IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SECURE CLOUD DATA STORAGE SYSTEM USING A DELEGATABLE PROOF OF STORAGE (DPOS) MECHANISM

R. Jenifer Littleda[1*], and Ms. S. Shanthinidevi[2]

[1*]Department of Computer Science and Engineering, Fatima Michael College of Engineering and Technology, Tamilnadu, India

[2]Associate Professor, Computer Science and Engineering, Fatima Michael College of Engineering and Technology, Tamilnadu, India

***Abstract*— Cloud is one of the widespread technologies in recent days, which reduces the user burden with the local data storage. Generally, ensuring the data integrity and security is highly essential for the cloud storage server. In which, the Proofs of Storage (POS) is identified as the emerging technique for addressing this issue. Then, the publicly verifiable POS allows the third party for verifying the data integrity of the data owner that improves the scalability of cloud service. In the existing works, the publicly verifiable POS schemes are very slow during the computation of authentication tags for the data blogs. Also, it requires expensive group exponentiation operation, which is the bottleneck of the setup phase of this scheme. Thus, this paper proposed a Delegatable Proofs of Storage (DPOS) scheme, which is a kind of lightweight privacy preserving technique. Here, the third party auditor can support and switch at any time based on the functionalities of the POS scheme. Moreover, we speed up the tag generation process without sacrificing the efficiency in other aspects. In addition to that, this mechanism can be extended to support the fully dynamic operations with better efficiency and reduced computation of any data update to O(log n). The results stated that the proposed scheme is better than the other privacy preserving models.**

***Index Terms*— Cloud, Delegatable Proofs of Storage (DPOS), Homomorphic Verifiable Tag, Owner Delegated Auditor, Graphical User Interface.**

I. INTRODUCTION

Cloud computing is one of the interesting and extensively deployed technology in our daily life, which offers various benefits to its users [1]. It includes high scalability, reduced cost, availability, and security. Moreover, people rely on cloud storage services intend to reduce the local storage burden [2]. In this structure, the data is outsourced to the server and can be accessed based on the need [3]. Moreover, ensuring the privacy and security of the data is a demanding issue to solve. For this purpose, the solution like Proof of Storage (POF) [4,5] is required that provides the proof to irretrievability and data possession.

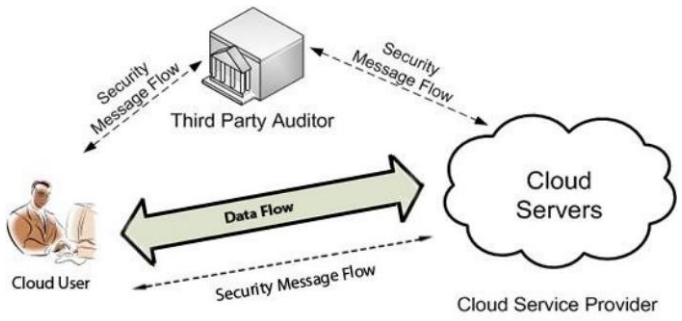

Fig 1. General cloud data storage architecture

The general cloud data storage architecture is illustrated in Fig 1, which contains the components of user, server and third party auditor. The data communication can be performed through the secure message flow. Here, the third party auditor ensures the privacy and confidentiality of the user data. In order to provide the secure cloud data storage, there are different algorithms have been proposed in the existing works. The disadvantages of the existing techniques are as follows:

1. Some data files could attract too much attention from public, which leads to the denial of service attack against the cloud storage server.
2. The data loss can occur due to the unpopular data files audited by the public.
3. The data owner could delegate the auditing task to some third party auditor.

Due to these issues, this paper proposed a Delegatable Proofs of Storage (DPOS) scheme, which provides data auditing and privacy preserving. In this work, a new approach is proposed to enable the fully dynamic operations, which include block insertion, deletion, and modification. Also, it reduces the computation of data updated with the minimized computational cost. This scheme provides the privacy preserving property for the outsourced data. Moreover, the performance of this scheme is improved by implementing a POS scheme with the tag generation process.

