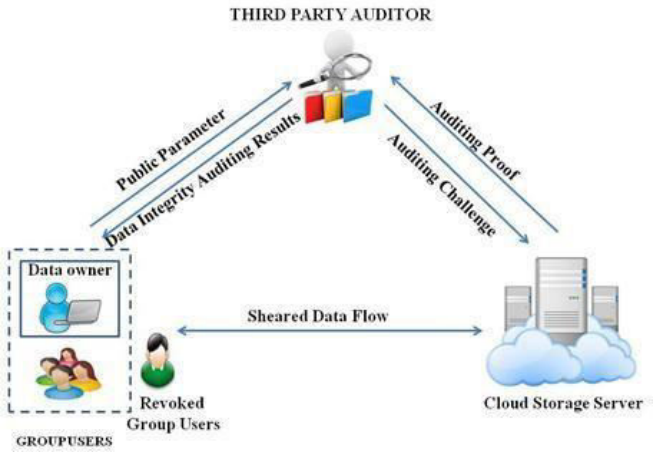


Figure1: System Architecture

1. Description:

This paper construct cloud storage auditing scheme for shared data with efficient user revocation .For efficient user revocation efficient key generation strategy is used .in this instead of public key group identity information is used which remain constant throughout the process Group key consist of two component one remain fixed and other change with user revocation. When user are removed from group all non-revoked user update their private key by this method by still making cloud storage in workable condition. In addition removed user will not be able to upload data to cloud anymore. The signature generated before user revocation does not require to recomputed. It is based on identity based cryptography which removes the complicated certificate management.

2. Algorithms

1. Authenticator generation Algorithm

- It is executed by group user
- Group user generates authenticators for each block of file F.
- It takes input as a file F, number user revocation and user private key and produce file tag
- The group user upload the file along with the file tag.
- Cloud check the correctness of file tag.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106066 |

2. Proof generation algorithm

- Execute by the cloud.
- Takes input as File authenticators and auditing challenge and produce proof P which is used to prove cloud accurately storing file.

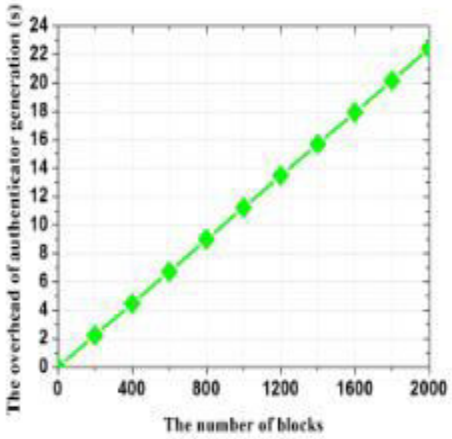
3. Verification algorithm

- Execute by TPA.
- Takes input as proof P and verifies from cloud.
- TPA retrieves the file tag and verifies the validity of by checking valid signature.

3.3.3 User revocation algorithm

- Execute by group manager and non-revokeduser.
- It increment the user revocation count.
- Group manager generate new partial key send to non-revoked user and compute new private key.
- The revoked user cannot upload new data to cloud anymore.

V. RESULTS AND DISCUSSION



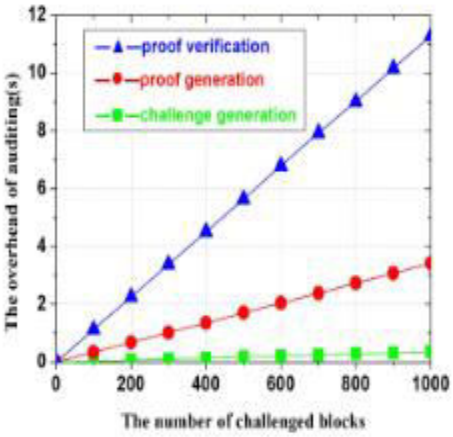


Fig 2.Computation overhead of user revocation on cloud side Fig.3 Computation overhead of user revocation at user side

In fig. 2 we compare user revocation on cloud side. In previous scheme the overhead of cloud resigning block is linear with number of revoked user block .As shown in figure 3 to resign 1,000,000 blocks it requires 4500s.In contrast to that proposed scheme does not need any operation.

Fig. 3 shows overhead of user revocation in group user side is associated with resigning key generation of revoked and non-revoked user. In proposed scheme overhead of user revocation comes with the solution of private key generation of non-revoked which only need addition operation.

VI. CONCLUSION

This paper investigated a new primitive referred to as identity-based remote data integrity checking for secure cloud storage. This paper dignified the security model of two vital properties of this primitive, namely, soundness and ideal information privacy. It provided a new construction of this primitive and showed that it achieves soundness and perfect information privacy with efficient user revocation.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106066 |

REFERENCES

[1] D. Kim and K. S. Kim, "Privacy-Preserving Public Auditing for Shared Cloud Data With Secure Group Management," in IEEE Access, vol. 10, pp. 44212-44223, 2022, doi: 10.1109/ACCESS.2022.3169793.
[2] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," In Proc. of IEEE Cloud 2012, pp. 295-302, 2012.
[3] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," In Proc. of International Conference on Applied Cryptography and Network Security, pp.
507-525, 2012.
[4] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao. "Enabling Public Auditing for Shared Data in Cloud Storage Supporting Identity Privacy and Traceability," Journal of Systems and Software, vol. 113, pp. 130-139, 2016.
[5] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu and R Hao, "Light-weight and Privacy-preserving Secure Cloud Auditing Scheme for Group Users via the Third Party Medium," Journal of Network and Computer Applications, vol. 82, pp.56-64, 2017.
[6] B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92-106, 2015.
[7] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726, Aug. 2015.
[8] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient Integrity Auditing for Shared Data in the Cloud with Secure User Revocation," IEEE Trustcom/BigDataSE/ISPA, pp. 434-442, 2015.
[9] Goran Candrli ˇ C, "How Much Is Stored in the Cloud?", ´ online at http://www.globaldots.com/how-much-is-storedin-the-cloud/.
[10] 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 2007, pp. 598- 610, 2007.
[11] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of Retrievability for Large Files," In Proc. of 14th ACM conference on Computer and communications security, pp. 584-597, 2007.
[12] H. Shacham and B. Waters, "Compact Proofs of Retrievability," In Proc. of ASIACRYPT 2008, pp. 90-107, 2008.
[13] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," In Proc. of 4th international conference on Security and privacy in communication netowrks, pp. 1-10, 2008.
[14] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol.22,no.5, pp. 847-859, 2011.
[15] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 409-428, 2013.
[16] D. Cash, A. Kupc¸ ¨ u, and D. Wichs, "Dynamic Proofs of ¨ Retrievability via Oblivious Ram," In Proc. 32nd Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT 13), pp. 279-295, 2013.
[17] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.
[18] M. Sookhak, A. Gania, M. K. Khanb, and R. Buyyac, "Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing," Information Science, vol. 380, pp. 101-116, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details