Remote Data Integrity Checking System Using Client's Authorization in Cloud

V.Akhila Reddy¹, G.Rakesh Reddy²

¹,²Assistant Professor, Department of CSE, Jaya Prakash Narayan College of Engineering, JNTUH, India

Abstract: Cloud storage allows cloud users to enjoy the on-demand high quality data storage services without the burden of local data storage and maintenance. However, the cloud servers are not necessarily fully trusted. Cloud computing has become an important thing in computer field. Cloud computing takes information processing as a service, such as storage and computing. Data integrity is important thing in cloud storage. In certain situations, clients should store their data such as image or text in multi cloud. When the client stores his/her data on multi cloud servers, the distributed storage and integrity checking is very important. Here we propose an Identity Based Distributed Provable Data Possession (ID-DPDP) protocol for multi-cloud storage. Remote data integrity checking is important in cloud storage. It can make the clients verify whether their data is kept as it is without downloading the entire data.

Keywords: Cloud Storage, Data Possession Checking, Homomorphic Hash Function, Dynamic Operations

I. INTRODUCTION

By dealing with a high-quality variety of disbursed computing sources in Internet, it possesses big virtualized computing potential and storage area[1]. Thus, cloud computing is widely popular and utilized in many actual programs[2]. As an vital provider for cloud computing, cloud provider company components dependable, scalable, and low-cost outsourced storage service to the customers. It affords the customers with a more flexible way referred to as pay-as-you-cross model to get computation and garage assets on-demand. Under this version, the users can rent essential IT infrastructures according to their requirement rather than buy them. Thus, the up-front investment of the users might be reduced greatly. In addition, it is convenient for them to modify the potential of the ventured resource whilst the dimensions of their programs adjustments. Cloud service provider attempts to offer a promising provider for information storage, which saves the customers fees of funding and useful resource. Nonetheless, cloud garage also brings diverse security issues for the outsourced facts. Although a few safety issues were solved[3-10], the important demanding situations of records tampering and records lost are still existing in cloud storage. On the only hand, the twist of fate disk error or hardware failure of the cloud storage server (CSS) may additionally reason the sudden corruption of outsourced documents. On the alternative hand, the CSS is now not fully sincere from the perspective of the information owner, it can also actively delete or modify documents for excellent economic blessings. At the same time, CSS can also conceal the misbehaviors and information loss injuries from records owner to maintain a good reputation. Therefore, it is essential for the statistics owner to make use of an green way to test the integrity for outsourced facts.

Remote facts ownership checking (RDPC) [11] is an effective approach to ensure the integrity for data documents stored on CSS. RDPC substances a technique for records proprietor to effectively confirm whether or not cloud carrier provider faithfully stores the unique files with out retrieving it. In RDPC, the information owner is able to undertaking the CSS at the integrity for the goal record. The CSS can
generate proofs to show that it keeps the entire and uncorrupted facts. The fundamental requirement is that the facts owner can carry out the verification of document integrity without having access to the whole unique record. Moreover, the protocol ought to resist the malicious server which attempts to affirm the facts integrity with out getting access to the entire and uncorrupted data [12].

II. RELATED WORK

A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up.

Ateniese et al. [6] were the first who defined the “provable data possession” (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilizes the RSA-based homomorphic authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor.

In their subsequent work, Ateniese et al. [10] described a PDP scheme that uses only symmetric key based cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not provide data availability guarantee against server failures, leaving both the distributed scenario and data error recovery issue unexplored. The explicit support of data dynamics has further been studied in the two recent works [11] and [12].

Schwarz et al. [13] proposed to ensure static file integrity across multiple distributed servers, using erasure-coding and block-level file integrity checks. Some ideas of their distributed storage verification protocol are being adopted. However, the scheme further support data dynamics and explicitly studies the problem of misbehaving server identification, while theirs did not.

V. Zhuo Hao et al. [14] proposed the remote data integrity checking protocol that supports public verifiability without the support of TPA and compared the properties of the proposed protocol with the then existing protocols. VI. Wang et al. [15] in their work proposed a flexible distributed cloud storage integrity auditing mechanism utilizing the homomorphic token and distributed erasure coded data that detects the Byzantine failure, malicious data modification attack and server clouding attacks.

All the above schemes provide efficient methods for secured data verifiability, data storage integrity and detection of server attacks in the cloud based storage separately with an idea proposed for file retrieval and error recovery. In this paper the proposed Seb’ et al’s protocol combines the mentioned characteristic functions togethersmaking it more efficient and secured when compared to other protocols.

Provable Data Possession (PDP) is one such scheme proposed in this scheme ensures that the data integrity is not lost. However, this scheme needs the users to download data for verification which causes security problem again. Therefore it is essential to have a scheme where data downloading is not required for verification. Towards this end PDP scheme such as Scalable PDP and Dynamic PDP came into existence. These schemes focused on single cloud storage providers. There are schemes like SPDP, DPDP and Merkle Hash Tree (MHT) make use of authenticated skip list in order to verify the adjacent blocks for integrity. These schemes do not work in multi-cloud environments as they can’t construct MHT for such environment. The
otherschemes such as CPOR and PDP make use of homomorphic verification tags where downloading data for verification is not required.

A. Multi cloud storage: Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer’s processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks. The cloud user uploadsthe data into multi cloud. Cloud computing environment is constructed based on open architectures and interfaces; it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud. A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

B. Data Integrity: Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence ingeneral. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

III. PROPOSED WORK

Remote data integrity checking is of crucial importance in cloud storage. In multi-cloud environment, distributed provable data possession is an important element to secure the remote data. We propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie Hellman) problem. The proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

The ID-PDP framework model and security definition are given in this area. An ID-PDP convention contains four very surprising substances. We have a tendency to depict them beneath:

Client: AN element, that has expansive information to be put away on the multi-cloud for upkeep and processing, maybe either singular customer or partnership.

CS (Cloud Server): AN element that is overseen by cloud administration supplier has imperative space for putting away and processing asset to deal with the customers’ data.

Combiner: AN element, that gets the capacity ask for and disseminates the piece label sets to the comparing cloud servers. When getting the test, it parts the test and disseminates them to the different cloud servers. When accepting the reactions from the cloud servers, it joins them and sends the joined reaction to the hero.

PKG (Private Key Generator): A substance, once getting the character, it yields the relating non-open key.

In identity-based public key cryptography, this paper focuses on distributed provable data possession in multycloud storage. The protocol can be made efficient by eliminating the certificate management. We propose the new remote data integrity checking model: IDDPDP. The system model and security
model are formally proposed. Then, based on the bilinear pairings, the concrete ID-DPDP protocol is designed. In the random oracle model, our IDDPDP protocol is provably secure. On the other hand, our protocol is more flexible besides the high efficiency. Based on the client’s authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.

IV. CONCLUSION

In this paper, we study the issue for integrity checking of datafiles outsourced to remote server and propose an efficient secure RDPC protocol with data dynamic. We presented the construction of an efficient PDP scheme for distributed cloud storage. Based on homomorphic verifiable response and hash Index hierarchy, we have proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero-knowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds.

REFERENCES


**BIO DATA**

V. Akhila Reddy, received M.Tech degree in Computer Science and Engineering from Jaya Prakash Narayan College of Engineering, JNTUH, India. Presently working as Assistant Professor in Jaya Prakash Narayan College of Engineering, JNTUH, India.

G. Rakesh Reddy, (Ph.D.) Research Scholar in in Computer Science and Engineering at JNTUH and currently working as Assistant Professor in Jaya Prakash Narayan College of Engineering, JNTUH, India.