Reliable TPA for Auditing Users Data Stored in Cloud

D.S. Jyothi*1, and K. Venkata Ramaiah#2

[1]P.G. Student, Dept. of CSE, Chebrolu Engineering college, chebrolu, Guntur.dt,AP, India

[2]HOD, Dept. of CSE, Chebrolu Engineering college, chebrolu, Guntur.dt,AP, India

Abstract— Cloud means collection of storage servers maintained by the cloud service provider which minimizes investment cost for individual users and organizations. It providing on-demand self service, resource pooling, rapid elasticity and measured service. But users are worrying about their data stored in untrusted cloud servers. For that introducing third-party auditor along with privacy preserving public auditing technique which audit, verifies and provides privacy of user's data in cloud.

I. INTRODUCTION

Cloud storage denotes a family of increasingly popular on-line services for archiving, backup, and even primary storage of files. Amazon S3 is a well known example. Cloud-storage providers offer users clean and simple file-system interfaces, abstracting away the complexities of direct hardware management. As a standalone tool for testing file retrievability against a single server, though, a POR is of limited value.1 Detecting that a file is corrupted is not helpful if the file is irretrievable and thus the client has no recourse. Thus PORs are mainly useful in environments where F is distributed across multiple systems, such as independent storage services. A POR uses file redundancy within a server for verification. In a second, complementary approach, researchers have proposed distributed protocols that rely on queries across servers to check file availability.

Strong file-intactness assurance:

HAIL enables a set of servers to prove to a client via a challenge-response protocol that a stored file F is fully intact—more precisely, that the client can recover F with overwhelming probability.

Low overhead:

The per-server computation and bandwidth required for HAIL is comparable to that of previously proposed PORs. Apart from its use of a natural file sharing across servers, HAIL improves on PORs by eliminating check values and reducing within-server file expansion.

Strong adversarial model:

HAIL protects against an adversary that is active, i.e., can corrupt servers and alter file blocks and mobile, i.e., can corrupt every server over time.

II. RELATED WORK

Ateniese et al. [1] are the first to consider public auditability in their "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphic linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file. However, among their two proposed schemes, the one with public auditability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor. Juels et al. [2] describe a "proof of retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Later, Bowers et al. [3] propose an improved framework for POR protocols that generalizes Juels' work. Dodis et al. [4] also give a study on different variants of PoR with private auditability. Shacham and Waters [5] design an improved PoR scheme built from BLS signatures [6] with proofs of security in the security model defined in [7]. Similar to the construction in [8], they use publicly verifiable homomorphic linear authenticators that are built from provably secure BLS signatures. Based on the elegant BLS construction, a compact and public verifiable scheme is obtained.

In other related work, Sebe et al. [9] thoroughly study a set of requirements which ought to be satisfied for a remote data possession checking protocol to be of practical use. Their proposed protocol supports unlimited times of file integrity verifications and allows preset tradeoff between the protocol running time and the local storage burden at the user.

III. EXISTING SYSTEM

The existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public auditability and data dynamics has not been fully addressed.

How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud Computing.

Existing System disadvantages:

- Csp hide data loss incidents to maintain a reputation.
- It does not immediately offer any guarantee on data integrity and availability.
- Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.
- Simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network.
- It is often insufficient to detect the data corruption.

IV. PROPOSED SYSTEM

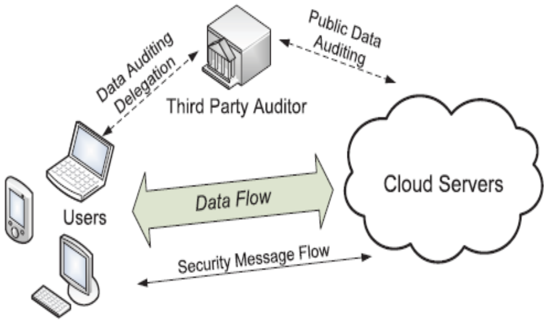
We motivate the public auditing system of data storage security in cloud computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content.

To the best of our knowledge, our scheme is the first to support scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.

Proposed System advantages:

- Users may resort to an independent third-party auditor to audit the outsourced data .
- TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users.
- TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform.
- Our scheme enables an external auditor to audit user's cloud data without learning the data content.

V. SYSTEM ARCHITECTURE



VI. MODULES

Cloud user:

Who has large amount of data files to be stored in the cloud. Before storing the data into cloud user should be registered.