The work is structured as follows: the existing techniques related to secure cloud data storage is surveyed in Section II. The working modules involved in the proposed system is stated in Section III. The performance evaluation of the proposed technique and existing techniques are illustrated in Section IV. The overall conclusion and future work of the paper are stated in Section V.

II. RELATED WORKS

This section surveys the existing techniques related to secure cloud data storage, which also provides the advantages and disadvantages of each method. Juels, et al [6] defined and explored the Proof of Retrievability (POR) concept for transmitting a data file with better reliability. Here, the POR protocols were deployed to reduce the communication costs, memory accesses for the prover and the storage requirements. Moreover, a semi trusted environment was considered in this work, where providing unusual security was highly concentrated. The advantage of this work was, it provided a quality of service within a certain time period.

Ateniese, et al [7] developed a new model named as Provable Data Possession (PDP) for ensuring the data originality. This model maintained certain metadata for verifying the proof, which leads to reduced computational time. Also, the response protocol could transmit the constant amount of data for reducing the network communication. Moreover, it supports for remote data checking for a large datasets in a distributed system. Shacham and Waters [8] proposed a proof of retrievability schemes for providing security to the cloud systems. Here, a strong Homomorphic authentication mechanism was developed with the public verifiability scheme for ensuring security. Erway, et al [9, 10] developed a new framework named as Dynamic Provable Data Possession (DPDP) for providing support to the cloud data storage. Here, the authentication based dictionaries have been utilized for offering the rank information, based on this the file could be maintained in the server. Also, the probability of misbehaviour detection rate was estimated to prove the performance of the suggested mechanism. Moreover, this technique was applied on both the version control and outsourced systems.

Curtmola, et al [11] implemented a Multiple Replica Provable Data Possession (MR-PDP) technique for increasing the security of cloud data. Here, the unique replica could be generated for file verification with reduced computational time. Also, each file stored on the cloud was separately encrypted and stored before processing. Wang, et al [12] developed a privacy preserving mechanism for providing security to the data shared on a cloud. In this scheme, a ring based signatures were generated for estimating the verification information that was required during the auditing of data integrity. Also, a third party auditor could be employed for ensuring the data integrity without retrieving the whole data. The benefits behind this paper were increased efficiency and reduced time consumption.

Wang, et al [13] deployed a new cloud storage system based on public auditing for ensuring the data security. Here, the third party auditor has the responsibility to ensure the integrity of the outsourced data. Then, the privacy preserving mechanism was employed to increase the security of cloud data. Xu, et al [14] implemented a new cryptographic tools named as, Proof of Storage (POS) for increasing the cloud data security. The major drawback of this work was, it is very slow during the computation of authentication tags and requires more expensive operations. So, it leads to increased time consumption and computational complexity. Ateniese, et al [15] used some Homomorphic protocols for cloud data security, where the authentication was performed based on the signature and message. Moreover, a public key linear authenticator was used to satisfy the Homomorphic properties.

III. PROPOSED METHODOLOGY

The proposed system mainly focused on the public verifiability and support data dynamics, where the POS is used to support the dynamic operations. In which, the data owners provide the request to modify, insert, and delete data blocks after outsourcing the original data into the cloud server. The basic idea behind this technique is to generate a Homomorphic Verifiable Tag (HVT) that is send to the cloud server with the data file. After that, a new variant formulation named as Delegatable Proofs of Storage (DPOS) is developed to support the delegation of data auditing task. Consequently, the cloud server can accept the file request send by the user, and the admin can view the ODA/data owner/user list based on the cloud registration process. Also, the admin can maintain the details of all users, clients, and ODA, who has the accessibility to view the audited files. The proposed scheme is also intended to support the fully dynamic operations with the reduced computation of data update, which leads to the reduced cost consumption for block verification. The architecture of the proposed system is shown in Fig 1, which includes the following modules;

