# File Splitting and Storing In Multiple Cloud Servers for Secured Cloud Storage

**A.Prema**
Department of Information Technology, Velammal Engineering College, Anna University.
Email: Prema@velammal.edu.in
**S.Aishwarya,**
Department of Information Technology, Velammal Engineering College, Anna University.
Email: aishu25198@gmail.com
**M.Keerthana**
Department of Information Technology, Velammal Engineering College, Anna University.
*Email:* keer707@gmail.com
**K.S.Nivetha**
Department of Information Technology, Velammal Engineering College, Anna University.
*Email:*nivethaksn@gmail.com

**----------ABSTRACT----------**

**Cloud users no longer physically possess their data, to ensure the integrity of the usually executed data becomes a challenging task. To address this problem and to audit static archive data, schemes such as "provable data possession" and "proofs of retrievability" were proposed and therefore they lack data dynamics support. Moreover, the threat in this scheme is that it usually assumes that there is a true data owner and focuses on detecting a false cloud service provider despite the fact that the clients of the cloud servers may also misbehave. In this paper public auditing scheme with data dynamics support and fairness arbitration of potential disputes is proposed. We design an index switcher to discard the disadvantages of index usage in tag computation in current schemes and achieve efficient handling of data dynamics. To resolve the problem we further expand the existing threat models and adopting signature exchange idea to design better arbitration protocols, so that no party can misbehave without being detected and any possible dispute can be fairly settled. By analysing the security, the scheme which is used is shown as provably secure and the evaluation of performance demonstrates that the overhead of data dynamics and dispute arbitration are reasonable.**

Keywords - **Cloud Service Provider, data Dynamics support, signature scheme, protocols and auditing scheme.**

---

## I. INTRODUCTION

Cloud computing is the concept of using the system resources that is hardware and software which are delivered as a service through a network typically internet. Cloud storage is one of the important applications of cloud computing. In this paper, to improve the security, a scheme has been adopted which includes a protocol(ID-DPDP - Identity-based Distributed Provable Data Possession) and a signature strategy (BLS - Boneh-Lynn-Shacham). ID-DPDP is used to store information in multi cloud by splitting them into desired entities. It also eliminats certificate management. BLS is used for batch auditing based on randomly generated private key. With these, the given file is splitted and stored in cloud in encrypted form, so that users cannot read the file directly and also integrity check is performed by TPA without downloading the entire file.

## II. RELATED WORK

The existing system aims primarily at the earlier auditing schemes that usually require the CSP to generate a deterministic proof by accessing the whole data file to perform integrity check. Secondly, some auditing schemes provide private verifiability that requires only the data owner who has the private key to perform the auditing task, which may potentially overburden the owner due to its limited computation capability. Thirdly, Proof of data possession and Proof of Retrievability intend to audit static data that are seldom updated, so these schemes do not provide data dynamics support. Current research usually assumes an honest data owner in their security models, which has an inborn inclination towards the cloud users. But the fact is not only the cloud, but also cloud users have the motive to engage in deceitful behavior. Both clients and the CSP may misbehave during auditing.

## III. PROPOSED SYSTEM

The proposed system extracts the threat in current model to provide dispute arbitration, which is more significant and practical for cloud data auditing. Furthermore and important, data owner delegates his auditing tasks to a TPA always who is trusted by the owner but not by the cloud necessarily. In this we use the idea of signature exchange to ensure the correctness of the metadata and fairness of the protocol, and also concentrate on combining the data dynamics support and dispute arbitration into a single auditing scheme efficiently.This paper proposes an auditing scheme which address the

problems of data dynamics support, public verifiability and dispute arbitration simultaneously.

3.1 Data owner

Associate in nursing entity, that has large information to store in multi cloud for maintenance and computation. Data owner uploads the file which is splitted by using the ID-DPDP protocol and stored in multi cloud. The splitted data are encrypted using BLS signature scheme based on randomly generated public key.

