

# Privacy Preserving Public Auditing for Shared Data in the Cloud using Hashing Algorithm

Ramnath Banerjee<sup>1</sup>, Abhishek Pawar<sup>2</sup>, Vishal Patil<sup>3</sup> & Pushparaj Nimbalkar<sup>4</sup>

<sup>1</sup>Assistant Professor, <sup>2,3,4</sup>BE Students  
<sup>1,2,3,4</sup>Computer Engineering, DYPIET, Ambi

---

**Abstract:** With distributed storage administrations, it is normal for information to be put away in the cloud, as well as shared over numerous clients. Be that as it may, open inspecting for such shared information — while protecting personality security — stays to be an open test. In this paper, we propose the first security safeguarding instrument that permits open calculating on shared information put away in the cloud. Specifically, we abuse Hashing Mechanism to figure the verification data expected to review the honesty of shared information. With the component, the character of the surety on every square in shared information is kept private from an outsider reviewer (TPA), who is still ready to openly confirm the honesty of shared information without retrieving the whole file. Our exploratory results exhibit the viability and efficiency of our proposed component when reviewing shared data.

**Keywords:** Public auditing, privacy-preserving, shared data, cloud computing

## 1. INTRODUCTION

All Cloud administration suppliers deal with a venture class framework that offers a scale-capable, secure and solid environment for clients, at a much lower peripheral expense because of the sharing way of assets. It is ordinary for clients to utilize distributed storage administrations to transmit information to others in a group, as information sharing turns into a general element in most appropriated storage offerings, including Drop box and Google Docs. The uprightness of information in distributed storage, be that as it may, is liable to doubt and investigation, as information put away in an untrusted cloud can without much of a stretch be lost or ruined, because of equipment disappointments and human mistakes. To secure the honesty of cloud information, it is best to perform open au-introducing so as to diting an outsider evaluator (TPA), who offers its examining administration with more intense calculation and correspondence capacities than standard clients. The 1st provable information ownership (PDP) component to perform open inspecting is intended

to check the accuracy of information put away in an untrusted server, without recovering the whole information. Propelling a stage, Wang et al. (alluded to as WWRL) is intended to build an open inspecting instrument for cloud information, so that amid open reviewing, the substance of private information having a place with an individual client is not revealed to the outsider evaluator. We trust that sharing information among various clients is maybe a standout amongst the most captivating elements that spurs distributed storage. An one of a kind issue presented amid the procedure of open reviewing for shared information in the cloud is the way to safeguard personality protection from the TPA, on the grounds that the characters of underwriters on shared information might demonstrate that a specific client in the gathering or an extraordinary square in shared information is a higher significant focus than others. For instance, Alice and Bob cooperate as a gathering and share a le in the cloud. The common le is partitioned into various little pieces, which are autonomously marked by clients. Once a square in this mutual le is modified by a client, this client needs to sign the new piece utilizing her open/private key pair. The TPA needs to know the character of the underwriter on every piece in this common le, with the goal that it can review the uprightness of the entire le taking into account demands from Alice or Bob. We propose another protection safeguarding open examining instrument for shared information in an uncertainty cloud. The use Hashing algorithm for preserving up User Privacy and also checking information Integrity of shared data .In expansion, we promote extend our instrument to backing clump evaluating, which can review various shared information at the same time in a solitary examining errand. In the interim, this mechanism keeps on utilizing arbitrary veiling to bolster information security amid open reviewing, and influence file hash tables to bolster completely dynamic operations on shared information. A dynamic operation demonstrates a supplement, erase or overhaul operation on a solitary square in shared information. An abnormal state examination in the middle of hashing and existing instruments

in the writing is appeared. To our best learning, this speaks to the rest endeavor towards planning a compelling protection saving open reviewing instrument for shared information in the cloud.