Third party auditor:

To allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users

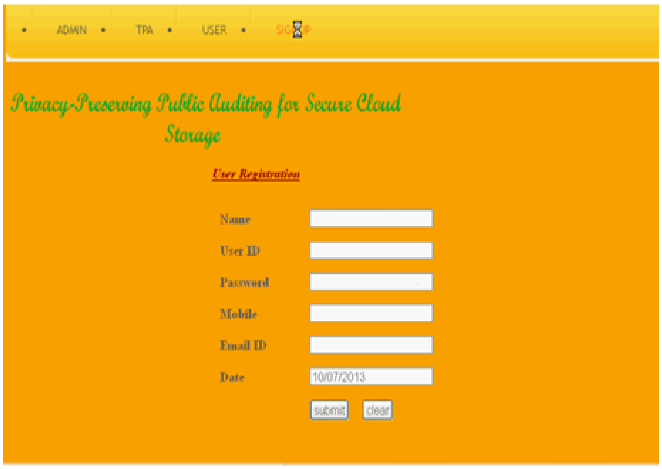
Cloud service provider: To provide data storage service and has significant storage space and computation resources.

VII. ALGORITHM

- The user blinds each file block data before file distribution k is the secret key for data vector is generated.
- Based on the blinded data vector, the User generates k parity vector via the secret matrix P.
- The user calculates the ith token for server j.
- The user sends the token secret matrix P, permutation and challenge key Kmaster key, and kchal to TPA for auditing delegation.

The blinding values in the servers are not taken by TPA response of the server are verified directly. As TPA does not know the secret blinding key there is no way for TPA to learn the data content information during auditing process. Thus the privacy-preserving third party auditing is achieved.

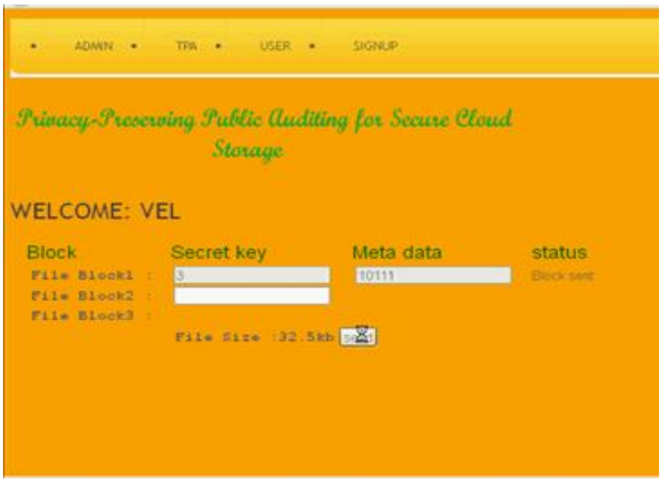
VIII. EXPERIMENTAL RESULTS



Privacy-Preserving Public Auditing for Secure Cloud Storage

User Registration

Name
User ID
Password
Mobile
Email ID
Date 10/07/2013



Privacy-Preserving Public Auditing for Secure Cloud Storage

WELCOME: VEL

Block	Secret key	Meta data	status
File Block1 :	3	10111	Block sent
File Block2 :			
File Block3 :			

File Size :32.5kb

IX. CONCLUSION

We propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

X. FUTURE WORK

Future research on for data recovery proposing when users data lost by the cloud server.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.

[2] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

[3] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 2009.

[4] Y. Dodis, S.P. Vadhan, and D. Wichs, "Proofs of Retrievability via Hardness Amplification," Proc. Theory of Cryptography Conf. Theory of Cryptography (TCC), pp. 109-127, 2009.

[5] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.

[6] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.

[7] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[9] F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

AUTHOR'S DETAIL:

MRS D.S.JYOTHI is a student of Chebrollu Engineering Collage of chebrollu. Presently she is pursuing her M.Tech computer science engineering from this collage and she received her B.Tech from Sri Saradhi Institute of Engineering and Technology Nuzvid affiliated to JNT University Kakinada in year 2006.Her area of interest includes computer networks and object oriented programming languages all current trends and techniques in computer science.

Mr.K.VenkataRamaiah, an excellent teacher Received M.Tech (CSE) from Bharath university and is working as Associate Professor and HOD, Department of MCA, M.Tech Computer science engineering, Chebrolu College of Engineering & Technology. He has 11 years of teaching experience in various engineering colleges. His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.