International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Remote Data IntegrityChecking System Using Client's Authorizationin Cloud

V.Akhila Reddy[1], G.Rakesh Reddy[2]
[1,2]*Assistant Professor,Department of CSE, Jaya Prakash Narayan College of Engineering,JNTUH,India*

Abstract: Cloud storage allows cloud users to enjoy the on-demandand high quality data storage services without the burden of local datastorage and maintenance. However, the cloud servers are not necessarilyfully trusted.Cloudcomputing has become an important thing in computer field.Cloud computing takes information processing as a service,such as storage and computing. Data integrity is importantthing in cloud storage. In certain situations, clients should storetheir data such as image or text in multi cloud. When the clientstores his/her data on multicloud servers, the distributedstorage and integrity checking is very important. Here wepropose an Identity Based Distributed Provable Data Possession(ID-DPDP) protocol for multi-cloud storage. Remote dataintegrity checking is important in cloud storage. It can make theclients verify whether their data is kept as it is withoutdownloading the entire data.

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

I. INTRODUCTION

By dealing with a high-qualityvariety of disbursed computing sources in Internet, itpossesses big virtualized computing potential and storage area[1]. Thus, cloud computing is widely popular and utilized inmany actual programs [2]. As an vital provider for cloudcomputing, cloud provider company components dependable, scalable,and low-cost outsourced storage service to the customers. It affordsthe customers with a more flexible way referred to as pay-as-you-cross modelto get computation and garage assets on-demand. Underthis version, the users can rent essential IT infrastructures according to their requirement rather than buy them. Thus, theup-front investment of the users might be reduced greatly. Inaddition, it is convenient for them to modify the potential of therented resource whilst the dimensions of their programs adjustments.Cloud service provider attempts to offer a promising providerfor information storage, which saves the customers fees of funding anduseful resource. Nonetheless, cloud garage also brings diversesecurity issues for the outsourced facts. Although a few safetyissues were solved [3-10], the important demanding situations ofrecords tampering and records lost are still existing in cloud storage.On the only hand, the twist of fate disk error or hardware failure ofthe cloud storage server (CSS) may additionally reason the suddencorruption of outsourced documents. On the alternative hand, the CSS isnow not fully sincere from the perspective of the information owner, itcan also actively delete or modify documents for excellent economicblessings. At the same time, CSS can also conceal the misbehaviors andinformation loss injuries from records owner to maintain a goodreputation. Therefore, it is essential for the statistics owner to make use ofan green way to test the integrity for outsourced facts.

Remote facts ownership checking (RDPC) [11] is aneffective approach to ensure the integrity for data documents storedon CSS. RDPC substances a technique for records proprietor to effectivelyconfirm whether or not cloud carrier provider faithfully stores theunique files with out retrieving it. In RDPC, the information owner isable to undertaking the CSS at the integrity for the goal record. TheCSS can

generate proofs to show that it keeps the entire anduncorrupted facts. The fundamental requirement is that the factsowner can carry out the verification of document integrity withouthaving access to the whole unique record. Moreover, the protocolought to resist the malicious server which attempts to affirm thefacts integrity with out getting access to the entire and uncorrupteddata [12].

II. RELATED WORK

A Novel Efficient Remote Data PossessionChecking Protocol in Cloud Storagefor 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 offile on untrusted storages. . Their scheme utilizes the RSA-based homomorphic authenticators for auditing outsourceddata and suggests randomly sampling a few blocks of the file. However, the public auditability in their schemedemands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol isnot 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 basedcryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions andappends to the stored file, which has also been supported in our work. However, their scheme focuses on single serverscenario and does not provide data availability guarantee against server failures, leaving both the distributed scenarioand data error recovery issue unexplored. The explicit support of data dynamics has further been studied in the tworecent works [11] and [12].

Schwarz et al. [13] proposed to ensure static file integrity across multiple distributed servers, using erasure-coding andblock-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 serveridentification, while theirs did not.

V. Zhuo Hao et.al [14] proposed the remote data integrity checking protocol that supports public verifiability without thesupport 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 thehomomorphic token and distributed erasure coded data that detects the Byzantine failure, malicious data modificationattack 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 errorrecovery. In this paper the proposed Seb'e et al's protocol combines the mentioned characteristic functions togethermaking it more efficient and secured when compared to other protocols.

Provable Data Possession (PDP) is one such schemeproposed in this scheme ensures that the data integrity is notlost. However, this scheme needs the users to download datafor verification which causes security problem again.Therefore it is essential to have a scheme where datadownloading is not required for verification. Towards thisend PDP scheme such as Scalable PDP and Dynamic PDPcame into existence. These schemes focused on single cloudstorage providers. There are schemes like SPDP, DPDP andMerkle Hash Tree (MHT) make use of authenticated skip listin order to verify the adjacent blocks for integrity. Theseschemes do not work in multi-cloud environments as theycan't construct MHT for such environment. The

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

otherschemes such as CPOR and PDP make use of homomorphicverification tags where downloading data for verification isnot required.

A. Multi cloud storage: Distributed computing is used to refer to any largecollaboration in which many individual personal computerowners allow some of their computer's processing time to beput at the service of a large problem. In our system the eachcloud admin consist of data blocks. The cloud user uploadsthe data into multi cloud. Cloud computing environment isconstructed based on open architectures and interfaces; it hasthe capability to incorporate multiple internal and/or externalcloud services together to provide high interoperability. Wecall such a distributed cloud environment as a multi-Cloud .Amulti-cloud allows clients to easily access his/her resourcesremotely through interfaces.

