ANVESAK
ISSN: 0378–4568
UGC Care Group1 Journal

AN EFFECTIVE PRIVACY PRESERVATIVE PROVABLE DATA PROCESSING IN CLOUD USING ENCRYPTION TECHNIQUES

[1]Dr. D. Srinivas Reddy, [2]Polu Satish
[1]Associate Professor, [2]Assistant Professor, [1,2]Dept. of Master of Computers and Applications,,
[1,2,]Vaageswari College of Engineering, Karimnagar, Telangana.
E-Mail: [1]srinivasreddydhava@gmail.com, [2]Polu.satish99@gmail.com

ABSTRACT
A new paradigm called "cloud computing" makes it possible for users (data owners) to store their data on servers in the cloud and for users (data consumers) to access that data. This paradigm lowers the data owner's storage and maintenance costs. Additionally, the owner of the data no longer has physical access to it, which increases the security threats. Therefore, a data integrity auditing solution is crucial for the cloud. The necessity to verify data ownership while preserving privacy has made this problem challenging. This paper suggests a secured and effective method of proving data ownership in order to overcome these challenges (SEPDP). Additionally, we broaden SEPDP to incorporate batch verification, data dynamics, and numerous owners. The most attractive feature of this scheme is that the auditor can verify the possession of data with low computational overhead.
Keywords: Cloud storage, SEPDP, Security

1. INTRODUCTION

Storage-as-a-service has emerged as a commercial alternative for local data storage due to its characteristics include less initial infrastructure setup, relief from maintenance overhead and universal access to the data irrespective of location and device. Though it provides several benefits like cost saving, accessibility, usability, syncing and sharing, it raises several security threats as data is under the control of the cloud service provider (CSP). CSP can discard the rarely accessed data to save space and earn more profit, or it can lie about the data loss and data corruption, as a result of software/hardware failure to protect its reputation. Therefore, it is necessary to check the possession of data in the cloud storage [1], [2]. Traditional cryptographic solutions for integrity checking of data, either need a local copy of the data (which the data users (DUs) do not have) or allow the DUs to downloads the entire data. Neither of these solutions seems practical as earlier one requires extra storage and later alternative increases the file transfer cost. To address this issue, several schemes including [3], [4], [5], [6] are proposed which employ block less frication to verify the integrity without downloading the entire data. One of the attractive features of these works is to allow the public eerier to verify. With public audit ability, DUs can recourse the auditing task to a third party auditor (TPA). It has expertise and capabilities to convince both the CSP and the DU [4], [7]. These schemes use provable data possession (PDP) technique, which gives probabilistic data possession guarantee by randomly verifying few blocks for ensuring possession of data in the entrusted cloud storage. Recently, several schemes [2],[3],[4],[5],[6],[8],[9],[10], [11], [11], [12], [13], [14], [15] have been proposed to allow TPA to check integrity of the data stored on the entrusted cloud. These schemes have their own pros and cons. Privacy preserving is essential to prevent TPA to infer the data using the cloud server's response while auditing. However, the schemes proposed in [2], [3] do not achieve privacy preserving requirement. Though data dynamics is an important feature to facilitate the data owners to insert, modify, and delete on a particular block of data, without changing the meta-data of other blocks, the techniques proposed in [3], [4] do not achieve data dynamics requirement.

Meanwhile, the schemes like [3], [10], [16] could not achieve batch auditing requirement which ensures that

TPA should be capable enough to deal with the multiple numbers of simultaneous verification requests from different DUs. This property is to save computation and communication cost between CSP and TPA. Unfortunately, the schemes [2], [3], [4], [11], [12], [13], [15], [16] use pairing based cryptographic operations which are intensive computation and need more time. In this work, we propose a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase. Most attractive feature of SEPDP is that it does not use any intensive computation like pairing based operation. Further, we extend SEPDP to support multiple data owners, batch auditing, and dynamic data operations. A probabilistic analysis to detect the integrity of the blocks stored at CSP. We evaluated the performance of the proposed scheme and compared with some of the existing popular mechanisms. We observe that the total time for verification carried out by TPA in the proposed scheme is less than that of the existing schemes. This signifies that SEPDP is efficient and suitable to implement the verificationat the low powered devices. Remainder of this paper is organized as follows. Section 2 discusses the overview of related works in this field. System model and design goals are presented in Section 3. The proposed scheme is discussed in Section 4. Extension of SEPDP to support multiple DOs, batch auditing and data dynamics requirements are explained in Section 5, 6 and7 respectively. Security analysis of the proposed SEPDP is performed in Section 8. SEPDP is evaluated in terms of performance in Section9.The concluding remarks are provided in Section 10.

