ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Novel Efficient Remote Data Possession Checking Protocol in Cloud

Donda Prabhu Dev
Department of Computer Science and Engineering,
SIMS College,
Guntur, Andhra Pradesh 522001, India.

B Mounika Chowdary
Department of Computer Science and Engineering,
SIMS College,
Guntur, Andhra Pradesh 522001, India.

ABSTRACT

As an important application in cloud computing, Cloud storage offers user scalable, flexible and high quality data storage and computation services. A growing number of data owners choose to outsource data files to the cloud. Because cloud storage servers are not fully trustworthy, data owners need dependable means to check the possession for their files outsourced to remote cloud servers. To address this crucial problem, some remote data possession checking (RDPC) protocols have been presented. But many existing schemes have vulnerabilities in efficiency or data dynamics. In this paper, we provide a new efficient RDPC protocol based on homomorphic hash function. The new scheme is provably secure against forgery attack, replace attack and replay attack based on a typical security model. To support data dynamics, an operation record table (ORT) is introduced to track operations on file blocks. We further give a new optimized implementation for the ORT which makes the cost of accessing ORT nearly constant. Moreover, we make the comprehensive performance analysis which shows that our scheme has advantages in computation and communication costs. Prototype implementation and experiments exhibit that the scheme is feasible for real applications.

Index Terms—Cloud Storage, Data Possession Checking, Homomorphic Hash Function, Dynamic Operations

INTRODUCTION

Cloud computing emerges as a novel computing paradigm subsequent to grid computing. By managing a great number of distributed computing resources in Internet, it possesses huge virtualized computing ability and storage space [1]. Thus, cloud computing is widely accepted and used in many real applications [2]. As an important service for cloud computing, cloud service provider supplies reliable, scalable, and low-cost outsourced storage service to the users. It provides the users with a more flexible way called pay-as-you-go model to get computation and storage resources on-demand. Under this model, the users can rent necessary IT infrastructuresaccording to their requirement rather than buy them. Thus, the up-front investment of the users will be reduced greatly. In addition, it is convenient for them to adjust the capacity of the rented resource while the scale of their applications changes. Cloud service provider tries to provide a promising service for data storage, which saves the users costs of investment and resource. Nonetheless, cloud storage also brings various security issues for the outsourced data. Although some security problems have been solved [3-10], the important challenges of data tampering and data lost are still existing in cloud storage. On the one hand, the accident disk error or hardware failure of the cloud storage server (CSS) may cause the unexpected corruption of outsourced files. On the other hand, the CSS is not fully trustworthy from the perspective of the data owner, it may actively delete or modify files for tremendous economic benefits. At the same time, CSS may hide the misbehaviors and data loss accidents from data owner to maintain a good reputation. Therefore, it is crucial for the data owner to utilize an efficient way to check the integrity for outsourced data. Remote data possession checking (RDPC) [11] is an effective technique to ensure the integrity for data files stored on

Cite this article as: Donda Prabhu Dev & B Mounika Chowdary, "Novel Efficient Remote Data Possession Checking Protocol in Cloud", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 7, 2019, Page 38-42.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CSS. RDPC supplies a method for data owner to efficiently verify whether cloud service provider faithfully stores the original files without retrieving it. In RDPC, the data owner is able to challenge the CSS on the integrity for the target file. The CSS can generate proofs to prove that it keeps the complete and uncorrupted data. The fundamental requirement is that the data owner can perform the verification of file integrity without accessing the complete original file. Moreover, the protocol must resist the malicious server which attempts to verify the data integrity without accessing the complete and uncorrupted data [12]. Another desired requirement is that dynamic data operations should be supported by the protocol. In general, the data owner may append, insert, delete or modify the file blocks as needed. Besides, the computing complexity and communication overhead of the protocol should be taken into account for real applications.

