A SUCCESSFUL METHODOLOGY FOR CLOUD-BASED DATA PROCESSING THAT MAINTAINS PRIVACY WHILE UTILIZING ENCRYPTION STRATEGIES

[1]K. Srikanth Reddy, [2]Sd. Afrin, [3]Chegu. Rupa Kalpana, [4]S.V. Padmaja Rani
[1,2,3]Dept of Computer Science and Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.
[4]Dept of Electronics and Communication Engineering, Sree Venkateswara College Of Engineering, Nellore (Dt), Andhra Pradesh, India.

ABSTRACT
Users (the data owners) can store their data on cloud servers, and users (the data consumers) can access that data owing to a novel paradigm known as "cloud computing." This paradigm lowers the data owner's storage and maintenance costs. There is a greater chance of a security breach because the original owner of the data no longer has access to it directly. Therefore, a data integrity auditing solution is crucial for the cloud. The requirement to validate data ownership while maintaining privacy complicates this matter. This research offers a secure and trustworthy method of proving data ownership (SEPDP) to overcome these problems. Additionally, we add batch verification, data dynamics, and multiple owners to SEPDP. The auditor may easily and cheaply verify the existence of data under this arrangement, which is its most compelling feature.
Keywords: Cloud storage, SEPDP, Security

1. INTRODUCTION

Since it requires less initial infrastructure setup, less maintenance work, and unrestricted data access from any location or device, storage-as-a-service has evolved into a useful commercial alternative to local data storage. In addition to offering many advantages including cost savings, accessibility, usability, synchronisation, and sharing because the cloud service provider (CSP) manages the data, it also carries a number of security threats because it is under the CSP's control. The infrequently used data can be deleted by CSP in order to save space and boost company profitability. However, if it wants to keep its reputation intact, it can also make up instances of data loss and corruption brought on by hardware or software malfunction. Therefore, it's crucial to ensure that data stored in the cloud is accessible. [1], [2]. Because data users (DUs) lack a local copy of the data, traditional cryptographic methods for data integrity verification either call for a local copy of the data, which DUs do not possess, or allow DUs to download the entire data set. Because the first requires additional storage and the second increases the cost of file transfers, neither of these solutions seems practical. Numerous methods—including those proposed in [3], [4], [5], and [6]—use block less frication to check the data's integrity without downloading the whole thing.

One of its enticing features is the public's capacity to verify these efforts. DUs may hire a third-party auditor (TPA) to conduct their audits if they have the ability to conduct public audits. It is equipped with the information and abilities required to influence both the CSP and the DU. [4], [7]. By randomly inspecting a limited number of blocks, these systems use the proven data possession (PDP) technique to confirm that data is present in the trusted cloud storage. Several methods [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15] have recently been developed to allow TPA to validate the accuracy of the data saved on the trusted cloud. Each of these strategies has benefits and drawbacks. Privacy protection is essential to stop TPA from using the cloud server's response during auditing to deduce the data. owever, the systems suggested in [2], [3] do not satisfy the

requirements for maintaining privacy.
The batch auditing criteria, which mandates that TPA be able to manage a large volume of simultaneous verification requests from numerous DUs, could not be met by schemes like [3], [10], or [16]. Through this feature, CSP and TPA may communicate and calculate at a cheaper cost. Unfortunately, the systems [2, [3], [4], [11], [12], [13], [15], and [16], which are slower and need more computing, employ pairing-based cryptographic operations. In this study, we present an efficient and secure method (SEPDP) for ensuring that verified data possession for cloud storage protects privacy. The key generation, signature generation, and auditing phases of operation are the three.
SEPDP's lack of any computationally intensive methods, including pairing-based procedures, is its most enticing feature. Additionally, we expand SEPDP's support to include batch auditing, currently applied methods. We see that the total time for TPA verification of the proposed scheme is less than the total time for existing schemes. This demonstrates the value and suitability of SEPDP for use in implementing verification at low powered devices. The subsequent sections of this essay are structured as follows.