- Cloud server
- Key generation
- ODA allocation
- Data dynamics

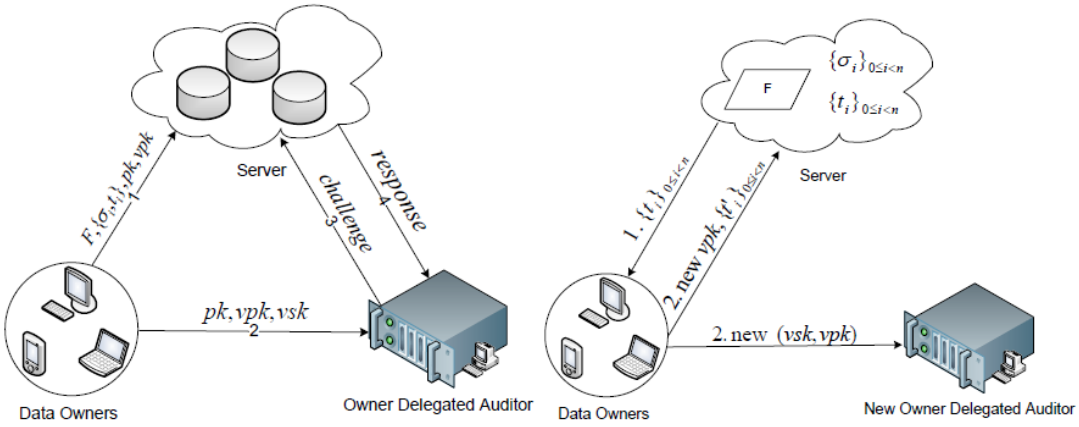

Fig 2. Architecture of the proposed system

The major advantages behind this work are as follows:

- It eliminates the burden of data owner.
- Data owner has the ability to select and revoke the ODA file.
- Data file is audited by ODA using HVT, which meant by the block auditing is done using ODA.

3.1 Cloud Server Module

In this module, the cloud can accept the file request sent by the user, and the admin can view the ODA/data owner/user list by using the registration process. Then, the admin also maintains the details of all clients, users and ODA. The cloud storage server is considered as the trusted party in data privacy, which has the access of the plaintext to offer an extra services to the owner. But, it is not considered as trusted in terms of maintaining the data integrity, because it could delete the rarely accessed files for their own benefits. Also, it can hide the exploitation actions caused due to failures for maintaining their reputation, thus it could be revoked at earlier. Then, the cloud server could update the file blocks based on the HVT from the data owner.

3.2 Key Generation

In this module, the data owner could upload the files into the cloud, where the whole data can be split into multiple blocks and each block is used to generate a HVT. After that, the HVT with the data file is send to the cloud server, and the cloud generates both the public/private keys. Then, these keys are delegated to the ODA, where the master private/public keys are kept as unchanged. Here, the ODA is treated as the trusted party that could perform the delegated auditing task for protecting the secret key in a secured way. But, this is not considered as trusted in terms of data privacy, because the revoked ODA can be either malicious and submits the verification secret key to the server.

3.3 Allocation of ODA

In this module, the data owner could assign the files to ODA and to their company members according to their domains. Here, the ODA has the authority to view the files, and it audit the files based on the following methods: set of data blocks and whole file. After that, the verification key can be updated once, then the ODA is revoked and the new one is selected by the data owner. Moreover, the communications between the data owner can be performed via a secured channel that ensures both the privacy and integrity.

3.4 Data Dynamics

In this module, the data owner could update or delete the file, and also it uses the master public key and HVT key for updating and uploading the file into the cloud. Here, the cloud admin could also update the HVT key, and the data owner has the rights to delete and audit the status of their file. Moreover, a new HVT that corresponds to the required tag can be regenerated and send to the cloud server. Then, the indices can be maintained and managed based in the data updated, which avoids the impact on other tags. Also, each data block is bound with a separate index that is not reused for other blocks, which is denoted as a synthetic index. This index could be determined based on the tag generation, and a semantic index can be change due to the dynamic operations. The proposed scheme allows the data owner could perform the operations like insert, delete, or update the data files with reduced computational and storage overhead by maintaining the synthetic index in an efficient way. The work flow operations performed between the data owner, ODA and cloud server is depicted in Fig 3.