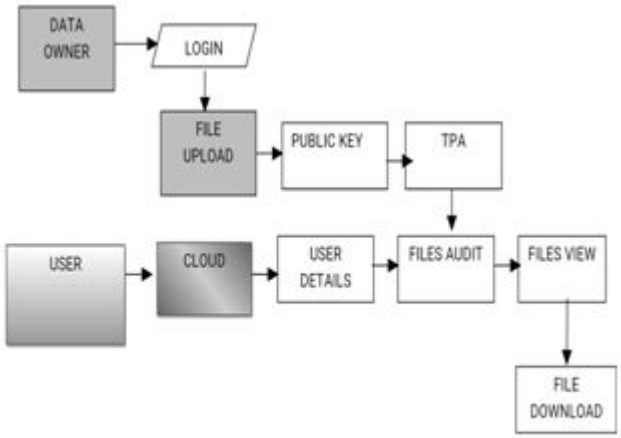


**Fig. 1 File splitting and auditing architecture**

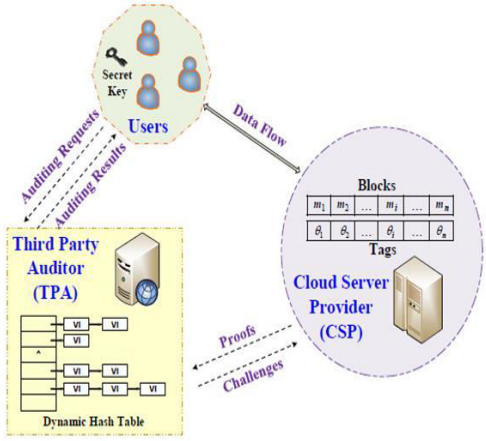


Fig. 2 Storage of block-tag pairs of splitted data in DHT

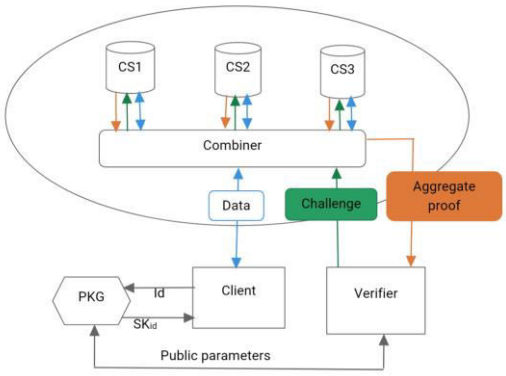


Fig. 3 ID-DPDP Protocol Architecture

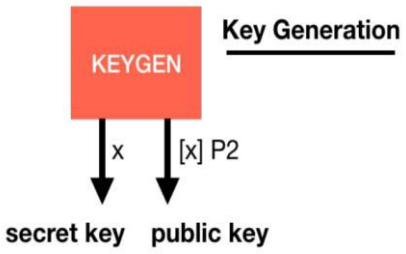


Fig. 4 Key Generation

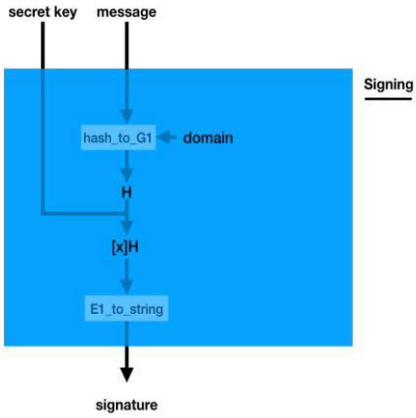


Fig. 5 Signing process

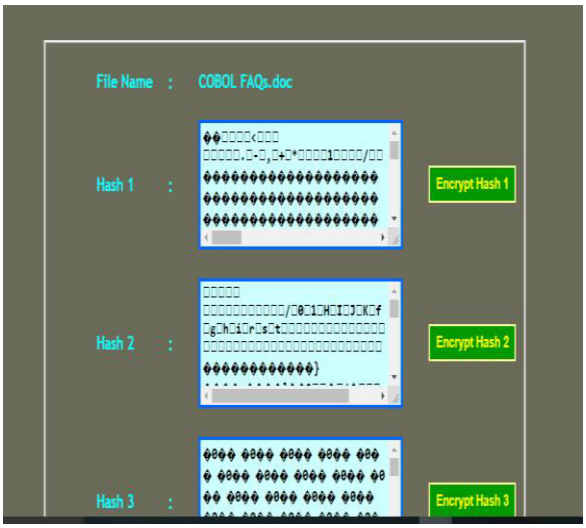


Fig. 6 Example of hashed data to be encrypted

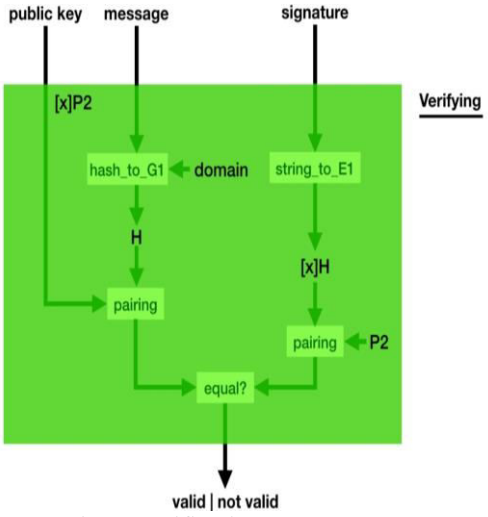


Fig. 7 Verification process

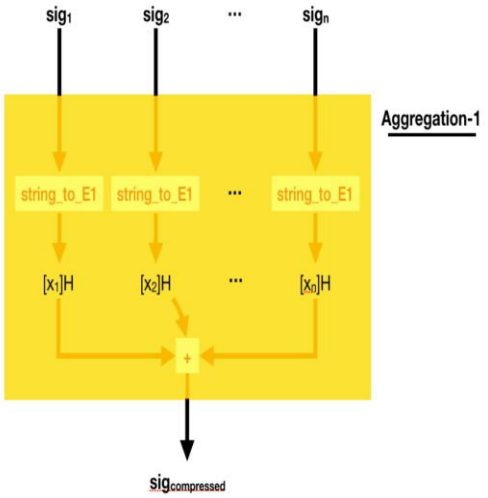


Fig. 8 Aggregating process

3.2 TPA

Third Party Auditor, who checks for integrity of stored data. Data owner's delegates all his tasks to TPA, which reduces the burden of data owner and supports data dynamics. The block-tag pairs of splitted data are stored using Dynamic Hash Table, which propose data dynamics support.

3.3 User

It is who uses the cloud services. If a user wants some data file from cloud services, user has to request the cloud and also user cannot read the file directly. User has to enter his/her key to get access, decrypt the file and only then the user can download the file.

3.5 Verifier

Data is accepted by cloud only after the Verifier verifies the data uploaded.

## IV. IMPLEMENTATION OF IDENTITY - BASED DISTRIBUTED PROVABLE DATA POSSESSION PROTOCOL

During this step, the data owner's information is distributed to multi cloud servers. PKG - Private Key Generator generates the non-public key for the consumer which contains the consumer distinctive id. Data owner's information is transferred to combiner who distributes the information in line withthe block-tag pairs. Verifier sends the challenges to the Combiner who further transfers the challenge to the relevant cloud in line with the storage data. The cloud servers respond the challenge and then, Combiner aggregates the result and check whether it's valid or not. The ID-DPDP protocol is built by using the idea of signature and distributed computing. BLS scheme is used to generate the private key, which is further used to generate the signature. Furthermore, it shares the public parameters with the Verifier.