2. RELATEDWORK

Two mobile apps based on the RSA approach are proposed as the first access control mechanism and data integrity under the proven data possession (PDP) paradigm in the paper [15]. The author of the paper [16] created a proof of retrievability (PoR) technique to validate the correctness of distant data. When a smaller authentication tag that is attached to it is used, the PoR system performs better [17]. The author of the research [18] suggests a more adaptable PDP approach that makes use of symmetric key encryption methods to facilitate dynamic processes.
The PDP protocol allows for some blocks to be added while it is operating because of its adaptability [19]. The performance of Flexibility is improved via a new PDP system that employs a different data structure [20]. To handle its data functions equally, a second PDP model with a distinctive data structure is developed [21]. The author of the study developed a multireplicas data verification method that completely supports dynamic data changes in order to improve the correctness of the data [22].
For multicloud servers, a special data integration protocol [3] is developed. The study's author [20] creates a solid plan to simultaneously guarantee the integrity of all copies while taking into account the difficult situation where multiple copies are held in various CSPs. To facilitate the delegation of data verification that employs concessions to guarantee auditor approval, a proxy PDP system [5] is developed. The limits placed on the verifier that made the scheme more robust are also lifted, and an alternative PDP certification mechanism is advised [6]. A PDP protocol for open research has been developed, and an information security concept has been put out [7] to assure the security of information. The PDP system with data protection has been implemented to address the issue with certification management.
Identity-based cryptography, which takes the user's individual identity as input, now makes it possible to establish a secret key [19]. To ensure anonymity, it is advised to utilise another PDP protocol [3].
A PDP technique that uses the proxy signature mechanism to revoke the user's access to the CSP has been developed to address the issue of user revocation, which has been discussed [15]. To track user privacy and identification, a PDP-based group data protocol was created [3]. It is suggested to use a PDP system [7] for data exchange between several senders. The study's author [3] suggests SEPDP systems while upholding data security.
For PPDP, there are two default settings: one is interactive and the other is not [5]. The noninteractive PPDP [2-6] setting is where the K-anonymity model [51] and its consequences are most commonly applied. Both an interactive setup of PPDP [8–10] and differential privacy (DP) [57] heavily rely on DP-based methods. PD-dependent methods for noninteractive circumstances have been documented in several research [6]. In order to safeguard the privacy of SN users, researchers have developed the procedures for anonymizing tabular data [2-

4].
Typically, internet photos are compressed. As a result, many research develop various methods for AMBTC-compressed images. Data hiding is a popular study topic right now. By putting sensitive information in the cover picture, we may conceal the data, and as a consequence, we obtain the stego image. There are two types of data concealment techniques: irreversible [5-8] and reversible [6-11]. A semi-trusted proxy may re-encrypt a cypher text chosen for data gathering without first decrypting it [12].

3. SYSTEM ANALYSIS

The two main categories of remote data integrity checking methodologies are as follows. Deterministic guarantee-based techniques like [17] [18] and [19], which require a significant amount of storage and computing, are used to verify each block of data. Alternative provable data possession (PDP) scheme types, such as [8], [3], and [20], use a probabilistic checking technique that involves randomly selecting a small sample of blocks to check for manipulation. In [8], PDP is introduced, which employs random sampling of a small number of blocks for integrity checking. Shacham et al. developed two alternative integrity verification processes. The second utilises boneh-lynn-shacham (BLS) signatures, but the first employs pseudo-random function (PRF), which is not publicly verifiable [20].
Both techniques offer blockless verification, however they fall short when it comes to safeguarding the DO's data. Blockless verification has to combine sampled blocks linearly, which offers TPA a hint on how to extract the data [4]. Wang et al.'s [4] public auditing technique was expanded to include batch auditing in order to protect the privacy of the data owner providing blockless verification. As a result, TPA is able to handle several auditing requests from various DUs at once. However, none of these schemes [3], [4], or [8] can accommodate data dynamics. Additionally, if one block is altered (added, modified, or deleted), the related verification meta-data (signature) of all other blocks must also be updated since the index numbers of the corresponding blocks are contained in the signatures of the data blocks.
In the technique outlined in [16], an index hash table (IHT) is utilised to promote data dynamics while lowering update costs in a public auditing system. Sadly, the batch auditing property is not supported by this scheme. Later, Wang et al. [7] added data dynamics to their original technique [4]. Yang et al. [11] introduced a dynamic auditing protocol that is efficient and safe and satisfies all requirements for public auditing. It also utilises fewer resources for communication and computing. A certificateless public auditing strategy is provided by Wang et al. [2] for validating data integrity in the cloud. Despite not requiring a certificate for key generation, this approach is unable to achieve the necessary privacy, data dynamics, and batch auditing qualities. But because pairing-based cryptography is used in the [2, 3, 4, 8, 11, 15, and 16] schemes, audit phase verification costs are higher.