2. RELATED WORK

The first access control mechanism and data integrity in the provable data possession (PDP) model is proposed in the paper [15], and it provides two mobile applications based on the RSA algorithm. Like the PDP, the author in the paper [16] proposed a proof of retrievability (PoR) scheme that is used to ensure the integrity of remote data. PoR scheme efficiency is improved using a shorter authentication tag that is integrated with the PoR system [17]. A more flexible PDP scheme is proposed by the author of the paper [18] that uses symmetric key encryption techniques to support dynamic operations. A PDP protocol with some flexible functionality is developed, in which, we can add some blocks at run time [19]. A new PDP system with a different data structure is introduced, and it improves flexibility performance [20]. Similarly, another PDP model with a different data structure is designed to handle its data functionality[21]. To improve the accuracy of the data, the author of the paper [22] designed a multireplicas data verification scheme that fully supports dynamic data updates.

A unique data integration protocol [3] for multicloud servers is developed. The author of the paper [20] also considers the complex area where multiple copies are stored in multiple CSPsand builds a solid system to ensure the integrity of all copies at once. A proxy PDP scheme [5] isproposed, which supports the delegation of data checking that uses concessions to verify auditor consent. In addition, the restrictions of the verifier are removed that strengthened the scheme, and it proposes a separate PDP certification system [6]. To maintain the security of information, a concept for information security is proposed and a PDP protocol for public research is developed [7]. To resolve the certification management issue, the PDP system with data protection is introduced 8].

Identity-based cryptography is developed, in which a user's unique identity is used as input to generate a secret key [19]. Another PDP protocol is recommended to ensure confidentiality [3]. The author of the paper [1] proposed a scheme, in which tags are generated through the ring signature technique for group-based data sharing that supports public auditing and maintains user privacy. A new PDP system is introduced for data sharing over the cloud while maintaining user privacy [12]. Additionally, it supports the dynamic group system and allows users to exit or join the group at any time. Another PDP system [13] that is based on broadcast encryption and supports dynamic groups [4] is introduced. The issue of user revocation has been raised [15], andto address this issue, a PDP scheme has been proposed, which removes the user from the CSP using the

proxy signature method. A PDP-based group data protocol was developed to track user privacy and identity [3]. A PDP system [7] is proposed for data sharing between multiple senders. The author of the paper [3] provides SEPDP systems while maintaining data protection.

However, the author of the paper [9] proved that the scheme proposed in [8] is vulnerable to malicious counterfeiting by the CSP. A collision-resistant user revocable public auditing (CRUPA) system [4] is introduced for managing the data that is shared in groups. Another scheme [4] is introduced as a way to ensure the integrity of mobile data terminals in cloud computing.

To address the PKI issue, identity-based encryption [2] is designed to enhance the PDP protocol and maintain user privacy in a dynamic community. Before sharing user-sensitive data with thirdparties or researchers, data owners ensure that the privacy of user-sensitive data is protected. We can do this using data anonymization techniques [3]. In recent years, the research community has focused on the PPDP search area and developed several approaches for tabular data and SN [4– 9]. There are two popular settings in PPDP: one is interactive, and the other is noninteractive [5].The K-anonymity model [51] and its effects are most commonly used in the noninteractive setting of PPDP [2–6]. Differential privacy (DP) [57] and an interactive configuration of PPDP make extensive use of DP-based methods [8–10]. Meanwhile, several studies for a noninteractive setting reported a PD-dependent approach [6]. Researchers have expanded the concepts used to anonymize tabular data to protect the privacy of SN users [2–4].

