Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 5, May 2018, pg.1 – 4

AN ENHANCED DATA CONTROLLING METHOD IN CLOUD

Asmitha S E
Computer Science and Engineering, SDIT, VTU, India
asmihashek@gmail.com

Abstract- Cloud computing is very widely used. Cloud storage is scalable flexible and gives high quality data storage and services. The data owners can upload their files to the cloud .But this cannot trust completely. The data owners want to make sure that their file didn't outsourced to cloud remote servers for alterations. As a solution to this problem RDPC (remote data possession checking) protocol has been used. This paper presents a new RDPC which is more efficient and it is based on homomorphic hash function. This will prevent attacks like forgery, replace, and replay based on security model. ORT (operation record table) is for tracking all the operations of every file block. The ORT accessing cost will be approximately constant. The overall performance analysis will give idea about computational and communication costs. This scheme is very much feasible for the real time applications.

Keywords – RDPC, Cloud computing, CSS, Hash tag, data possession and operation record table.

I. INTRODUCTION

Cloud computing appear as novel computing prototype following grid computing. It manages several number of computing resources through internet and possesses very huge computing ability and even storage space so that cloud is widely accepted and also used for real applications important service of cloud is the service provider provides reliable flexible scalable and low cost service to the user [1]. It has pay-as-you-go model so the computation and resources will be accessible on demand and it is very flexible and also provides rending option of IT infrastructures according to the user requirement instead of buying them, so that the investment of user will be minimized [2]. According to the application changes of the user the rented resource capacity can be adjustable

The cloud service provider make sure about the service of data storage and it will save the investment and the cost of resources cloud storage cannot be trusted completely there can be several security problems for the data which is outsourced. Some security issues have been solved yet [3-10]. But still issues exist like data tampering, data modifying and data loss the unexpected hardware failure causes corruption of outsourced data files in cloud storage server (CSS). For incredible economic advantages the files will get actively modify or delete so the cloud storage server cannot trust fully. And also CSS will try to hide the issues like data loss and misbehaviors from the data owner with the intention of keeping good reputation. Therefore, the integrity checking for the outsourced data for the data owner comes crucial.

In this paper introduces an effective method for ensuring the integrity of outsourced data files which is stored on CSS that is remote data possession checking (RDPC) [11]. RDPC provides method for the owner of the data to verify the integrity of the files which is stored in cloud. RDPC challenges CSS about the integrity of target file [12]. It is based on the proof which is created by CSS and it is used to prove that the data files are uncorrupted. The data owner does not need to access the full data file for integrity checking, it can be done by using the proof .The data owner can apply any changes to the uploaded file like insertion deletion and
Modifications required. All the operations will be supported by the RDPC protocol. For the real applications the communications will be complex.

The uploaded file of the data owner will be divided in to some blocks an each block has its own hash code. If any misbehaviour happened to the file so that the owner can come to know by comparing with the hash code.ORT keeps every operation table which is used for make sure the integrity of file. Data owner challenge the CSS about the integrity the CSS can return the proof generated to the owner, so the proof can be verified. Challenge is denoted by *C* proof is *P* and *A* generates the proof. RDPC makes the cloud more trustful.

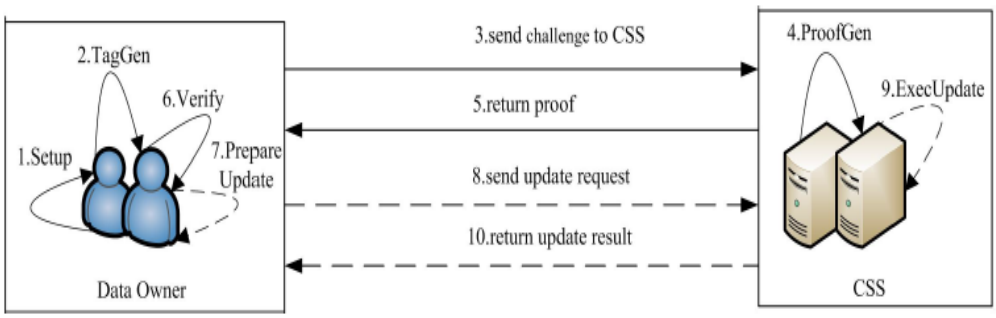
II. RELATED WORK

RDPC first proposed by Deswarte et al. [1] by using the RSA hash function the disadvantage of this is the entire file blocks will access for each challenge. Ateniese et al. [3] presented PDP (provable data possession) in 2007. In this model does not need to access the entire file blocks during integrity checking, and they proposed (S-PDP, E-PDP) schemes based on RSA. These schemes had great performance but the problem was they didn't include dynamic operations in 2008 they proposed dynamic PDP by using symmetric encryption [4]. It also has draw back that doesn't support block insert operation. There were several research works based on dynamic PDP protocols Sebe et al.[5] introduced a RDPC protocol large integer which supports data dynamics. Erway et al. [6] presented DPDP it is fully dynamic PDP with skip list so data owner can delete insert an update file blocks anytime.

Wang et al. [7] used MHT (Merkle hash tree) it is other method for data checking in which each node is leaf of MHT. Storing all the leaf notes from left to right MHT can identify the block position for dynamic operation. The MHT causes high computation cost. In 2013 Yang and jia [8] forwarded a scheme in which dynamic operations are supported by index table. By using this index table the logical location and the version number of each and every block for the outsourced file can be recorded. For delete and insert operation in one data block first the verifier will find the position of the block and next will shift the entries to insert or delete a row in the table, but problem is it has high computation cost.

