A Cryptographic Model for Supervised Data Service in Multi-Cloud Storage

K. Vijay Krupa Vatsal[1], Aarepu Lakshman[2]
[1,2]*Assistant Professor, Department of Computer Science and Engineering*
[1,2]*Malla Reddy Engineering College (A), Maisammaguda, Hyderabad, Telangana, India.*

Abstract

In today cloud storage service is very faster profit growth by providing its features for client's data. Security preservation and data integrity is main issues faced by single cloud service users. Present client stores his data on multi-cloud servers and distributed storage and integrity checking are indispensable. In multi-cloud data distributed provable data possession is main element to secure the remote data. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. Proposed system is providing security verification, delegated verification as well as public verification. The method achieves batch auditing in large data auditing tasks from users is performed simultaneously by the TPA by splitting them into batches. Batch auditing is TPA may concurrently handle number of auditing upon different user's delegation. We uses AES method for cryptographic to reduce the memory size using variable length and verification based on hashing algorithm. Cloud service users are semi honest server so attacker can easily attack data. The scheme achieves batch auditing is large amount of data auditing tasks from users can be performed simultaneously by the TPA by splitting them into batches.

Index Terms: *Cloud computing, Provable data possession, Data Integrity Checking, zero-knowledge, cryptography, Encryption , AES algorithm.*

1. Introduction

The cloud computing facilitates many straight benefits to clients as on demand service, location independence, elasticity, network-based model, resource pooling and so on [1]. The cloud storage provisioning is one of the important services of cloud computing. The cloud storage facilitates massive amount of data storage which magnetize small and medium scale organizations to utilize remote storage for efficient and economic storage management [2]. It is a model of data storage where the data is stored in logical pool, the physical storage spans multiple servers and the physical environment is owned and managed by a hosting entity. The tasks like keeping the data available and accessible, and the physical environment protected, and running is done by cloud storage providers [3]. The cloud provides server-based applications and all data services to the user, with output displayed on the client device. Memory allocated to the client system's web browser is used to make the application data appear on the client system display, but all computations and changes are recorded by the server, and results including files created or altered are permanently stored on the cloud servers. Performance of the cloud application is dependent upon the network access, speed and reliability as well as the processing speed of the client device. While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards user's outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is relinquishing user's ultimate control over the fate of their data [4]. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity [5-7]. Second, for the benefits of their own, there do exist various motivations for cloud service providers to behave

unfaithfully towards the cloud users regarding the status of their outsourced data These problems, impedes the successful deployment of the cloud architecture.

