Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

SECRECY WITH CONFIDENCE AND ABILITY IMPLEMENTING VERIFIABLE STATISTICS CONTROL IN THE CLOUD

Ms. B.Triveni Assistant professor in the department of AI & IT at DVR & DR.HS MIC College of Technology (Autonomous), Kanchikacherla, NTR (DT)..

Mr. P.Sasidhar MCA student in the department of IT at DVR&Dr.HS MIC College of Technology, Kanchikacherla, NTR(District

ABSTRACT_A secure and adaptable framework is provided by the emerging paradigm of cloud computing for users to store their data and for information buyers to access it via cloud servers. This point of view lowers the stockpiling and maintenance costs for the information owner. Since the data owner no longer has physical access to it or ownership of it, a number of new security risks now exist. A cloud auditing service is necessary as a result. This has grown to be a challenging issue in terms of ensuring the security of the data while confirming its ownership. To address these issues, we provide a secure and practical method of preserving verifiable information ownership.We also expand SEPDP to support various data owners, dynamic data, and clump verification. The reviewer can validate the existence of data with little financial outlay when using this scheme, which is its most appealing aspect.

1.INTRODUCTION

Because it requires less initial infrastructure setup, less maintenance work, and universal data access regardless of location or device, storage-as-a-service has become a viable commercial alternative to local data storage. Although it offers many advantages, including cost savings, accessibility, usability, syncing, and sharing, it also poses a number of security risks because the cloud service provider (CSP) controls the data. To save space and increase its profits, CSP can discard the infrequently used data. However, if it wants to maintain its good name, it can also fabricate data loss and corruption due to hardware or software failure.The availability of data stored in the cloud must therefore be verified [1], [2], and [3]. Data users (DUs) do not have a local copy of the data required by traditional cryptographic solutions for data integrity checking, nor are DUs permitted to download the entire data. Both of these solutions don't seem feasible because the earlier one needs additional storage and the later one raises the cost of file transfers. To solve this problem, a number of schemes, such as [4], [5], [6], and

[7], are put forth that use blockless verification to check the data's integrity without downloading the entire file.These works' ability to be verified by the general public is one of their appealing qualities. With public auditability, DUs can hire a third-party auditor (TPA) to conduct the audit. It possesses the knowledge and skills necessary to persuade both the CSP and the DU. [5], [8]. These schemes employ the provable data possession (PDP) technique, which ensures the possession of data in unreliable cloud storage by randomly verifying a small number of blocks. To enable TPA to verify the integrity of the data stored on the unreliable cloud, a number of schemes [10], [11 have recently been proposed.Each of these plans has advantages and disadvantages. To prevent TPA from inferring data from the cloud server's response during auditing, privacy protection is essential. In any case, the plans proposed in [2], [4] don't accomplish protection safeguarding necessity. The methods proposed in [4] and [5] do not meet the data dynamics requirement, despite the fact that data dynamics is an essential feature that makes it easier for data owners to insert, modify, and delete on a particular block of data without affecting the meta-data of other blocks. In the meantime, schemes like [4], [11],were unable to meet the batch auditing requirement, which guarantees that TPA should be able to handle multiple simultaneous verification requests from various DUs. The purpose of this property is to reduce CSP and TPA's costs of computation and communication. Sadly, the schemes [[12], [13], [14] and make use of pairing-based cryptographic operations, which require more time and require a lot of computation.

2.LITERATURE SURVEY

2.1 Privacy-Preserving Public Auditing for Secure Cloud Storage

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new

vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

2.2 Data Storage Auditing Service in Cloud Computing: Challenges, Methods And Opportunities

Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. The first offered cloud service is moving data into the cloud: data owners let cloud service providers host their data on cloud servers and data consumers can access the data from the cloud servers. This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. In this paper, we investigate this kind of problem and give an extensive survey of storage auditing methods in the literature. First, we give a set of requirements of the auditing protocol for data storage in cloud computing. Then, we introduce some existing auditing schemes and analyze them in terms of security and performance. Finally, some challenging issues are introduced in the design of efficient auditing protocol for data storage in cloud computing