Most images on the internet are in a compressed form. Hence, various studies design some techniques for AMBTC-compressed images. Data concealment has become an active research area. We can hide the data by adding confidential information to the cover image, and as a result, we get the stego image. There are two types of data hiding schemes: one is irreversible [5–8], and the other is a reversible data hiding scheme [6–11]. A cipher text designated for data collection can be re-encrypted as designated for another by a semitrusted proxy without decryption [12]. The first concrete construction of collusion-resistant unidirectional identity-based proxy re-encryption scheme, for both selective and adaptive identity, is proposed in the paper [13]. One of the data hiding schemes is the histogram shifting scheme [7], and it is the most widely used. A histogram-shifting data hiding scheme [7] that detects pixel histograms in the cover image is introduced. When big and diverse data are distributed everywhere, we cannot control the vicious attacks. Therefore, we need a cryptosystem to protect our data [8–10].

Some identity-based signature (IBS) schemes [1–4] are introduced that are based on bilinear pairing. However, the authentication schemes based on bilinear pairing over elliptic curve are more efficient and safer than traditional public key infrastructure [5, 6]. The paper [7] proposed apreserving proxy re-encryption scheme for public cloud access control. A differential attack is performed on one-to-many order preserving encryption OPE by exploiting the differences of the ordered ciphertexts in [8]. Another scheme is proposed, which consists of a cancelable biometric template protection scheme that is based on the format-preserving encryption and Bloom filters [9]. Some of the researchers also use the concept of paring free identity-based signature schemes [10–13].

3. SYSTEM ANALYSIS

Remote data integrity checking protocols can be broadly categorized into two kinds. The deterministic guarantee based schemes like [17] [18] and [19], verify each block of data and therefore require a significant amount of storage and computation. Alternative kind of schemes called provable data possession (PDP) includes [8], [3], [20] use probabilistic checking method, in which a few blocks are randomly selected to detect manipulation. PDP is introduced in [8] that use random sampling of a few blocks for integrity verification. Shacham et al. [3] designed two different integrity verification mechanisms. One uses pseudo-random function (PRF) which fails to provide public verifiability, while the other one uses boneh–lynn–shacham (BLS) signatures [20]. Both the schemes support blockless verification but fail to provide privacy of

the DO's data. Blockless verification requires linearcombination of sampled blocks which gives a clue to TPA to extract the data [4]. To preserveprivacy of the data owner supporting blockless verification, Wang et al. [4] proposed a public auditing scheme and extended that to support batch auditing further. As a result, TPA can simultaneously perform multiple auditing requests from different DUs. But, all these schemes [3], [4], [8] fail to support data dynamics. Moreover, as signatures of the data blockscontain index number of the corresponding blocks, if one block is updated (inserted/modified/deleted), the corresponding verification meta-data (signature) of all other blocks need to be updated. The scheme proposed in [16] uses index hash table (IHT) to support data dynamics in public auditing mechanism reducing the update overhead. Unfortunately, this scheme fails to support batch auditing property. later on, Wang et al. [7] extended their previous technique [4] to support data dynamics. Yang et al. [11] proposed an efficient and secure dynamic auditing protocol that achieves all essential features of public auditing. Also it consumes lesser computation and communication cost. A certificateless public auditing scheme for verifying data integrity in the cloud is proposed by Wang et al.[2]. Although this scheme does not require certificate for key generation, it fails to achieve privacy, data dynamics, and batch auditing properties. But, [2], [3], [4], [8], [11], [15], [16] schemes are based on pairing based cryptography, which requires more verification cost in audit phase.

4. PROPOSED SYSTEM

In the proposed work, the system proposes a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase. Most attractive feature of SEPDP is that it does not use any intensive computation like pairing based operation.

Further, the system extends SEPDP to support multiple data owners, batch auditing, and dynamic data operations. A probabilistic analysis to detect the integrity of the blocks stored at CSP. The system evaluated the performance of the proposed scheme and compared with some of the existing popular mechanisms.

The system observes that the total time for verification carried out by TPA in the proposed scheme is less than that of the existing schemes. This signifies that SEPDP is efficient and suitable to implement the verification at the low powered devices.