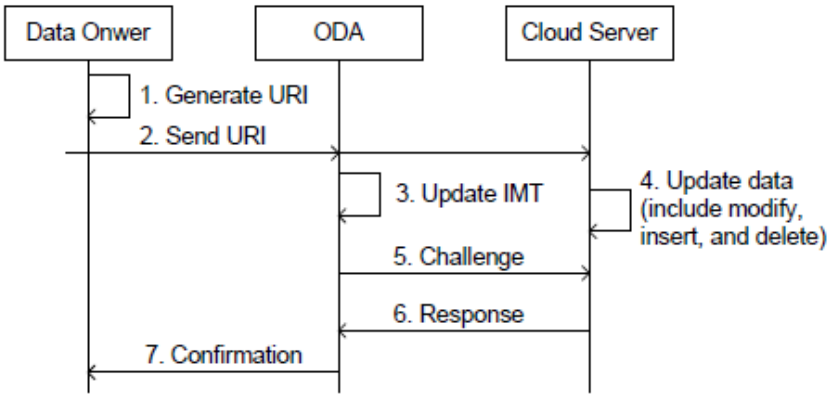

Fig 3. Workflow operations between the data owner, ODA and cloud server.

Moreover, the dynamic operations can be performed based on the tag generation process of DPOS. During this process, the semantic and synthetic indices are identical, and the tag is sent to ODA for auditing. This DPOS scheme is considered as secure and privacy preserving, because it does not change the tag generation and block verification processes.

IV. PERFORMANCE ANALYSIS

This section evaluates the performance analysis of the existing and proposed techniques. The results are evaluated in terms of data preprocessing time, auditor computation time, server computation time, and communication cost. Moreover, some of the existing techniques are considered in this paper for analyzing the betterment of the proposed technique. Table 1 shows the software and hardware requirements of the proposed system.

Table 1. Software and hardware requirements

Software Requirements	
Operating system	Windows 7, 8, 10
Front end	Visual Studio 2010, ASP.net, C#
Back end	SQL Server 2008R2
Hardware Requirements	
Processor	Pentium-IV
Speed	1.1 GHz
RAM	256 MB (Min)
Hard disk	20 GB
Key board	Standard windows keyboard
Mouse	2 or 3 Button mouse
Monitor	SVGA

Fig 4 shows the data preprocessing time of the existing and proposed techniques in terms of varying file size (MB). Generally, the data preprocessing can be done by the data owner, so it is considered as an essential factor for analyzing the Quality of Service (QoS). From the results, it is evident that the proposed DPOS scheme provides the better results compared than the other techniques. Fig 5 and 6 shows the auditor's and server's computation time of the existing and proposed techniques, which is estimated with respect to the number of sampled blocks. In this proposed system, a constant number of exponentials and pairing have been done during the processes of verification and proofing. The results stated that the proposed DPOS scheme provides the reduced auditor's and server's computation time, when compared to the other techniques. Fig 7 depicts the communication cost of the existing and proposed methods with respect to the number of sampled blocks. Naturally, communication cost is estimated based on the auditor and server response with respect to the challenge and proof of transcripts. The results stated that the proposed DPOS scheme consumes less computation cost, when compared to the existing techniques. The overall analysis illustrated that the proposed DPOS mechanism performs an efficient authentication and tag generation processes. It leads to the minimized communication cost, computational time, and data preprocessing time with the use of HVT.