## 2. LITERATURE REVIEW

[1] In 2007 G. Ateniese, R. Blaze, R. Urtmola, J. Herring, L. Kissner, Z. Peterson, and D. Melody, dealt with "Provable Data Possession at Untrusted Stores" This paper clarifies about Provable information ownership (PDP) plan which permits a verifier to check the accuracy of a customer's information put away at an untrusted server by using RSA-based homomorphic authenticators including inspecting systems. The benefit of this plan is the verifier can openly review the uprightness of information without recovering the whole information, which is intimate to as open inspecting. Downside: This instrument is suitable for examining the trustworthiness of individual information.

[2] In 2009 C. Wang, Q. Wang, K. Ren, and W. Lou, took a shot at "Guaranteeing Data Storage Security in Cloud Computing" This technique use utilized homomorphic tokens to guarantee the accuracy of eradication codes-construct information conveyed with respect to numerous servers. The significant commitment of this component is capable bolster dynamic information, distinguish got into mischief servers. Downside: The spillage of personality security to open verifiers.

[3][4] In 2010 ,B. Chen, R. Curtmola, G. Ateniese, and R. Smolders, hacked away at "Remote Data Checking for Network Coding-Based Distributed Storage Systems" This paper presented a component for reviewing the rightness of information under the multi-server situation, where these information are encoded by system coding as opposed to utilizing deletion codes. This plan minimizes correspondence overhead in the period of information repair. Disadvantage: This plan requires two enhanced plans. The principal plan is BLS marks, and the second one pseudo-arbitrary capacity.

[5][7] In 2007 A. Juels and B.S. Kaliski, chipped away at "PORs: Proofs of Retrievability for Large Files" .This paper give POR's plan which is additionally ready to check the accuracy of information on an untrusted server. The first document is included with an arrangement of haphazardly esteemed check squares called sentinels. The verifier difficulties the untrusted server by determining the positions of a association

of sentinels and requesting that the untrusted server give back the related sentinel values. Sentinel Based POR convention is amiable to certifiable application. Disadvantage: Only concentrate on individual information in the cloud. Integrity Threats: First, an enemy might attempt to degenerate the uprightness of shared information. Second, the cloud administration supplier might incidentally degenerate (or even uproot) information in its stockpiling because of equipment obstacle and human blunders. Aggravating matters, the cloud administration supplier is monetarily spurred, which implies it might be unwilling to advise clients about such defilement of information. Privacy Threats: The character of the underwriter on every piece in shared information is private.

## 3. RELATED WORK

displayed an effective PDP component taking into account symmetric keys. This instrument can bolster upgrade and erase operations on information; be that as it may, embed operations are not accessible in this component. It abuses symmetric keys to check the trustworthiness of information, it is not open evident. Downside: This plan gives a client a set number of checks.

rightness of shared information trustworthiness, might attempt to uncover the personality of the endorser on every piece in shared information taking into account confirmation metadata.

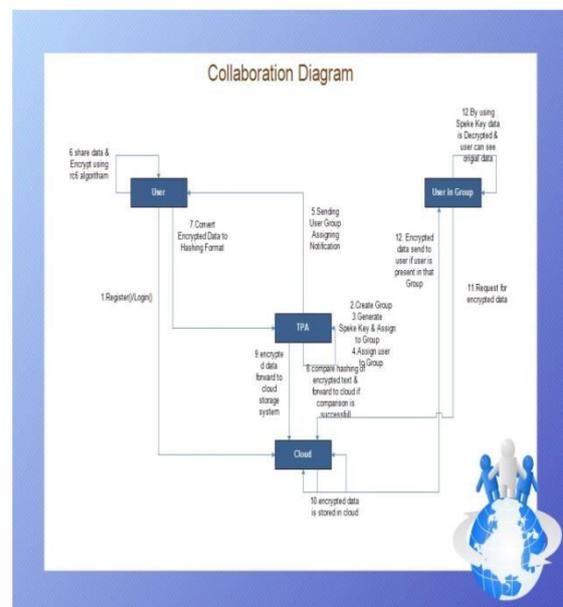
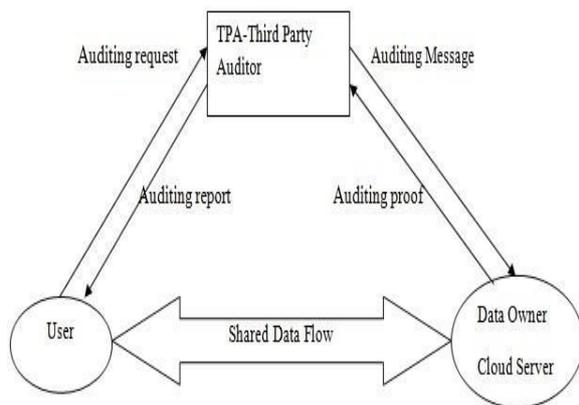