4. PROPOSEDSYSTEM

A secure and efficient SEPDP (Secure and Efficient Privacy Preserving Provable Data Possession) for cloud storage is suggested by the system in the proposed work. The three phases of operation are key generation, signature generation, and auditing. SEPDP's lack of any computationally intensive methods, including pairing-based procedures, is its most enticing feature.
The system significantly enhances SEPDP by supporting multiple data owners, batch auditing, and operations on dynamic data. a probabilistic technique to determine the integrity of the blocks stored at CSP. The system assessed the recommended plan's efficacy and contrasted it with a few currently popular procedures.
The suggested scheme's TPA validates data more fast than the present approaches do, according to the system's observations. This demonstrates the efficacy and suitability of SEPDP for use in carrying out the verification at low powered devices.

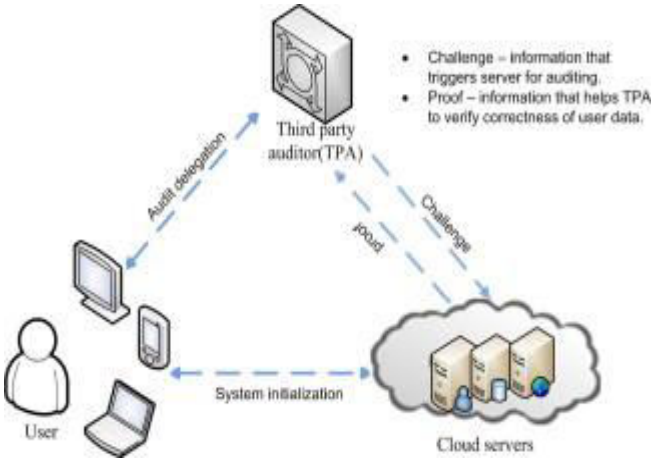

Fig.1. For cloud storage, a safe and effective privacy-preserving provable data possession technique (SEPDP) is used.

5. IMPLEMENTATION

DataOwners

The data owner can upload blocks, verify blocks (data auditing), update blocks, delete files, and view uploaded blocks in this module.

Fig.2. Data can upload into blocks and verify

User

He logs in to this module using his or her user name and password. Receiver will carry out actions such as View All Data Owner Files after logging in. demand for file, View Response to File, Download File

CloudServiceProvider

In addition to managing a server for data storage, the service provider can perform the following tasks, such as see data owners, view end users, and more. Viewing a hash table, a file request, a transaction, an attacker, a result, a file time delay result, or a file throughput result will all show you information about that file.

CONCLUSION

SEPDP, a privacy-preserving data possession mechanism for erratic and external storage systems, is presented in this paper. Additionally, batch auditing and multiple owners updating dynamic data have been made possible by the expansion of SEPDP. Investigation into the system's security reveals that SEPDP shields data privacy from TPA while prevents CSP from forging responses without preserving the necessary blocks. The ability of the suggested method to manage all crucial elements, including blockless verification, privacy preservation, batch auditing, and data dynamics, with minimal processing overhead is one of its most alluring advantages.