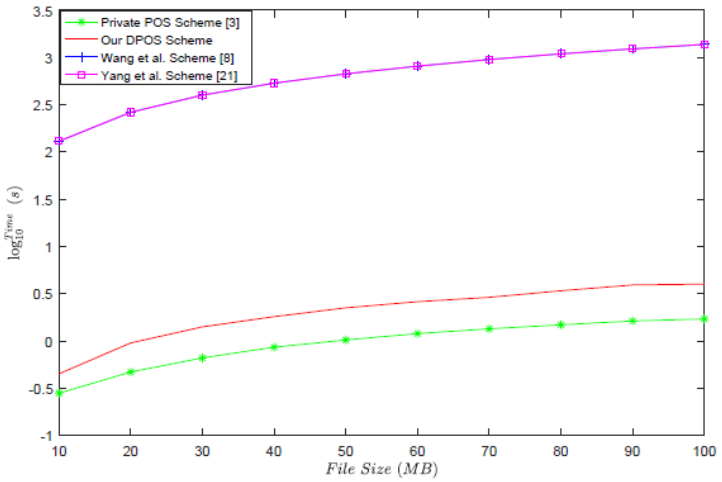

Fig 4. Data preprocessing time

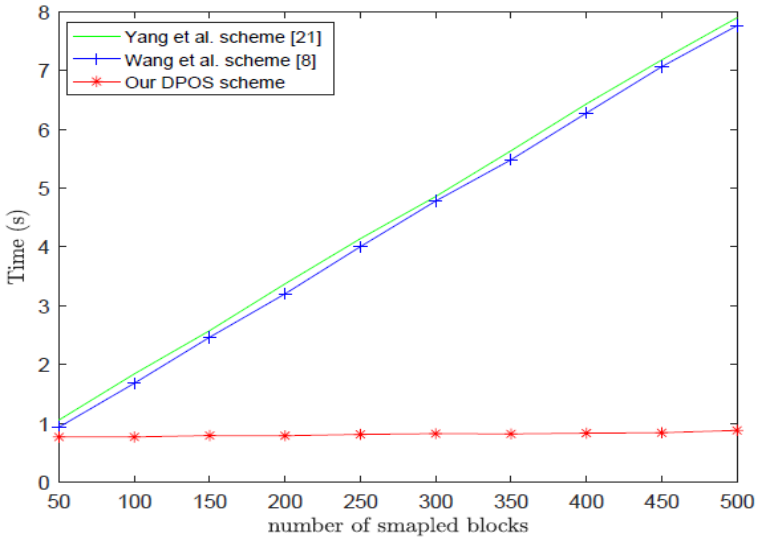

Fig 5. Auditor computation time

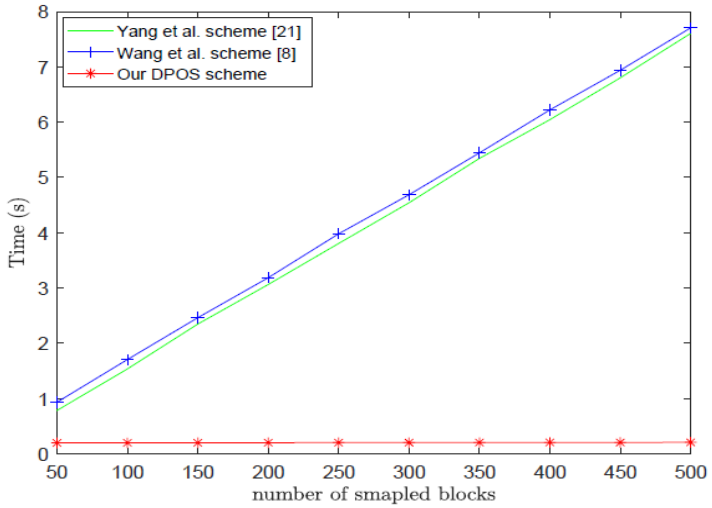

Fig 6. Server computation time

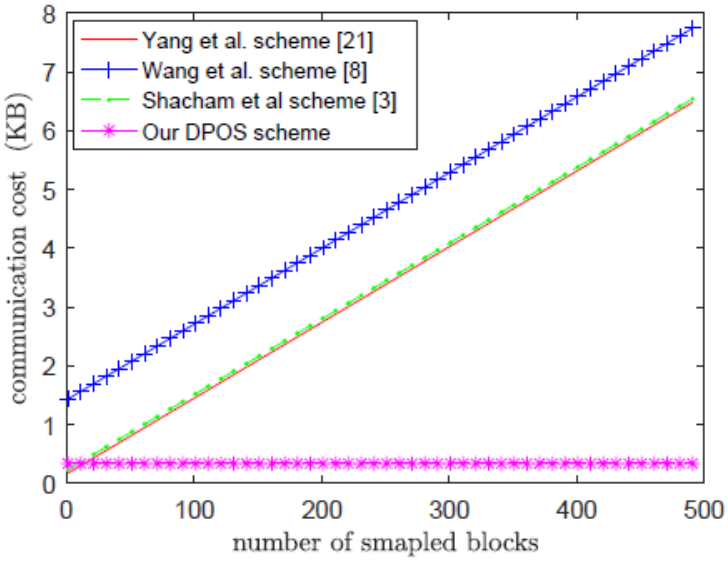

Fig 7. Communication cost

V. CONCLUSION

In this paper, a lightweight and privacy preserving mechanism named as, POS is proposed for secure cloud data storage. This technique is more efficient in authentication and tag generation processes. For this reasons, the techniques such as HVT and DPOS are utilized in this paper. On other hand, this scheme supports the third party auditor (i.e. ODA) to revoke an auditor at any cost, which is close to the functionality of publicly verifiable POS scheme. The experimental results illustrated that the DPOS provides the better performance results, when compared to the existing publicly verifiable POS schemes. Because, it implements a strong authentication and tag generation processes. Moreover, this technique prevents the data leakage to the auditor during the auditing process.

REFERENCES

[1] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in CRYPTO '92: *Annual International Cryptology Conference on Advances in Cryptology*, pp. 31–53.

[2] J. Alwen, Y. Dodis, and D. Wichs, "Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model," in CRYPTO '09: *Annual International Cryptology Conference on Advances in Cryptology*,pp. 36–54, 2009.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," *ACM Transaction on Information and System Security, TISSEC 2011*, vol. 14, no. 1, pp. 12:1–12:34, 2011.

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," *Journal of Cryptology, JOC 2013*, vol. 26, no. 3, pp. 442–483, 2013.

