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 12, Issue 3, March 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

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: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203097 |

# Cloud Storage with Data Integrity Assurance

**Rexeena X[1], Dhanya R[2]**

Assistant Professor, Department of Computer Application, Bharathamatha College of Arts and Science, Kozhinjampara, Kerala, India[1]

Assistant Professor, Department of Computer Application, Bharathamatha College of Arts and Science, Kozhinjampara, Kerala, India[2]

**ABSTRACT**: The project entitled " DATA INTEGRITY PROOF IN CLOUD COMPUTING" has been envisioned as the de-facto solution to the rising storage costs of IT Enterprises. The high costs of data storage devices and rapid rate at which data is being generated it proves costly for enterprises or individual users to frequently update their hardware. Apart from reduction in storage cost, data outsourcing to the cloud also helps in reducing the maintenance. Cloud storage moves the user's data to large data centres, which are located remotely, on which user does not have any control. The data storage in cloud is much effective way, however this feature of the cloud faces many new security challenges which need to be clearly understood and resolved. Provides a cloud data integrity method for customers to verify that their data is correct in the cloud. This proof of integrity is negotiable both with the cloud and with the customer, and can be included in service level agreements (SLAs).

KEYWORDS: Data integrity, cloud storage.

## I.INTRODUCTION

Here we deal with the problem of implementing a method or algorithm for obtaining a proof of data possession in the cloud sometimes referred to as Proof of irretrievability (POR).Thisproblem tries to investigate and to find a proof that the data stored by a user at a remote data storage in the cloud (called cloud storage archives or simply archives) is not modified by the archive and thereby the integrity of the data is ensured. Thiskinds of proofs are very much helpful in peer-to-peer storage systems, network file systems, long-term archives, web-service object stores, and database systems. Such verification systems prevent the cloud storage archives from modifying the data stored in it without the consent of the data owner by using frequent checks on the storage archives. Such checks must allow the data owner to efficiently, quickly and securely verify that the cloud archive is not cheating the owner. The main aim of this project is to ensure maximum integrity to user's data that they considered to be valuable assets.

## II.RELATED WORK

The verification of remotely stored data has recently attracted a lot of growing interest [2]–[4]. For the first time, Ateniese et al"provable .'s data possession" (PDP) methodology for confirming file ownership takes public auditability into account on unreliable storage. They achieve public auditability with their system by using RSA-based homomorphic tags for auditing outsourced data. Ateniese et al. do not take into account the scenario of dynamic data storage, and extending their plan directly from the static data storage case to the dynamic case may have design and security issues. Ateniese et al. suggest a dynamic variation of the earlier PDP method in their following work. The system sets an a priori limit on the amount of queries, however, and it only supports very basic block operations with extremely limited capability. Block insertions thus cannot be supported.

## III.METHODOLOGY

The algorithm automatically generates security key without user interaction that contains only text regions to be imprinted. Here the client has to register with the cloud to get access to cloud storage. The client can sign in only by entering a security key sent to mail to view his home page. If he wants to upload afile, he will be provided with an encryption key and to download the file a key will be generated and forwarded to mail. Only with the key the client can do any operations on cloud storage. Admin and TPA will maintain the client files and ensure data integrity and security.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

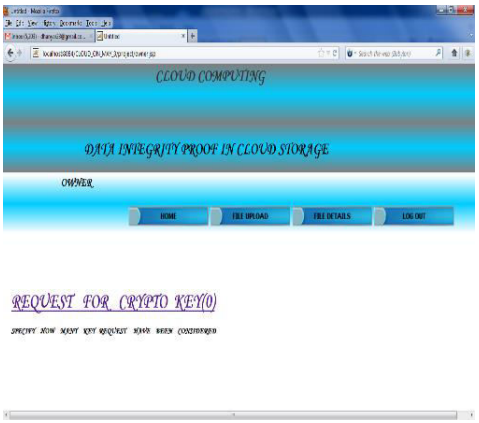
| DOI:10.15680/IJIRSET.2023.1203097 |

## IV. EXPERIMENTAL RESULTS

Fig(a) In home page, data stored remotely can be controlled by admin, TPA or user by signing in to website. The information stored in archive is not modified by anyone as only authorised persons are able to view the information. Before viewing their individual home page they have to sign in separately in main home page. Fig(b) Data outsourcing to cloud server is becoming more popular among many people because of economic benefits. The owner of cloud storage will be provided with security key each time he tries to login in. This method ensure security as each time he will be provided with different security key. Fig(c) Verifies files before placing them in archive and add some metadata to a file and save it to archive. At the moment verifiers use this metadata to verify the integrity of data. Here the checking of data integrity is done each time file is uploaded and downloaded.


Fig(a) Home Page


Fig(b) Owner Security




Fig(c) Owner Home page

## V. CONCLUSION

"DATA INTEGRITY PROOFS IN CLOUD STORAGE" project have worked to facilitate the client in getting a proof of integrity of the data which he wishes to store in the cloud storage servers with bare minimum costs and efforts. Our method was developed to reduce the computational and storage overhead of both the client and cloud storage server. At the client we only store two functions, the key generator function g, and the function h which is used for encrypting the data. Hence the data storage at the client is very much minimal and this scheme proves advantageous to thin clients like PDAs and mobile phones.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203097 |

## REFERENCES

[1] CongWang ;Chow,S.S.M. ; QianWang ; KuiRen ;WenjingLou "Privacy_preserving Public Auditing for Secure CloudStorage", IEEE Transactions on Computers Volume: 62, Issue: 2 2013 ,PP no : 362–375

[2] 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.

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

[4] 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, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009- 28, Univ. of California, Berkeley, Feb. 2009.

[5] R. Sravan kumar and Saxena ,"Data integrity proofs in cloud storage" in IEEE 2011.

[6] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," Trans. Storage, vol. 2, no. 2, pp. 107–138, 2006.

[7] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in SP '00: Proceedings of the 2000 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2000, p. 44.

[8] A. Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS '07: Proceedings of the 14th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2007, pp.584–597.

[9] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS"07: Proceedings of the 14th ACM conference on Computer and communications security.

[10] H. Shacham and B. Waters, "Compact Proofs of Retrievability," In Proceedings.of Asiacrypt "08, Dec. 2008.

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