REFERENCES

1. K.YangandX.Jia,–Datastorageauditingserviceincloudcomputing:challenges,methods and opportunities,‖ WorldWide Web,vol.15,no.4,pp.409–428,2012.
2. B.Wang, B. Li,H. Li, and F. Li,–Certificatelesspublic auditingfordata integrity inthe cloud,‖inProceedingsIEEEConferenceonCommunicationsandNetworkSecurity (CNS),2013, pp.136–144.
3. H. Shacham and B. Waters, –Compact proofs of retrievability,‖in Proceedings of 14th ASIACRYPT,2008, pp.90–107.
4. C. Wang, Q.Wang, K.Ren, and W. Lou, –Privacy-preserving public auditing for data storagesecurityincloudcomputing,‖inProceedingsof29thIEEEConferenceonComputer Communications(INFOCOM),2010,pp.1–9.
5. L.Yuchuan, F.Shaojing, X.Ming, and W.Dongsheng,–Enable data dynamicsfor algebraic signatures based remote data possession checking in the cloud storage,‖ China Communications,vol. 11, no. 11, pp. 114–124, 2014.
6. A. F. Barsoum and M. A. Hasan, –Provable multicopy dynamic data possession in cloud computing systems,‖IEEE Transactions onInformation Forensics and Security, vol. 10, no. 3,pp. 485–497,2015.
7. C.Wang,S.S.Chow,Q. Wang,K.Ren,andW.Lou,–Privacypreserving publicauditingfor securecloudstorage,‖IEEETransactionsonComputers,vol.62,no.2,pp.362–375,2013.
8. G.Ateniese,R.Burns,R.Curtmola,J.Herring,L.Kissner,Z.Peterson,andD.Song,–Provable data possession at untrusted stores,‖ in Proceedings of the 14th ACM conference on Computerandcommunications security, 2007, pp. 598–609.
9. B.Wang,H.Li,X.Liu,F.Li,andX.Li,―Efficientpublicverificationontheintegrityofmulti-ownerdatainthecloud,‖JournalofCommunicationsandNetworks,vol.16,no.6,pp.592–599,2014.
10. Y.Zhu,H.Hu,G.-J.Ahn,andM.Yu,–Cooperativeprovabledatapossessionforintegrity verification in multicloud storage,‖ IEEE Transactions on Parallel and Distributed Systems, vol.23, no.12, pp. 2231–2244, 2012.
11. K.YangandX.Jia,–Anefficientandsecuredynamicauditingprotocolfordatastoragein cloud computing,‖ IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp.1717–1726, 2013.
12. H.Wang,–Proxy provable data possession in public clouds, ‖IEEE Transactions on Services Computing, vol. 6, no. 4, pp. 551–559, 2013.
13. C.Wang,Q.Wang,K.Ren,N.Cao,andW.Lou,–Towardsecureanddependablestorage services in cloud computing,‖ IEEE transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012
14. Y.Zhu,G.-J.Ahn,H.Hu,S.S.Yau,H.G.An,andC.-J.Hu,–Dynamicauditservicesfor outsourced storages in clouds,‖ IEEE Transactions on Services Computing, vol. 6, no. 2, pp.227–238, 2013.
15. Y.Zhu,H.Wang,Z.Hu,G.-J.Ahn,H.Hu,andS.S.Yau,―Dynamicauditservicesforintegrityverificationofoutsourcedstoragesinclouds,‖inProceedingsofthe2011ACMSymposiumon AppliedComputing. ACM,2011, pp. 1550–1557.
16. F.Seb´e,J.Domingo-Ferrer,A.Martinez-Balleste,Y.Deswarte, andJ.-J.Quisquater, –Efficient remote data possession checking in critical information infrastructures,‖IEEE Transactionson Knowledgeand DataEngineering, vol. 20, no.8, pp. 1034–1038, 2008.
17. D. L. Gazzoni Filho and P. S. L. M. Barreto, –Demonstrating data possession and uncheatabledatatransfer.‖IACRCryptologyePrint Archive,vol.2006/150,2006.
18. Z. Hao, S. Zhong, and N. Yu, –A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability,‖ IEEE transactions on Knowledge and DataEngineering,vol. 23, no.9, pp. 1432–1437, 2011.

19. D. Boneh, B. Lynn, and H. Shacham, ―Short signatures from the weil pairing,‖in Proceedingsof7thASIACRYPT,2001,pp.514–532.[21]P.Adusumilli,X.Zou,andB.Ramamurthy, ―Dgkd: Distributed group key distribution with authentication capability,‖in Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop. IEEE, 2005, pp.286–293.
20. M. Nabeel, M. Yoosuf, and E. Bertino, ―Attribute based group key management,‖in Proceedings of the 14th ACM symposium on Access control models and technologies, 2014, pp.115–124.
21. B.Lynn,―The pairing-based cryptography library,‖ Internet: crypto.stanford.edu/pbc/[Mar.27, 2013], 2006.