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in *The 14th European Symposium on Research in Computer Security, ESORICS 2009*, vol. 5789 of LNCS, pp. 355–370, Springer, 2009.

[6] Juels, Ari, and Burton S. Kaliski Jr. "PORs: Proofs of retrievability for large files." In *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 584-597. 2007.

[7] 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, CCS 2007*, pp. 598–609, ACM.

[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Advances in Cryptology - ASIACRYPT 2008*, vol. 5350 of LNCS, pp. 90–107, Springer, 2008.

[9] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS 2009, pp. 213–222, ACM, 2009.

[10] C. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," *ACM Transactions on Information and System Security*, vol. 17, pp. 15:1–15:29, April 2015.

[11] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in *Proceedings of the 28th International Conference on Distributed Computing Systems*, ICDCS 2008, pp. 411–420, IEEE, 2008.

[12] B.Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in *Proceedings of 5th International Conference on Cloud Computing*, Cloud 2012, pp. 295–302, IEEE, 2012.

[13] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, Privacy preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, TC 2013, vol. 62, no. 2, pp. 362–375, 2013.

[14] J. Xu, A. Yang, J. Zhou, and D. S. Wong, "Lightweight Delegatable proofs of storage," in *Proceedings of 21st European Symposium on Research in Computer Security, ESORICS 2016,* pp. 324–343, Springer International Publishing, 2016.

[15] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in *Advances in Cryptology -ASIACRYPT 2009,* vol. 5912 of LNCS, pp. 319–333, Springer, 2009.