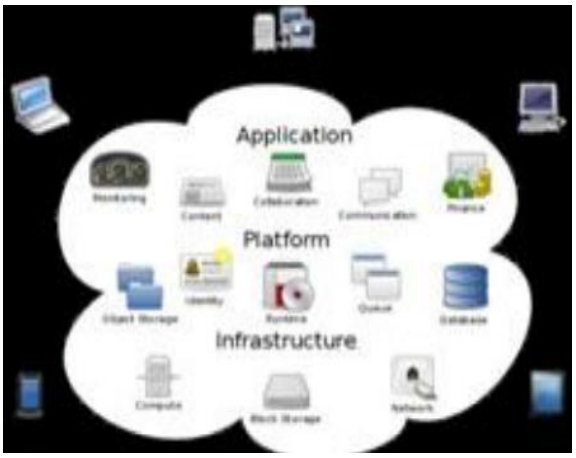


Figure 1. Cloud Computing

2. Related Work

In cloud computing, remote data integrity checking is an important security problem. The clients' massive data is outside his control. The malicious cloud server may corrupt the client's data in order to gain more benefits. Many researchers proposed the corresponding system model and security model. The verifier only maintains small metadata to perform the integrity checking. PDP is an interesting remote data integrity checking model. In 2012, Wang proposed the security model and concrete scheme of proxy PDP in public clouds [8]. At the same time, Zhu proposed the cooperative PDP in the multi-cloud storage. Many remote data integrities checking models and protocols have been proposed are as follows [8], [9], [10], In 2008, Sachem presented the first proof of irretrievability (POR) scheme with provable security [11]. In POR, the verifier can check the remote data integrity and retrieve the remote data at any time. On some cases, the client may delegate the remote data integrity checking task to the third party. One of benefits of cloud storage is to enable universal data access within dependent geographical locations. This implies that the end devices may be mobile and limited in computation and storage. Efficient integrity checking protocols are more suitable for cloud clients equipped with mobile end devices [12]. the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. After that, proposed dynamic PDP model and concrete scheme although it does not support insert operation. In order to support the insert operation, in 2009, Erway proposed a full-dynamic PDP scheme based on the authenticated flip table [13]. The similar work has also been done PDP allows a verifier to verify the remote data integrity without retrieving or downloading the whole data. It is a probabilistic proof of possession by sampling random set of blocks from the server, which drastically reduces I/O costs.

3. System Architecture

In the cloud paradigm, clients can be relieved from the burden of storage and computation by putting the large data files on the remote cloud servers. As the clients no longer possess their data locally, it is of critical importance for them to ensure that their data are being correctly stored and will not get altered or damaged. That is, clients should be equipped with efficient security means so that they can periodically verify the correctness of the remote data even with no existence of local copies [14]. A public auditing scheme consists of four algorithms KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification

metadata, which may consist of MAC, signatures, or other related information that will be used for auditing. GenProof is run by the cloud server to generate a proof of data storage correctness. VerifyProof is run by the TPA to audit the proof from the cloud server. Running a public auditing system consists of two phases, Setup and Audit. The user initializes the public and secret parameters of the system by executing KeyGen and pre-processes the data file F by using SigGen to generate the verification metadata. The user stores the data file F and the verification metadata at the cloud server and deletes its local copy [15]. As part of pre-processing, the user may alter the data file F by expanding it or including additional metadata to be stored at server. The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message from a function of the stored data file F and its verification metadata by executing GenProof. The TPA then verifies the response via Verify Proof [16].

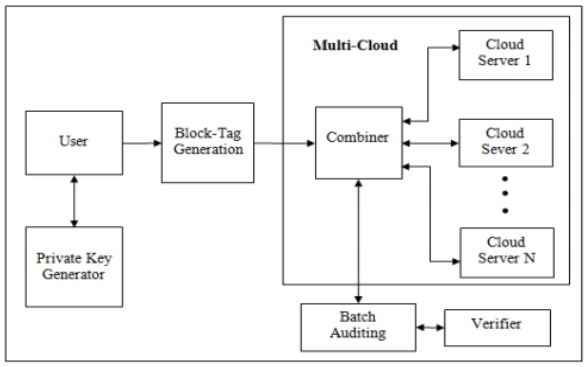


Figure 2. TPA verifies

4. Proposed System

The proposed scheme is extended to support scalable and efficient public auditing in Cloud Computing. The scheme achieves batch auditing where large data auditing tasks from users can be performed simultaneously by the TPA by splitting them into batches. Batch auditing is TPA may concurrently handle multiple auditing upon different user's delegation. This work addresses the construction in an efficient PDP scheme for sharing cloud storage to take data migration and security service, we consider the privies models different cloud service users to cooperatively store and maintain the user data. It presents a cooperative PDP (CPDP) model is homomorphism checking response and hash index hierarchy. Different users zero knowledge id model. The model is used to prove the security model. Which can satisfy knowledge different completeness and zero knowledge models.