Fig 1: Collaboration diagram

In this paper, a novel privacy preserving open evaluating instrument. All the more particularly, we use ring marks to build homomorphic

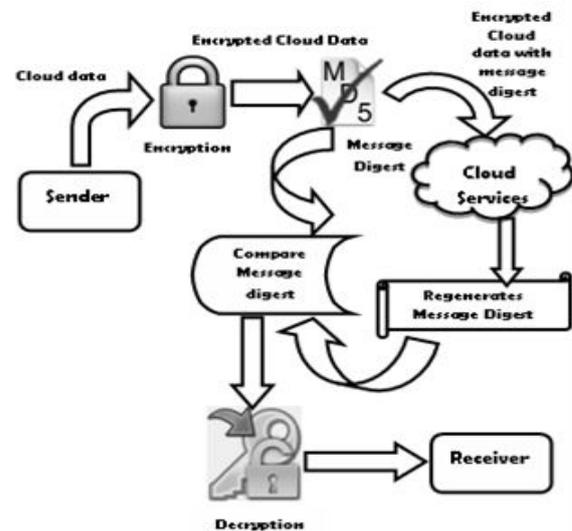
authenticators in hashing, so that an open verifier can confirm the trustworthiness of shared information without recovering the whole information while the personality of the endorser on every piece in shared information is kept private from people in normal verifier. Moreover, we facilitate extend our instrument to backing clump evaluating, which can perform different inspecting assignments at the same time and enhance the productivity of check for numerous examining errands. In the meantime, mechanism is perfect with arbitrary veiling, which has been used in WWRL and can protect information security from open verifiers. Additionally, we likewise influence record hash tables from a past open evaluating answer for bolster dynamic information. An abnormal state correlation among existing instruments is displayed.



System Architecture

The architecture involves three parties: the cloud server, the third party auditor (TPA) and client. There are two types of users in a group: the original user and a different number of group users. The original user and group users are both members of the group. Group members are allowed to enter and modify shared data created by the original user based on access control policies. Shared data and its verification information (i.e. signatures) are both stored in the cloud server. The third party auditor is able to authenticate the integrity of shared data in the cloud server on behalf of group members. Our system model includes the cloud server, the third party auditor and client. The user is responsible for deciding who is able to share her data before outsourcing data to the cloud. When a user make choices to check the integrity of shared data, she first sends an analyzing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud server, and fetch an auditing proof of shared data from the cloud server. Then the TPA

verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.



The distributed computing model for conveying processing administrations offers less costly access to an assortment of institutionalized administrations from different suppliers. Yet, in the wake of outsourcing a support of the cloud, the proprietor no more controls the stage on which the administration runs. The client will undoubtedly believe the Cloud Service Provider for Accuracy, Privacy, and Integrity of its information and calculations. Cryptographic components can lessen such trust by permitting the client to ensure its information and calculations, and also to confirm parts of remote calculation [11]. Likewise with other facilitated administrations, information assurance is an issue when considering distributed computing. The principle information insurance dangers to the cloud information are loss of information by outsider administration suppliers, unapproved access to the cloud information, vindictive exercises focusing on Cloud Service Provider and poor inside IT security bargaining information assurance. Some time recently presenting a distributed computing framework, a danger evaluation of these risks and their potential effect on the information ought to be done [12]. Abnormal amounts of information assurance are important for cloud applications, and the related efforts to establish safety must be taken to ensure the private information on the cloud from these risks. This paper addresses the accompanying ranges of dangers in distributed computing:

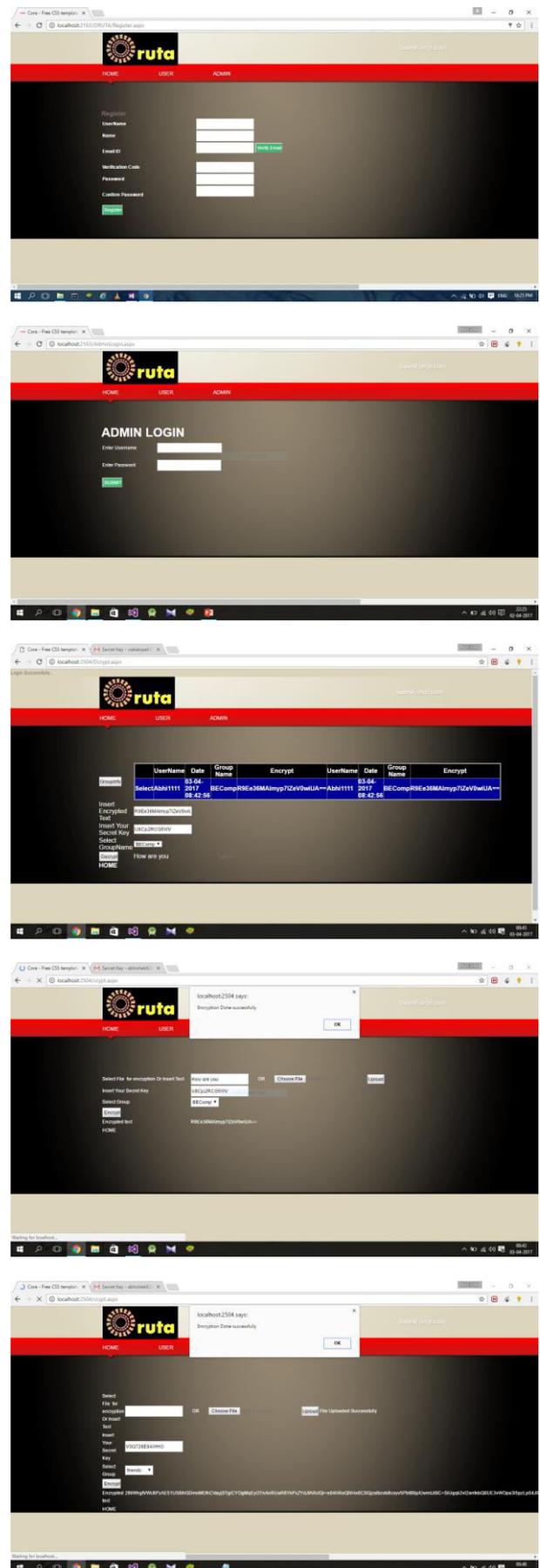
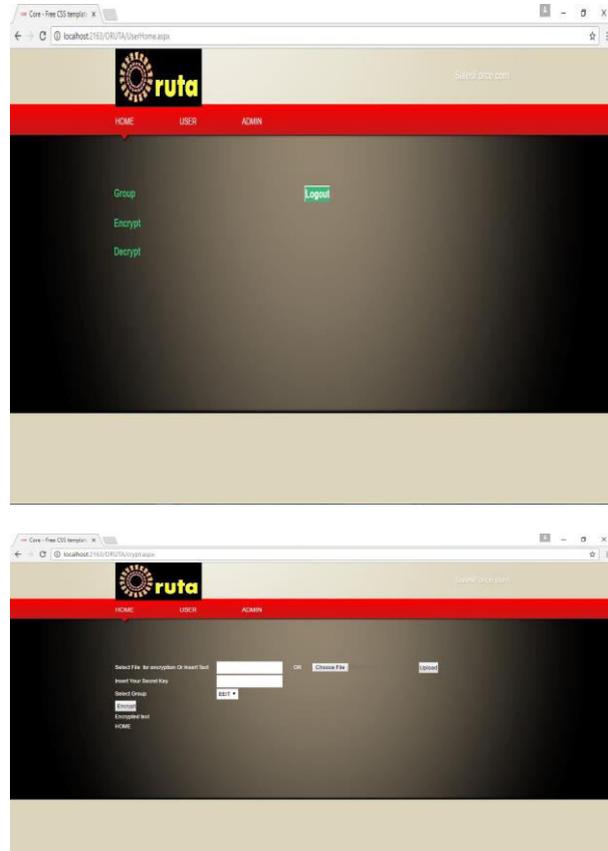
- 1) Secure stockpiling of information in the cloud environment
  - 2) Protecting information from unapproved access
- Fig.2 clarifies the methodology which depends on unbalanced cryptography and