Related Work

The first RDPC was proposed by Deswarte et al. [11] based on RSA hash function. The drawback of this scheme is that it needs to access the entire file blocks for each challenge. In 2007, the provable data possession (PDP) model was presented by Ateniese et al. [13], which used the probabilistic proof technique for remote data integrity checking without accessing the whole file. In addition, they supplied two concrete schemes (S-PDP, E-PDP) based on RSA. Although these two protocolshad good performance, it's a pity they didn't support dynamic operations. To overcome this shortcoming, in 2008, they presented a dynamic PDP scheme by using symmetric encryption [14]. Nonetheless, this scheme still did not support block insert operation. At the same time, lots of research works [15-19] devoted to construct fully dynamic PDP protocols. For instance, Sebé et al. [15] provided a RDPC protocol for critical information infrastructures based on the problem to factor large integers, which is easily adapted to support data dynamics. Erway et al. [16] first presented a fully dynamic PDP scheme (DPDP) by using authenticated skip list, which allowed data owner to append, delete, insert and update file blocks at anytime. Wang et al. [17] used Merkle hash tree (MHT) to propose another dynamic method for remote data checking, in which each block was hashed to be a leaf node of MHT. By sorting all leaf nodes from left to right, the MHT implicitly identified the block position which is essential for dynamic operations. However, using MHT caused heavy computation cost. In 2013, Yang and Jia [18] presented an efficient scheme, in which an index table was utilized to support dynamic operations. By the index table, the data owner recorded the logical location and version number for each block for the outsourced file. However, to delete or insert one data block, the verifier had to find the position of the block and shift the remaining entries to insert or delete a row in the index table, which still incurred high computation cost. In [19], Chen et al. provided a dynamic RDPC scheme by using homomorphic hash function defined in [20]. Unfortunately, their scheme was proved insecure by Yu et al. [21]. To overcome the drawback, Yu et al. [21] presented a new RDPC protocol based on RDPC scheme in [19] and proved the security. They also used MHT to achieve data dynamic operations, which caused the same shortcoming of inefficient as in [17].

B. Motivation and Contribution It is essential for data owners to verify the integrity for the data stored on CSS before using it. For example, a big international trading company stores all the imports and exports record files on CSS. According to these files, the company can get the key information such as the logistics quantity, the trade volume etc. If any record file is discarded or tampered, the company will suffer from a big loss which may cause bad influence on its business and development. To avoid this kind of circumstances, it is mandatory to check the integrity for outsourced data files. Furthermore, since these files may refer to business secret, any information exposure is unacceptable. If the company competitor can execute the file integrity checking, by frequently checking the files they may obtain some useful information such as when the file changes, the growth rate of the file etc, by which they can guess the development of the company. Thus, to avoid this situation, we consider the private verification

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

type in our scheme, that is, the data owner is the unique verifier. In fact, the current research direction of RDPC focuses on the public verification, in which anyone can perform the task of file integrity checking with the system public key. Although RDPC with public verification seems better than that with private verification, but it is unsuitable to the scenario mentioned above. Motivated by the above application scenarios, we present a novel efficient RDPC scheme by using homomorphic hash function [20], which has been used to construct RDPC schemes [19,21]. Unfortunately, these schemes are either insecure or not efficient enough. To overcome these drawbacks, we refer to the idea of [35] and introduce a private key for each tag generation in our RDPC scheme. Simultaneously, a new construction of ORT is presented for data dynamic which can improve the efficiency of the protocol greatly. Compared with the previous ones, our scheme has better performance in term of computation and communication. Our contributions are summarized as follows: We present a novel efficient RDPC scheme with datafunction technique, in which the hash value of the sum for two blocks is equal to the product for two hash values of the corresponding blocks. We introduce a linear table called ORT to record data operations for supporting data dynamics such as block modification, block insertion and block deletion. To improve the efficiency for accessing ORT, we make use of doubly linked list and array to present an optimized implementation of ORT which reduces the cost to nearly constant level. We prove the presented scheme is secure against forgery attack, replay attack and replace attack based on a typical security model. At last we implement our scheme and make thorough comparison with previous schemes. Experiment results show that the new scheme has better performance and is practical for real applications.