4.1. Architecture Diagram

Multi cloud server having a greater number of private clouds and multi clouds User or owner can upload file to multi cloud or download file from multi cloud. TTP giving security to uploading and downloading files After receiving request from user or owner, TTP only verify that file whether accept or not and having more challenges and response of multi cloud storing files. Combiner or divider is used to secure the file from semi honest attacker. Uploading and downloading files stored into a greater number of blocks in multi cloud. While uploading divider concept id used and downloading combiner concept is used. deal with the construction of a well-organized PDP scheme for multi cloud storage and many items identity known as item-based attacker and set baser attacker. Shared data flow process (uploading and downloading) performed between user or owner and multi cloud.

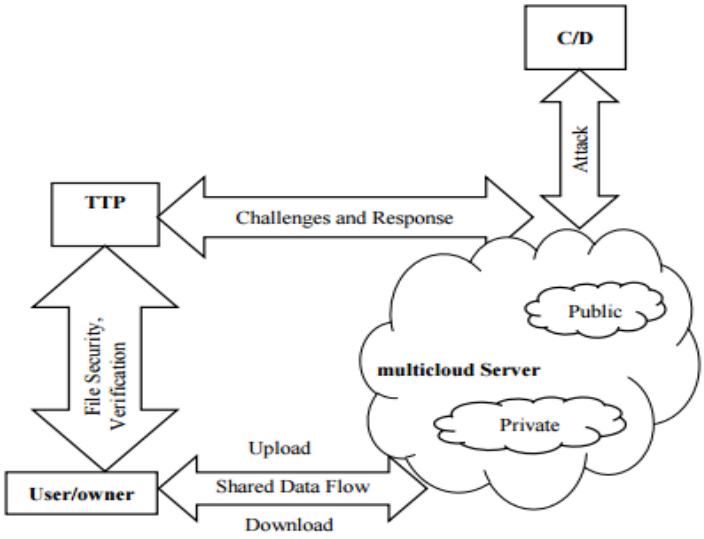


Figure 3. Architecture Diagram

4.2. Hash index hierarchy

To support distributed cloud storage, architecture used in cooperative PDP scheme as shown in our structure has a hierarchy structure which resembles a natural representation of file storage. This structure consists of three layers to represent relationships among all blocks for stored resources. This hierarchy structure and layers are described as follows.

1) Express Layer: This layer offers an abstract representation of the stored resources;

2) Service Layer: This layer offers and manages cloud storage services;

3) Storage Layer: This layer represents data storage on many physical devices

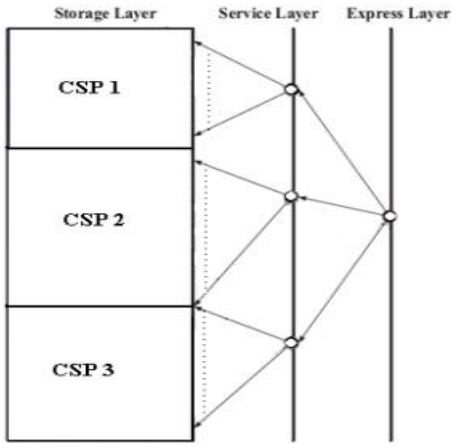


Figure 4. Hash index hierarchy

4.3. Security Analysis

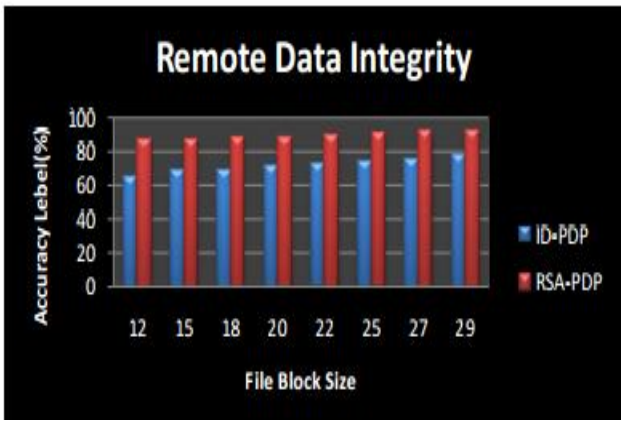
Multi-Prove zero-knowledge proof system is directly used for security, which satisfies following properties:

1. Collision resistant for index-hash hierarchy: The index hash hierarchy in CPDP scheme is collision resistant even if the client generates files with the same file name and cloud name collision doesn't occur there.