3.PROPOSED SYSTEM

We propose a protected and effective security saving provable information possession scheme (SEPDP) for cloud storage. It works in three stages, to be specific, key age, signature age and evaluating stage. Most appealing element of SEPDP is that it doesn't utilize any serious calculation like matching based task. Further, we stretch out SEPDP to help numerous information proprietors, group examining, and dynamic information activities. A probabilistic investigation to distinguish the respectability of the squares put away at CSP. We assessed the execution of the proposed plan and contrasted and a portion of the current prominent instruments. We see that the absolute time for check completed by TPA in the proposed plan is not as much as that of the current plans. This implies SEPDP is productive and reasonable to execute the confirmation at the low fueled gadgets. Likewise, the casual security demonstrates that the proposed plan can withstand different possibilities assaults against detached and dynamic enemies. To

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

additionally fortify the security, the proposed plan is reproduced for the formal security confirmation utilizing the popular AVISPA apparatus. The reenactment results guarantee that the plan withstands both replay just as man-in- middle attacks. A thorough similar investigation for the correspondence and calculation costs alongside security and usefulness highlights has been performed among the proposed plan and other existing plans. The relative comparative study shows that the performance of the proposed scheme is better than other schemes.

3.1 IMPLEMENTATION

1. Data Provider

In this module, data provider has to register and login. Data owner selects file, encrypt the file and upload with the trapdoor to the cloud server. Data owner can view all file uploaded and audit request. And provide permission to user.

2. Cloud

Cloud will module store all the registered users and the data owners. Also can view all the files uploaded to the cloud, the transactions details.

3. Trusted Authority

In Trusted Authority, when data user requests for the private key for the corresponding file the request will be sent to Trusted Authority for the key generation, an also view audit requests and send response to owner

4. User

User has to first register and then has to login to download the file from the cloud server. User has to request the Private key for Trusted Authority, the file he has to download. And also view list of available file and that can download file by using secret keys.

