



A FRAMEWORK FOR AUTHENTICATING OF NUMEROUS DATA COPIES OVER MISTRUSTFUL CLOUD SERVER

P. Anil Kumar¹, D Murli Krishna Reddy²

*¹Pursuing M.Tech (CSE), ²Working as Assistant Professor (CSE),
Nalanda Institute Of Engineering & Technology (NIET), Kantepudi(V),
Sattenpalli(M), Guntur(D), Andhra Pradesh (India)*

ABSTRACT

For purpose of increasing level of scalability, durability and availability, several clients may need their data to be replicated on several cloud servers. The multiple copies the cloud service provider (CSP) is needed to store, the much payments the clients are charged. Here we propose a pairing-based provable multi-copy data possession (PB-PMDP) scheme, which offers here there are four things we have to consider one is Data Owner, Third party Authorization (TPA), cloud service provider (CSP) and Authorized person. Data owner will simply upload the file it means it simply shared to TPA, then TPA will receive the file and will upload into multiple cloud services providers (CSP) here there multiple cloud server are there for storing the data on it, if any unauthorized user change the original content uploaded by the data owner in cloud database that message is transferred to data owner, then immediately data owner will need to react about the modification of data, here we are proposing the three mechanisms i.e., security of data, data integrity means providing the confidentiality of data if any modifications or changes are happened in the cloud and will know about the capacity data storage. Authorized person will have the permissions like view the files which are uploaded by the user, download the files, and update the files etc.,

I. INTRODUCTION

Subcontracting data to a centralized cloud service provider (CSP) permits organizations to store large data on the CSP than on personal systems. Such outsourcing also permits valid users to remotely accessing the data from various geographic locations.

Once the data has been outsourced to a remote CSP, which may not be trustworthy, the data owners lose the direct control over their sensitive data. This lack of control raises new formidable and challenging tasks related to data confidentiality and integrity protection in cloud computing systems. The confidentiality issue can be handled by encrypting sensitive data before outsourcing to remote servers. As for data integrity, the data owners need to have strong evidence that the cloud servers still possess their data and it is not being tampered with or partially deleted over time, especially because the internal operation details of the CSP may not be known to cloud customers. Consequently, many researchers have focused on the problem of provable data possession (PDP) and proposed different schemes to audit the data on remote storage sites.



PDP is a system for accepting information trustworthiness over remote servers. In a run of the mill PDP model, the information proprietor produces some metadata/data for an information record to be utilized later for check purposes through a test reaction convention with the remote/cloud server. Analysts have proposed diverse varieties of PDP plans under distinctive cryptographic suspicions; e.g., see [1]–[7].

PDP plans exhibited in [1]–[7] concentrate on a solitary duplicate of the document and give no evidence that the CSP stores different duplicates of the proprietor's record. More subtle elements and a near investigation of different PDP plans can be found in our specialized report [8]. Curtmola et al. [9] were the first to present a various imitation PDP (MR-PDP) plan that makes numerous duplicates of a proprietor's document and review them. The MR-PDP plan expands information accessibility; a ruined information duplicate can be recreated utilizing copied duplicates on different servers. The collaboration between approved (clients who have the privilege to get to the proprietor's document) and the CSP was not considered in [9]. The MR-PDP plan bolsters private unquestionable status, i.e., just the information proprietor can check information ownership. Open unquestionable status is a key element in remote information checking plans to maintain a strategic distance from debate that may happen between the information proprietor and the CSP. Assigning the reviewing procedure (without uncovering mystery keys) to a trusted outsider for checking the information uprightness can comprehend such quest

Main contributions. Here our contributions can be classified as follows:

- Here we are proposing a new approach called pairing –based provable multi-copy data possession (PB-PMDP) scheme. In this scheme provides as an passable guarantee that the cloud service provider stores all copies that are accepted upon in the service agreement. And these copies are complete. The valid user can faultlessly access the duplicates received from the CSP. The PB-PMDP structure supports community verifiability.
- We legitimize the effectiveness of the proposed PB-PMDP plan through execution examination, exploratory results, and correlation with the MR-PDP model [9]. Also, we talk about a slight alteration of the proposed PB-PMDP plan to distinguish defiled duplicates.
- We demonstrate the security of our plan against conniving servers.