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

III. PROPOSED WORK

Remote data integrity checking is of crucial importance incloud storage. In multi-cloud environment, distributedprovable data possession is an important element to securethe remote data. we propose a novel remote data integritychecking model: ID-DPDP (identity-based distributedprovable data possession) in multi-cloud storage. Theproposed ID-DPDP protocol is provably secure under thehardness assumption of the standard CDH (computationalDiffi Hellman) problem. The proposed ID-DPDP protocolcan realize private verification, delegated verification andpublic verification.

The ID-PDP framework model and security definition aregiven in this area. AN ID-PDP convention contains four verysurprising substances. We have a tendency to depict thembeneath:

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

CS (Cloud Server): AN element that is overseen by cloudadministration supplier has imperative space for putting awayand processing asset to deal with the customers' data.

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

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

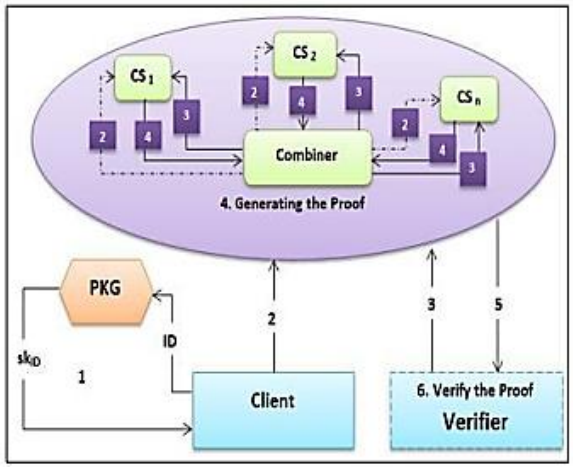

Fig.1 IDPDP protocol

In identity-based public key cryptography, this paper focuses on distributed provable data possession in multicloud storage. The protocol can be made efficient byeliminating the certificate management. We propose the newremote data integrity checking model: IDDPDP. The systemmodel and security

model are formally proposed. Then,based on the bilinear pairings, the concrete ID-DPDPprotocol is designed. In the random oracle model, our IDDPDP protocol is provably secure. On the other hand, ourprotocol is more flexible besides the high efficiency. Basedon the client's authorization, the proposed ID-DPDP protocolcan realize private verification, delegated verification andpublic verification.

IV. CONCLUSION

In this paper, we study the issue for integrity checking of datafiles outsourced to remote server and propose an efficientsecure RDPC protocol with data dynamic. We presented the construction of an efficient PDP schemefor distributed cloud storage. Based on homomorphicverifiable response and hash Index hierarchy, we haveproposed a cooperative PDP scheme to support dynamicscalability on multiple storage servers. We also showed thatour scheme provided all security properties required by zeroknowledge interactive proof system, so that it can resistvarious attacks even if it is deployed as a public audit servicein clouds

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloudcomputing and emerging IT platforms: Vision, hype, and reality fordelivering computing as the 5th utility," Future Gener. Comp. Sy., vol.25, no. 6, pp. 599 – 616, 2009.

[2] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy preserving personal healthrecord using multi-authority attribute-based encryption withrevocation," Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

[3] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Flexible and fine-grainedattribute-based data storage in cloud computing," IEEE Trans. ServiceComput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourcedattribute-based encryption with keyword search function for cloudstorage," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2542813.

[5] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policyattribute-based encryption with revocation in cloud storage," Int. J.Commun. Syst., DOI: 10.1002/dac.2942.

[6] J.G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving DecentralizedKey-Policy Attribute-Based Encryption," IEEE Transactions on Parallel andDistributed Systems, vol. 23, no.11, pp. 2150-2162, 2012

[7] Z. J. Fu, X. M. Sun, Q. Liu, L. Zhou, and J. G. Shu, "Achieving efficientcloud search services: multi-keyword ranked search over encryptedcloud data supporting parallel computing," IEICE Transactions onCommunications, vol. E98-B, no. 1, pp.190-200, 2015.

[8] Z. J. Fu, K. Ren, J. G. Shu, X. M. Sun, and F. X. Huang, "Enablingpersonalized search over encrypted outsourced data with efficiencyimprovement," IEEE Transactions on Parallel and Distributed Systems,DOI: 10.1109/TPDS.2015.2506573, 2015.

[9] Z. H. Xia, X. H. Wang, X. M. Sun, and Q. Wang, "A secure anddynamic multi-keyword ranked search scheme over encrypted clouddata," IEEE Transactions on Parallel and Distributed Systems, vol. 27,no. 2, pp. 340-352, 2015.

[10] Y. J. Ren, J. Shen, J. Wang, J. Han and S. Y. Lee, "Mutual verifiableprovable data auditing in public cloud storage," Journal of InternetTechnology, vol. 16, no. 2, pp. 317-323, 2015.

[11] Y. Deswarte, J. J. Quisquater, and A. Saïdane, "Remote integritychecking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst.(IICIS), 2003, pp. 1–11.

[12] Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote dataintegrity checking protocol with data dynamics and public verifiability,"IEEE Trans. Knowl. Data Eng., vol. 23, no. 9, pp. 1432–1437, Sep.2011.

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

[14] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, ''Scalable andfficient Provable Data Possession,'' in Proc. 4th Int'l Conf. Securityand Privacy in Commun. Netw. (SecureComm), 2008, pp. 1-10.

[15] F. Sebé, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J.Quisquater, "Efficient Remote Data Possession Checking in CriticalInformation Infrastructures," IEEE Trans. Knowledge and Data Eng.,vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

BIODATA

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.