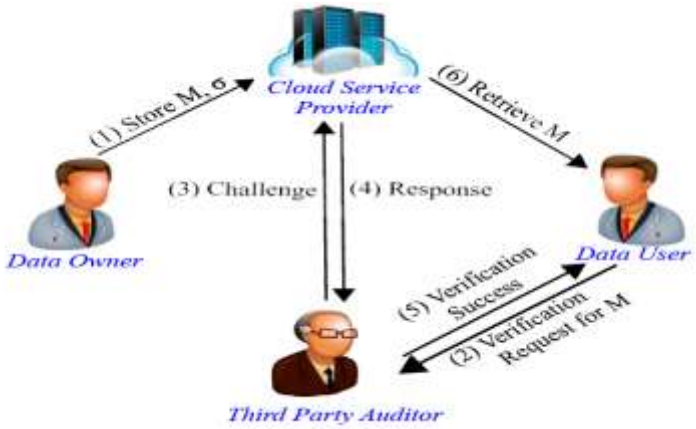

Fig 1:Architecture

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

4.RESULTS AND DISCUSSION

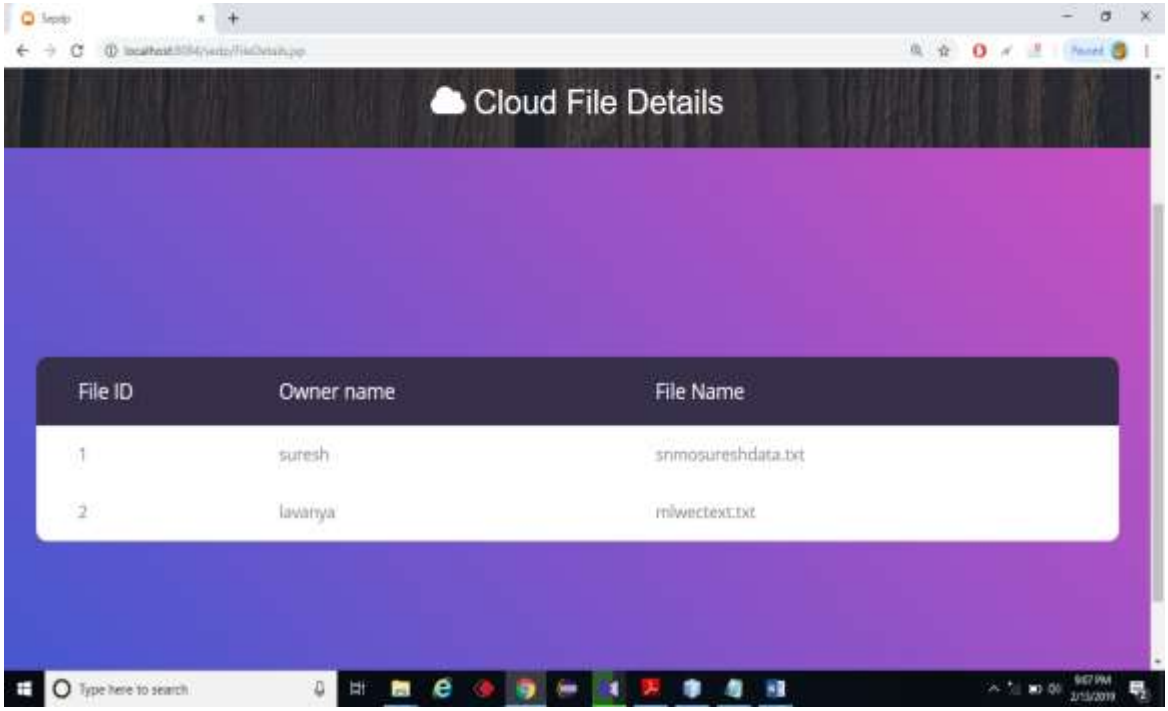

Fig 2:View Cloud Files

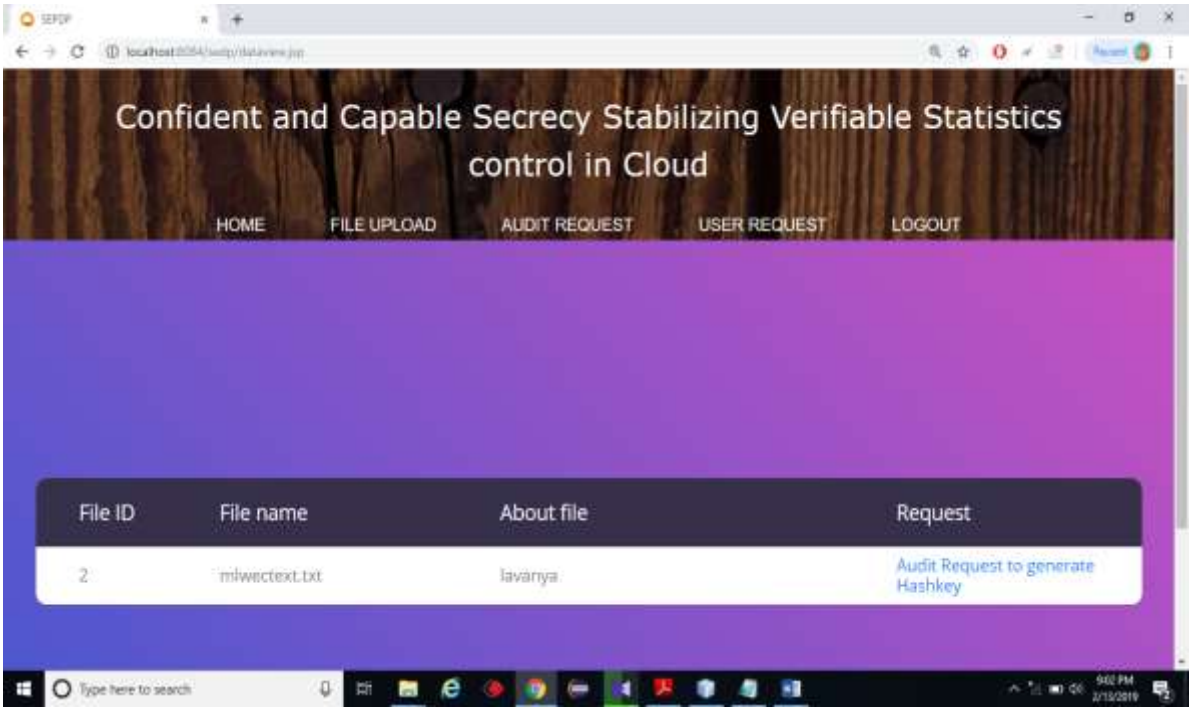

Fig 3:Audit request to generate hashkey

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

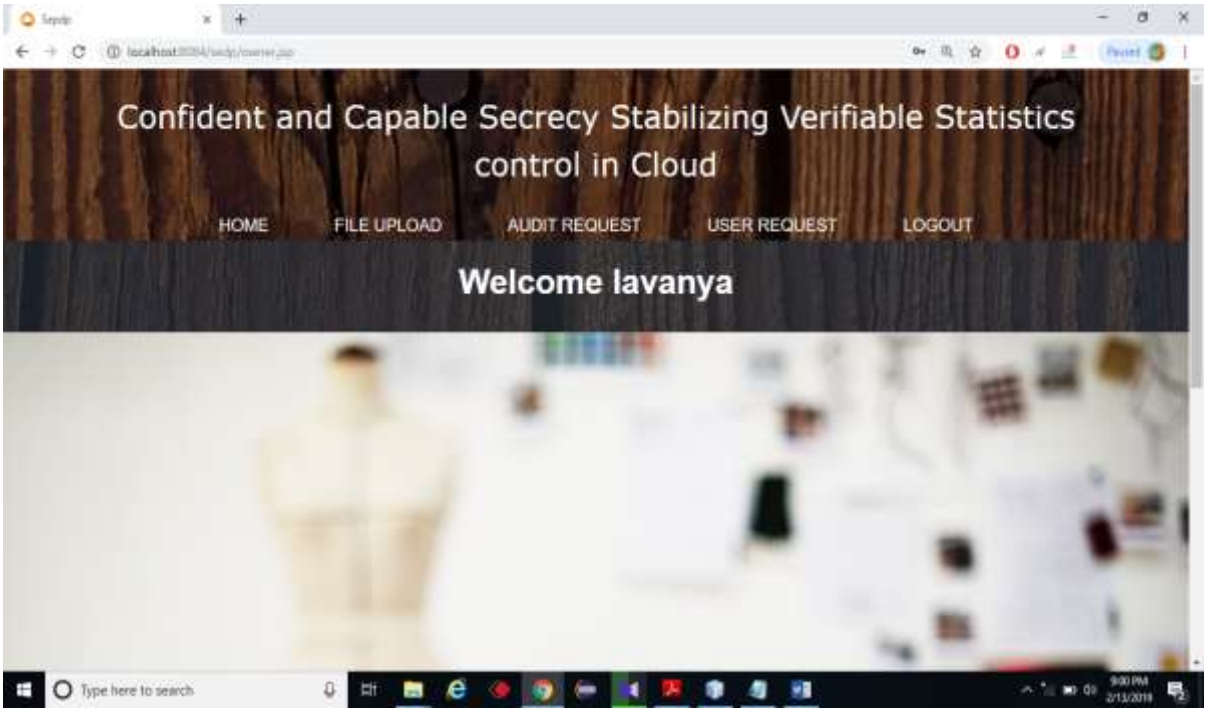

Fig 4:Data Owner Main Page

Computation Overhead Comparison

Schemes	Phase			Overall Computation
	KeyGen	Signing	Auditing	
Shacham et al. scheme [4]	T_e	$2nT_e + nT_m + nT_h$	$2T_p + (2c+1)T_e + (3c-1)T_m + cT_h$	$2T_p + (2n+2c+2)T_e + (n+3c-1)T_m + (n+c)T_h$
Zhu et al. scheme [17]	$2T_e$	$(2n+1)T_e + 2nT_m + (n+1)T_h$	$4T_p + (2c+3)T_e + (4c-1)T_m + cT_h$	$4T_p + (2n+2c+6)T_e + (2n + 4c-1)T_m + (n+c+1)T_h$
Wang et al. scheme [8]	$2T_e$	$2nT_e + nT_m + nT_h$	$2T_p + (2c+3)T_e + (3c+1)T_m + (c+2)T_h$	$2T_p + (2n+2c+5)T_e + (n+3c+1)T_m + (n+c+2)T_h$
Yang et al. scheme [12]	T_e	$(n+2)T_e + nT_h$	$3T_p + (2c+3)T_e + 2cT_m + cT_h$	$3T_p + (n+2c+6)T_e + 2cT_m + (n+c)T_h$
SEPDP	T_e	$T_e + 2nT_m + nT_h + T_i$	$3T_e + (3c+1)T_m + cT_h$	$5T_e + (2n+3c+1)T_m + (n+c)T_h + T_i$

Table 1: Computation Overhead Comparison

5.CONCLUSION

This project proposes the SEPDP strategy for untrusted and outsourced storage systems as a tried-and-true data possession scheme that protects privacy. SEPDP can also be used for dynamic data updates from various owners and batch audits. The CSP cannot forge a response without the right