## V. IMPLEMENTATION OF BONEH-LYNN-SCACHAM SIGNATURE SCHEME

In cryptography, the Boneh–Lynn–Shacham (BLS) signature scheme is used to verify that a signer is authentic by a user. The three functions are key generation, signing and verification.

1) Key Generation : The key generation algorithm selects a random integer 'x' in the interval [0, r − 1], which is a private key. By holding the private key, public key is published, $g^x$.
2) Signing : Given the private key 'x', and some message 'm', the signature is computed by hashing the bitstring 'm', as h=H(m). Output of the signature is, sigma =$h^x$.
3) Verification : Given a signature sigma and a public key $g^x$ , we verify that e(sigma ,g)=e(H(m),$g^x$).

performs multiple auditing tasks simultaneously, of which the principle is to aggregate all the signatures by different users on various data blocks into a single short one and to verify it for only once to reduce the communication cost in the verification process.

## VI. CONCLUSION

In multi-cloud place for storing, this paper offers fastened type to the ID-DPDP system style and safety style to be traced. The purpose of this paper is to provide an integrity auditing scheme with public verifiability, efficient data dynamics and fair disputes arbitration. We achieve this by designing arbitration protocols (ID-DPDP) which is used for splitting and storing the files, based on the idea of exchanging metadata signatures by using Boney-Lynn-Schacham signature scheme, which is used to generate the public parameters by randomly generated a private key within given interval. It performs multiple auditing tasks simultaneously, of which the principle is to aggregate all the signatures by different users on various data blocks into a single short one and to verify it for only once to reduce the communication cost in the verification process. Moreover, we would like to point out that no single method can achieve audits for all types of cloud data perfectly, just as no standard has a universal validity. Thus, it will be a new trend to design a more effective scheme, including different audit strategies for different

types of cloud data, which is also the direction for our future work.

**REFERENCE**


[1] H. Dewan and R. C. Hansdah. ″A Survey of Cloud Storage Facilities″, Proc. 7th IEEE World Congress on Services, pp. 224- 231, July 2011.

[2] K. Ren, C. Wang and Q. Wang. "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 6973, 2012.

[3] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell. ″Cloud Security Auditing: Challenges and Emerging Approaches″, IEEE Security & Privacy, vol. 12, no. 6, pp. 68- 74, 2014.

[4] C. Wang, K. Ren, W. Lou and J. Li. ″Toward Publicly Auditable Secure Cloud Data Storage Services″, IEEE network, vol. 24, no. 4, pp. 19- 24, 2010.

[5] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li. ''Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,'' IEEE Trans. on Parallel and Distributed Systems, vol.22, no. 5, pp. 847- 859, 2011.

[6] F. Sebé, J. Domingo- Ferrer, A. Martínez- Ballesté, Y. Deswarte and J.- J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans.Knowledge Data Eng., vol. 20, no. 8, pp. 1034- 1038, 2008.

[7] G. Ateniese, R.B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, ''Provable Data Possession at Untrusted Stores,'' Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), pp. 598- 609, 2007.

[8] 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

[9] C. Wang, Q. Wang, K. Ren and W. Lou, ''Privacy- Preserving Public Auditing for Data Storage Security in Cloud Computing,'' Proc. IEEE INFOCOM, pp. 1- 9, 2010.

[10] C. Wang, S. M. Chow, Q. Wang, K. Ren and W. Lou, ″Privacy- Preserving Public Auditing for Secure Cloud Storage,″ IEEE Trans. on Computers, vol. 62, no. 2, pp. 362- 375, 2013.

[11] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi- Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231- 2244, 2012.

[12] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. on Parallel and Distributed Systems, vol. 24, no. 9, pp.1717- 1726, 2013.

[13] C. C. Erway, A. Küpçü, C. Papamanthou and R. Tamassia."Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security, pp. 213- 222, 2009.

[14] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu and S. S.Yau, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Trans. on Services Computing, vol. 6, no. 2, pp. 227–238, 2013.