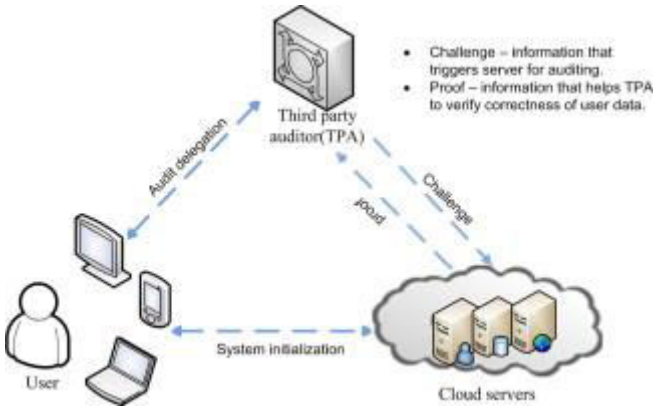

Fig.1. secure and efficient privacy preserving provabledata possession scheme (SEPDP) for cloud storage

5. IMPLEMENTATION

Data Owners

In this module, the data owner performs operations such as Upload Blocks, Verify Block(Data Auditing) , Update Block , Delete File , View Uploaded Blocks

- **User**
  In this module, he logs in by using his/her user name and password. After Login receiver will perform operations like View All Data Owner Files, Request File, View File Response, Download File
- **Third Party Auditor**
  In this module, the sector can do following operations View Hash Table, View Attackers , View File Updated or Deleted , View Results
- **Cloud Service Provider**
  The Service Provider manages a server to provide data storage service and can also do the following operations such as View Data Owners , View End Users , View Hash Table, View File Request, View Transactions, View Attackers, View Results, View File Time Delay Results, View File Throughput Results

6. CONCLUSION

This work presents SEPDP, a privacy-preserving proved data possession technique for unreliable and external storage systems. SEPDP has also been expanded to facilitate batch auditing and multiple owners updating dynamic data. The scheme's security is examined, and it is demonstrated that SEPDP safeguards data privacy from TPA while making it impossible for CSP to counterfeit the response without storing the necessary blocks. The suggested scheme's ability to handle all crucial elements, such as blockless verification, privacy preservation, batch auditing, and data dynamics with lessened computational overhead, is one of its most compelling aspects.

REFERENCES

1. K. Yang and X. Jia, ―Data storage auditing service in cloud computing: challenges, methods and opportunities,‖ World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.
2. B. Wang, B. Li, H. Li, and F. Li, ―Certificateless public auditing for data integrity in the cloud,‖ in Proceedings IEEE Conference on Communications and Network Security (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 storage security in cloud computing,‖ in Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM), 2010, pp. 1–9.
5. L.Yuchuan, F.Shaojing, X.Ming, and W.Dongsheng,―Enable data dynamics for 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 on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, 2015.
7. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, ―Privacypreserving public auditing for secure cloud storage,‖ IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
8. G.Ateniese, R.Burns,R. Curtmola,J. Herring, L.Kissner, Z.Peterson, and D. Song, ―Provable data possession at untrusted stores,‖ in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 598–609.
9. B.Wang,H.Li,X.Liu,F.Li,andX.Li,―Efficientpublicverification on the integrity of multi-owner data in the cloud,‖ Journal of Communications and Networks, vol. 16, no. 6, pp. 592–599, 2014.
10. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, ―Cooperative provable data possession for integrity verification in multicloud storage,‖ IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231–2244, 2012.
11. K. Yang and X. Jia, ―An efficient and secure dynamic auditing protocol for data storage in 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, and W. Lou, ―Toward secure and dependable storage 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, and C.-J. Hu, ―Dynamic audit services for 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,―Dynamic audit services for integrity verification of outsourced storages in clouds,‖ in Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 1550–1557.
16. 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 Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1034–1038, 2008.
17. D. L. Gazzoni Filho and P. S. L. M. Barreto, ―Demonstrating data possession and uncheatable data transfer.‖ IACR Cryptology ePrint 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 Data Engineering, vol. 23, no. 9, pp. 1432–1437, 2011.
19. D. Boneh, B. Lynn, and H. Shacham, ―Short signatures from the weil pairing,‖ in Proceedings of 7th ASIACRYPT, 2001, pp. 514–532. [21] P. Adusumilli, X. Zou, and B. 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.
22. Amazon Elastic Compute Cloud (Amazon EC2) Available: https://aws.amazon.com/ec2/.