blocks, demonstrating how SEPDP safeguards data privacy from TPA. The suggested system has a lower computational overhead and some of its most appealing features include blockless verification, privacy preservation, batch auditing, and data dynamics.

REFERENCES

[1] K. Yang and X. Jia, "Data storage auditing service in cloudcomputing: Challenges, methods and opportunities," World WideWeb, vol. 15, no. 4, pp. 409–428, 2012.

[2] B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing fordata integrity in the cloud," in Proc. IEEE Conf. Commun.Netw.Secur., 2013, pp. 136–144.

[3] S. K. Nayak and S. Tripathy, "Privacy preserving provable datapossession for cloud based electronic health record system," inProc. IEEE Trustcom/BigDataSE/ISP,, 2016, pp. 860–867.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," inProc. 14th Int. Conf. Theory Appl. Cryptology Inf. Secur., 2008,pp. 90–107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc.29th IEEE Conf. Comput.Commun., 2010, pp. 1–9.

[6] L. Yuchuan, F. Shaojing, X. Ming, and W. Dongsheng, "Enabledata dynamics for algebraic signatures based remote data possession checking in the cloud storage," China Commun., vol. 11,no. 11, pp. 114–124, 2014.

[7] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamicdata possession in cloud computing systems," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 3, pp. 485–497, Mar. 2015.

[8] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Trans.Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores,"in Proc. 14th ACM Conf. Comput. Commun.Secur., 2007, pp. 598–609.