the message digest. The information put away in the cloud might at first be scrambled utilizing a hilter-kilter cryptographic calculation like RSA to deliver a figure content and afterward a message summary is been created for that figure content utilizing MD5 Algorithm. At whatever point the customer get to the information put away in the cloud, the message overview is been recovered utilizing the same hash capacity to check the accuracy of information in the cloud. On the off chance that the rightness is accomplished, then the figure content is unscrambled to get the first plaintext or information beforehand put away.

#### 4. CONCLUSION

The privacy preserving public auditing mechanism for shared data in the cloud. The utilization Hashing Algorithm so the TPA is able to analyze the integrity of shared data. To improve the efficiency of verification for multiple auditing tasks, for further enhance our mechanism to support batch auditing. An interesting problem in our future work is how to efficiently to analyze the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

#### 5. RESULT



## 6. REFERENCES

- [1] 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.
- [2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 598–610.
- [3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 525–533.
- [4] R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer-Verlag, 2001, pp. 552–565.
- [5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer-Verlag, 2003, pp. 416–432.
- [6] H. Shacham and B. Waters, "Compact Proofs of Retrievability," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer-Verlag, 2008, pp. 90–107.
- [7] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds," in *Proc. ACM Symposium on Applied Computing (SAC)*, 2011, pp. 1550–1557.
- [8] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 534–542.
- [9] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," in *Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*. Springer-Verlag, 2001, pp. 514–532.
- [10] D. Boneh and D. M. Freeman, "Homomorphic Signatures for Polynomial Functions," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer-Verlag, 2011, pp. 149–168.
- [11] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical Short Signature Batch Verification," in *Proc. RSA Conference, the Cryptographers' Track (CT-RSA)*. Springer-Verlag, 2009, pp. 309–324.
- [12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2006, pp. 89–98.
- [13] A. Juels and B. S. Kaliski, "PORS: Proofs of Retrieval for Large Files," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 584–597.
- [14] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," in *Proc. International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2008.
- [15] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2009, pp. 213–222.
- [16] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," in *Proc. IEEE/ACM International Workshop on Quality of Service (IWQoS)*, 2009, pp. 1–9.
- [17] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-based Distributed Storage Systems," in *Proc. ACM Cloud Computing Security Workshop (CCSW)*, 2010, pp. 31–42.
- [18] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2012.
- [19] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of Ownership in Remote Storage Systems," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2011, pp. 491–500.
- [20] Q. Zheng and S. Xu, "Secure and Efficient Proof of Storage with Deduplication," in *Proc. ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2012.
- [21] M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, "Oblivious Outsourced Storage with Delegation," in *Proc. Financial Cryptography and Data Security Conference (FC)*, 2011, pp. 127–140.
- [22] S. D. C. di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati, "Efficient and Private Access to Outsourced Data,"