II. OUR SYSTEM AND ASSUMPTIONS

Framework segments. The distributed computing stockpiling model considered in this work comprises of three fundamental parts as outlined in Figure 1: (i) an information proprietor that can be an individual or an association initially having delicate information to be put away in the cloud; (ii) a CSP who oversees cloud servers and gives paid storage room on its framework to store the proprietor's records; and (iii) approved clients — an arrangement of proprietor's customers who have the privilege to get to the remote information.

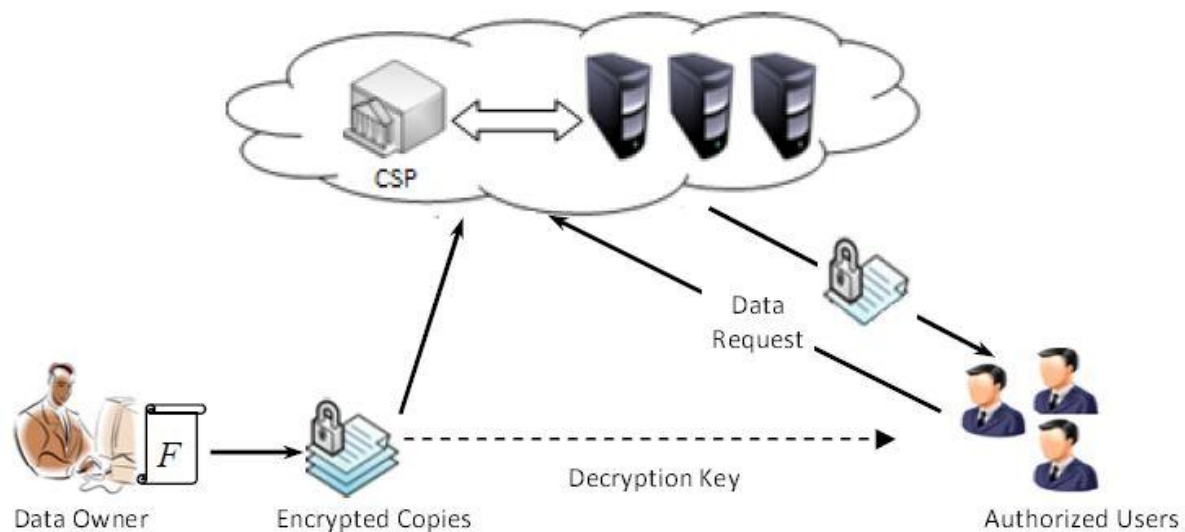


Figure 1: Cloud Computing Data Storage System Model.

The capacity model utilized as a part of this work can be received by numerous handy applications. For instance, in e-wellbeing applications, a trusted government association can be considered as the information proprietor, and the doctors as the approved clients who have the privilege to get to the patients' restorative history put away on cloud servers. In this work, we concentrate on touchy chronicled and warehoused information, which is vital in numerous applications, for example, advanced libraries and galactic/restorative/experimental/lawful vaults. Such information is liable to occasional change, so we regard them as static.

Outsourcing and accessing. The information proprietor has a document F comprising of m pieces and the CSP offers to store n duplicates of the proprietor's record in return for pre-determined charges metered in GB/month.

For information secrecy, the proprietor scrambles his information before outsourcing to the CSP. An approved client of the outsourced information sends an information access solicitation to the CSP and gets a document duplicate in a scrambled structure that can be decoded utilizing a mystery key imparted to the proprietor. The approved client is unconscious of which duplicate has been gotten.