III. SYSTEM DESIGN

A. Work procedure of RDPC protocol



In RDPC protocol two participants involved one is CSS and other one is data owner CSS has huge and powerful storage and also computation resources. Data owner send request to CSS for storing the data file and supply services. Data owner places several numbers of files to CSS without having backup copies CSS is not completely trustful according to circumstances it may misbehave like modification or deletion of data file portions. In these cases owner can verify the integrity very efficiently

- TagGen – Tags are generated using this algorithm and it is executed by data owner input is key *K*, sk is the private key file is *F*, Tag for output is *T* its is collection of several tags.
- Challenge – This algorithm used for generating challenge information input is challenged block c , output is challenge (*chal*)
- ProofGen- it is denoted by *P* this algorithm used for generating proof *P* Input is file *F*, output is proof *P*, Tag set is *T*, and challenge is *chal*.
- Verify-this algorithm is based on the proof returned by CSS that is *P*. using homomorphism key *K*, private key sk.if output is 1 then *P* is correct, otherwise wrong
- PrepareUpdate – this algorithm used for creating dynamic data operations on data blocks new file block is Fi, position of block is i, Ut is input that is update type URI is the request information for updating. UT has three options insert Delete and modify.
- ExecUpdate – It is for running update operation. URI is the input and execution result is the output. Returns success when update operation finished and if not returns fail.

Security requirements

Malicious behaviours occurs to CSS a hides the data corruption from the owner for good reputation. By [8] there are three types of attacks on RDPC forgery attack, reply attack, replace attack.

- Forgery attack: for a particular block CSS forges its valid tag and cheat the data owner.
- Reply attack: without accessing challenged block and its tag the CSS will use the previous proofs which are valid or other information for possession.
- Replace attack: instead of the challenged block CSS make use of other valid pair of blocks and tag as the proof of the actual challenged one it may interfered or discarded.

All the attacks above should resist by a secure RDPC protocol. RDPC guarantees that the owner can construct valid proof and the verification actually posses the entire file. [3, 9, 11] these three covers all the three attacks and capture the data possession. The challenger is indicated by C owner is A, the untrusted CSS shown below,

Setup. KeyGen algorithm is executed by *C* and gets homomorphic key *K* and private key *sk*. Both the keys are kept secretly.

Query. *A* can make two types of query with *C*.

- Tag query : A flexibly choosing data blocks and forwards to see for querying the tags *C* uses TagGen algorithm and gets valid tag for every block and returns the tags to *A*
- Proof verification query: *A* generates the proofs of data possession and sends the proof to C; tags have been queried for every block.Verify algorithm will run to check the proof validation and send the result to *A*.

Challenge: *C* will submit challenge *chal* to *A*, proof of data possession *P* will return to challenge blocks by *A*.

Forge: Proof P computes by *A*, and returns the results to *C*. if proof is correct *A* wins the game.

IV. IMPLIMENTATION

A. Hardware Requirements

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Color.
- RAM: 512 Mb.

B. Software Requirements

- Operating system: Windows XP/7.
- Coding Language: JAVA/J2EE
- IDE: NetBeans 8.1
- Database: MySQL

V. CONCLUSION

In this paper we are going through the problem of integrity of data files which is out sourced to server for this proposing an efficient and secure protocol that is RDPC includes data dynamics. To make sure the integrity of the files which is outsourced to remote server uses homomorphic hash function. This helps to reduce the cost of storage and cost of computation of the data owner.

This protocol works as the number of node shifting reduces maximum and with minimum computation cost introduces a design with light weight hybrid data structure which supports all the dynamic operations. Operations like insert delete and modification of blocks with efficiency can be performed by data owner by using this data structure. This model proved secure among the existing model. Here cost of community, computation, storage is minimum. The experimental results show that our protocol is practical in the cloud world.

ACKNOWLEDGEMENT

I would like to thank my institution and my guides for their constant support and guidance.

REFERENCES

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

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

[3] 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.

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

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

[6] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession,'' in Proc. 16th ACM Conf. on Comput. And Commun. Security (CCS), 2009, pp. 213-222.

[7] 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. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847-859, May, 2011.

[8] K. Yang and X. Jia, ''An efficient and secure dynamic auditing protocol for data storage in cloud computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717-1726, 2013.

[9] L. Chen, S. Zhou, X. Huang and L. Xu, ''Data dynamics possession checking in cloud storage, '' Comput.Electr f. oErnrge.m, ovtoel .d 3a9ta, no. 7, pp. 2413-2424, 2013.

[10] M. N. Krohn, M. J. Freedman and D. Mazieres, ''On-the-fly verification of rateless erasure codes for efficient content distribution,'' in Proc. 2004 IEEE Symp.on Security and Privacy (S&P), 2004, pp. 226–240.

[11] Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang and C. Xu, ''Improved security of a dynamic remote data possession checking protocol for cloud storage,'' Expert Syst. Appl., vol. 41, no. 7, pp. 7789-7796, 2014.

[12] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ''MR-PDP: Multiple-replica provable data possession'' in Proc. 28th IEEE Conf. on Distrib. Comput. Syst. (ICDCS), 2008, pp. 411-420.