PERFORMANCE ANALYSIS

The performance for the proposed scheme is evaluated in this section. We first compare our new scheme with other RDPC schemes in term efficiency. Then we show the experimental results for our new scheme.

Efficiency Evaluation

Our scheme is built on a secure homomorphic hash function and supports fully dynamic operations about blocks including insertion, deletion and modification. A new light weight data structure called ORT is adopted to realize dynamic operations. By introducing a novel optimized implementation of ORT, we reduce the cost of accessing ORT to nearly constant level. Meanwhile, our scheme has no restrictions on the verification times and challenged block numbers, which can be set freely by the data owners according to their requirements. To demonstrate the features of our scheme, we list the comprehensive efficiency comparison for our scheme with the state-of-the-art in Table1. Further, we will analyze the detailed cost of our RDPC scheme.

Computation cost:

Let T_{mul}, T_{exp},T_{prf},T_{prp} ,T_{hash},T_{add} denote the time cost for multiplication, modular exponentiation, pseudo-random number generation, permutation operation, hash operation and addition operation respectively. Setup algorithm runs on the data owner side, it is responsible for outputting homomorphic key and private key. The computation cost of Setup cannot be confirmed strictly because it is related to the means for generating big primes p, q and the vector g . Thus we are unable to give the specific theoretical values of the Setupcomputation cost, but we will show the real time spend in the experiment later, which can give us a more clear knowledge than the theoretical analysis. However, Setup will run only once in system. No matter how much time it costs, the influence on the computation overhead of the data owner is very little. Thus, we ignore the Setup cost in the following analysis about the computations cost for the data owner.

CONCLUSION

In this paper, we study the issue for integrity checking of data files outsourced to remote server and propose an efficient secure RDPC protocol with data dynamic. Our scheme employs a homomorphic hash function to verify the integrity for the files stored on remote server, and reduces the storage costs and computation costs of the data owner.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We design a new lightweight hybrid data structure to support dynamic operations on blocks which incurs minimum computation costs by decreasing the number of node shifting. Using our new data structure, the data owner can perform insert, modify or delete operation on file blocks with high efficiency. The presented scheme is proved secure in existing security model. We evaluate the performance in term of community cost, computation cost and storage cost. The experiments results indicate that our scheme is practical in cloud storage.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering 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 health record using multi-authority attribute-based encryption with revocation," 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-grained attribute-based data storage in cloud computing," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016. 2542813.

[5] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policy attribute-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 Decentralized Key-Policy Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed 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 efficient cloud search services: multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Transactions on Communications, 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, "Enabling personalized search over encrypted outsourced data with efficiency improvement," 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 and dynamic multi-keyword ranked search scheme over encrypted cloud data," 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 verifiable provable data auditing in public cloud storage," Journal of Internet Technology, vol. 16, no. 2, pp. 317-323, 2015.

[11] 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.

[12] 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.

[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. and Commun. Security (CCS), 2007, pp. 598-609.

[14] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, ''Scalable andEfficient Provable Data Possession,'' in Proc. 4th Int'l Conf. Security and 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[16] 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.

[17] 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.

[18] 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.

[19] L. Chen, S. Zhou, X. Huang and L. Xu, ''Data dynamics for remote data possession checking in cloud storage, '' Comput. Electr. Eng., vol. 39, no. 7, pp. 2413-2424, 2013.

[20] 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.

[21] 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.

[22] 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.

[23] Z. Hao and N. Yu, ''A multiple-replica remote data possession checking protocol with public verifiability,'' in Proc. 2th Int'l Symp. Data, Privacy, E-Comm. (ISDPE), 2010, pp. 84-89.

Author Details

Donda Prabhu Dev
MCA Student,
Reg No: 316233620003
SIMS College.

B Mounika Chowdary
M.Tech (CST),
Assistant Professor,
SIMS College.