Threat model. The uprightness of clients' information in the cloud may be at danger because of the accompanying reasons. To begin with, the CSP – whose objective is prone to make a benefit and keep up a notoriety – has a motivating force to conceal information misfortune (brought about by episodes like equipment disappointment, administration blunders, noxious assaults) or recover discarding so as to stockpile information that has not been or is seldom gotten to. Second, a deceptive CSP may store less duplicates than what has been settled upon in the administration contact with the data owner.



III. PROPOSED PB-PMDP SCHEME

A. Overview and Rationale

Generating unique differentiable copies of the data file is the core to design a multi-copy provable data possession scheme. Identical data copies enable the CSP to simply deceive the owner by storing only one copy and pretending that it stores multiple copies. Using a simple yet efficient way, the proposed scheme generates distinct copies utilizing the diffusion property of any secure encryption scheme. There will be an unpredictable complete change in the ciphertext, if there is a single bit change in the plaintext. The interaction between the authorized users and the CSP is considered through this methodology of generating distinct copies, where the former can decrypt and access a file copy received from the CSP without recognizing the copy index. Homomorphic linear authenticators (HLAs) [10], [14],[16] are basic building blocks in the proposed scheme. We utilize the BLS HLAs [10].

Table I: Notation of cryptographic operations

Notation	Description	Notation	Description
\mathcal{H}_G	Hashing to G	\mathcal{H}_{QR_N}	Hashing to QR_N
\mathcal{E}_G	Exponentia. in G	$\mathcal{E}_{\mathbb{Z}_N^*}$	Exponentia. in \mathbb{Z}_N^*
\mathcal{M}_G	Multiplication in G	$\mathcal{M}_{\mathbb{Z}}$	Multiplication in \mathbb{Z}
$\mathcal{M}_{\mathbb{Z}_p}$	Multiplication in \mathbb{Z}_p	$\mathcal{D}_{\mathbb{Z}}$	Division in \mathbb{Z}
$\mathcal{A}_{\mathbb{Z}_p}$	Addition in \mathbb{Z}_p	$\mathcal{A}_{\mathbb{Z}}$	Addition in \mathbb{Z}
\mathcal{P}	Bilinear pairing	\mathcal{E}_K	Encryption using K
\mathcal{R}	Random-number generation		

IV. PERFORMANCE ANALYSIS AND EXPERIMENTAL RESULTS

The record F utilized as a part of our execution examination and exploratory results is of size 64MB partitioned in squares of 4KB. Without loss of sweeping statement, we accept that the coveted security level is 80-bit. Along these lines, we use an elliptic bend characterized over Galois field $GF(p)$ with $|p| = 160$ bits (a point on this bend can be spoke to by 161 bits utilizing packed representation [18]), and the measure of the RSA modulus N is 1024 bits.

4.1. Performance Analysis

The computation cost for the MR-PDP and PB-PMDP schemes is estimated in terms of the used cryptographic operations, which are notated in Table I. G indicates a group of points over a suitable elliptic curve in the bilinear pairing, and QR_N is the set of quadratic residues modulo N .

To perform a reasonable examination between our plan and the MR-PDP plan [9], we expect two little adjustments to the first MR-PDP model exhibited in [9]. To start with, we accept that the squares' files being tested are the same over all duplicates (this supposition is a streamlining for the confirmation calculations of [9]). Second, for the CSP to demonstrate the pieces' ownership (not simply just their whole), every square being tested ought to be increased by an arbitrary worth.

Let n , m , and s mean the quantity of duplicates, the quantity of pieces per duplicate, and the quantity of areas per square, separately. Let c indicates the quantity of pieces to be tested, and $|F|$ signifies the record's extent



duplicate. Let the keys utilized with $_$ and be of size 128 bits. Table II displays a hypothetical examination for the setup, stockpiling, correspondence, and calculation expenses of the two plans.

Table II: Storage, correspondence, and calculation costs for MR-PDP and PB-PMDDP plans. The images utilized as a part of the correlation is characterized in Table I. y There are an improvement for this reaction to be $1024 + 160n$ bits utilizing hashing.