[10] B. Wang, H. Li, X. Liu, F. Li, and X. Li, "Efficient public verification on the integrity of multi-owner data in the cloud," J. Commun.Netw., vol. 16, no. 6, pp. 592–599, 2014.

[11] Y. Zhu, H. Hu, G.-J.Ahn, and M. Yu, "Cooperative provabledata possession for integrity verification in multicloudstorage,"IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244,

Dec. 2012.

[12] K. Yang and X. Jia, "An efficient and secure dynamic auditingprotocol for data storage in cloud computing," IEEE Trans.

ParallelDistrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[13] H. Wang, "Proxy provable data possession in public clouds," IEEETrans. Serv. Comput., vol. 6, no. 4, pp. 551–559, Oct.–Dec. 2013.

[14] H. Wang, "Identity-based distributed provable data possession inmulticloud storage," IEEE Trans. Serv. Comput., vol. 8, no. 2,pp. 328–340, Mar./Apr. 2015.

[15] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secureand dependable storage services in cloud computing," IEEETrans. Serv. Comput., vol. 5, no. 2, pp. 220–232, Jan. 2012.

[16] Y. Zhu, G.-J.Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu,"Dynamic audit services for outsourced storages in clouds,"IEEE Trans. Serv. Comput., vol. 6, no. 2, pp. 227–238, Apr.–Jun.2013.

[17] Y. Zhu, H. Wang, Z. Hu, G.-J.Ahn, H. Hu, and S. S. Yau,"Dynamic audit services for integrity verification of outsourcedstorages in clouds," in Proc. ACM Symp. Appl. Comput., 2011,pp.

.