2. Completeness property of verification: In this scheme, the completeness property implies public verifiability property. Due to this property allows client as well as anyone other than client (data owner) can challenge the cloud server for data integrity and data ownership without the need for any secret information.
3. Zero-knowledge property of verification: This paper makes use of the zero-knowledge property to preserve the privacy of data blocks and signature tags. Initially, randomness is adopted into the CSPs' responses in order to resist the data leakage attacks.
4. Knowledge soundness of verification: The soundness means that it is infeasible to fool the verifier to accept false statements. Often, the soundness can also be considered as a stricter notion of unforge ability for file tags to avoid cheating the ownership. This denotes that the CSPs, even if collusion is tried, cannot be tampered with the data or forge the data tags if the soundness property holds. Thus, CPDP scheme can resist the tag forgery attacks to avoid cheating the CSPs' owner ship.

5. Results and Discussion

Uploading data are stored into number of blocks in multi cloud. If the uploading data are larger that splitting into a greater number of blocks while combining and dividing large data, the accuracy level more high. These combiner and divider is used to secure data from semi honest attacker



6. Conclusion

Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, ID-DPDP protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency to enhance identity-based provable data possession is more striking and as a result, more advantageous to learn. Based on client's approval, projected procedure can recognize private verification, delegated verification as well as public confirmation. Distributed computing is normally utilized to build up client information above multi-cloud servers.

7. Future Work

The proposed protocol can be extended to work on secure data sharing. The client can set access control policy for the data's they are uploading on multi cloud servers. When any other user tries to access the client's, data means they can access only if the user has the access rights to that data. These access rights can be designed by the client

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, "Provable Data Possession at Untrusted Stores", CCS'07, pp. 598-609, 2007.

[2] Wang H., "Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage", Services Computing, IEEE Transactions 2014

[3] Huaqun Wang, Qianhong Wu, Bo Qin , Domingo-Ferrer, J., "Identity-based remote data possession checking in public clouds", Information Security,

[4] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", SecureComm 2008, 2008.

[5] Amazon.com, "Amazon s3 availability event: July 20, 2008,".

[6] S. Wilson,"Application engine outage,"Online- http:// www.cio-weblog.com/50226711/appengineoutage. php, June 2008.

[7] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices washingtonpost.com/ securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[8] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", CCS'10, pp. 756-758, 2010.

[9] R. Curtmola, O. Khan, R. Burns, G. Ateniese, "MRPDP: Multiple-Replica Provable Data Possession", ICDCS'08, pp. 411-420, 2008.

[10] A. F. Barsoum, M. A. Hasan, "Provable Possessionand Replication of Data over Cloud Servers", CACR,University of Waterloo, Report2010/32,2010.

[11] Amazon.com, "Amazon s3 availability event: July 20, 2008,"

[12] K. D. Bowers, A. Juels, A. Oprea, "Proofs of Retrievability: Theory and Implementation", CCSW'09, pp. 43-54, 2009.

[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,D. Song, "Provable Data Possession at Untrusted Stores", CCS'07, pp.598-609, 2007.

[14] A. F. Barsoum, M. A. Hasan, "On Verifying Dynamic Multiple Data Copies over Cloud Servers", IACR eprint report 447, 2011.

[15] G. Ateniese, R. DiPietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession", Secure Comm, 2008.

[16] F. Sebe, J. Domingo-Ferrer, A. Martınez-Ballest, Y.Deswarte, and J.Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures", IEEE Transactions on Knowledge and Data Engineering, Vol.20, No.8, pp.1-6, 2008.