		MR-PDP [9]	PB-PMDDP
System Setup	Copies Generation	$E_K + nmR + nmA_Z$	nE_K
	Tags Generation	$2m\mathcal{E}_{Z_N^*} + m\mathcal{M}_Z + m\mathcal{H}_{QR_N}$	$(s+1)nm\mathcal{E}_G + (ns+n-1)m\mathcal{M}_G + nm\mathcal{H}_G$
Storage	File Copies	$n F $	$n F $
	CSP Overhead	1024m bits	161m bits
Communication Cost	Challenge	1280 + $\log_2(c)$ bits	256 + $\log_2(c)$ bits
	Response	1024(n+1) bits †	161 + 160ns bits
Computation Cost	Proof	$(c+n)\mathcal{E}_{Z_N^*} + (cn+c-1)\mathcal{M}_Z + (c-1)nA_Z$	$c\mathcal{E}_G + (c-1)\mathcal{M}_G + csn\mathcal{M}_{Z_p} + (c-1)snA_{Z_p}$
	Verification	$(2n+c+1)\mathcal{E}_{Z_N^*} + (cn+c+n-1)\mathcal{M}_Z + (c-1)nA_Z + c\mathcal{H}_{QR_N} + \mathcal{D}_Z$	$2\mathcal{P} + (c+s+1)\mathcal{E}_G + (c+s-1)\mathcal{M}_G + (n-1)sA_{Z_p} + c\mathcal{H}_G$

V. CONCLUSION

Here We have proposed a BP-PMDDP scheme. The communication between the valid users and the CSP is careful in our system. Furthermore, the proposed system supports public verifiability, and permits limitless number of checking. Safety examination is given in [8]. Through performance examination, experimental outcomes, and contrast with the MR-PDP model, we have defensible the competence of the future scheme. The confirmation time of PB-PMDDP is almost independent of the more number of file reproductions. In this proposed scheme is to identify the corrupted copies, and provide the data integrity.



REFERENCES

- [1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in CCS '07, 2007, pp. 598–609.
- [2] K. Zeng, "Publicly verifiable remote data integrity," in Proceedings of the 10th Int. Conference on Information and Communications Security, ser. ICICS '08, 2008, pp. 419–434.
- [3] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in 6th Working Conference on Integrity and Internal Control in Information Systems (IICIS), 2003, pp. 1–11.
- [4] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," Cryptology ePrint Archive, Report 2006/150, 2006.
- [5] F. Seb e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. and Data Eng., vol. 20, no. 8, 2008.
- [6] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
- [7] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," Trans. Storage, vol. 2, no. 2, 2006.



- [8] A. F. Barsoum and M. A. Hasan, "Provable possession and replication of data over cloud servers," Centre For Applied Cryptographic Research (CACR), University of Waterloo, Report 2010/32, 2010.
- [9] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MRPDP:multiple-replica provable data possession," in 28th IEEE ICDCS, 2008, pp. 411–420.
- [10] H. Shacham and B. Waters, "Compact proofs of retrievability," Cryptology ePrint Archive, Report 2008/073, 2008.
- [11] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07, 2007, pp. 584–597.
- [12] R. Curtmola, O. Khan, and R. Burns, "Robust remote data checking," in StorageSS '08, 2008, pp. 63–68.
- [13] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in CCSW '09, 2009, pp. 43–54.
- [14] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC '09, 2009, pp. 109–127.
- [15] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a highavailability and integrity layer for cloud storage," in CCS '09, 2009, pp. 187–198.
- [16] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in ASIACRYPT '09, 2009, pp. 319–333.

AUTHOR DETAILS

	<p>P. Anil Kumar pursuing M.Tech (CSE) from Nalanda Institute Of Engineering & Technology (NIET), Kantepudi(V), Sattenpalli(M), Guntur(D)-522438, Andhra Pradesh.</p>
	<p>D Murli Krishna Reddy working as Assistant Professor (CSE) from Nalanda Institute Of Engineering & Technology (NIET), Kantepudi(V), Sattenpalli(M), Guntur(D)-522438, Andhra Pradesh.</p>