IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Flexible and Secure Auditing of outsourced Database in Cloud Computing

Mr. Darshan T. Kavathekar[1], Mrs. B. S. Shetty[2]

M. Tech in Computer Science and Engineering (Specialization-Information Technology), WCE, Sangli, Shivaji University Kolhapur, India[1]

Assistant Professor, Walchand College of Engineering, Sangli, India[2]

Abstract: Now a days increasing number of enterprise outsource their IT services to third parties who can provides services for a lower cost due to economy of scale. The database management to cloud service provider that provides various database services to different users. For securing database outsourced to the cloud, it is important to allow cloud users to verify that their queries to the cloud –hosted database are correctly executed by the cloud. Existing solutions on that issue suffer from a high communication cost, a heavy storage overhead or an overwhelming computational cost on clients. In this paper, we propose a new auditing scheme for outsourced database, which can simultaneously achieve the correctness and completeness of search results. Furthermore, we can prove that our construction can achieve security properties even in the encrypted outsourced database. Our audit services can be extended to support dynamic database operations.

Keywords: Cloud computing, Audit service, Database encryption, Outsourcing computation.

I. INTRODUCTION

The cloud service provider (CSP) offers network services, infrastructure or business application in the cloud. The large benefit of using a cloud service provider comes efficiency and economic of scale. By outsourcing database to the cloud, cloud users enjoy data sharing and other benefits such as cost saving, on-demand self-service, resource elasticity, etc. In particular, users who request a query to database which is outsourced to the cloud may wonder whether or not their queries are always correctly executed by cloud servers. To set forth, clients need to verify the integrity and completeness of their queries over the outsourced database: for any query request, we need to ensure that the query is executed by the cloud on correct data and the returned results have not been modified (integrity); the results shall include the complete data set (completeness)[1].

Preserving the security of the outsourced databases is great challenge in current scenario. Confidentiality, integrity in context of completeness and correctness, authenticity, etc. are consider as the pillars of security services[2]. Therefore, implementing them in an efficient manner is very important from security point of view. There are various techniques used for realizing the security in database outsourcing. These techniques include encryption, authenticated data structures, indexing, signature schemes, etc.

II. RELATED WORK

The number of techniques [3] have been proposes, aiming to provide both completeness and correctness of queries to remote database or cloud. These existing techniques can be mainly divided into two groups: tree-based techniques and signature-based techniques. Among the existing tree-based techniques, the best one is proposed by Li et.al [4] , which introduce a fiction embedded Merkle B+ Tree structure and obtain integrity of the query result with simple hash operations. However, the communication complexity of [4] is linear to the number of tuples and attributes associated with the query results, which extent its performance for queries results with large ranges.

Another concern about data integrity is the issue of storage integrity on outsourced data, which permits the data user to verify the integrity of his own data files stored on untrusted server without retrieving it. The seminal works include Provable Data Possession (PDP) [5] and Proof of Retrievability (POR) .

III.PROPOSED SCHEME

In this paper, we propose new auditing scheme for outsourced database, which can achieve the correctness and completeness of search results. We prove that the proposed scheme is secure compared with the existing auditing scheme. The proposed scheme can support the dynamic database. Also analyze the performance of data outsourcing and retrieving of proposed scheme.

DOI10.17148/IJARCCE.2017.65108

IV. ARCHITECTURE

This paper introduce an audit system architecture for outsourced data in clouds as shown in Fig. 1. In this architecture, we consider that data storage service involves four entities: the data owner, the users, cloud service provider, and arbitration center (Auditor).

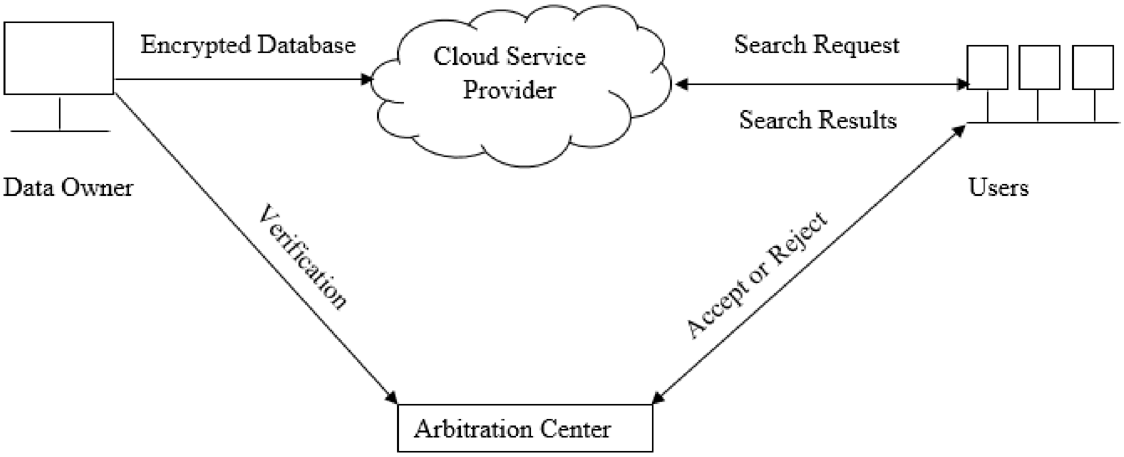

Fig. 1 The outsourced database

The data owner relate to the entity who wants outsource database to the CSP. He generates an authentication structure. The user wants to access database services, who may have limited storage capacity and computing power. The cloud service provider is responsible for storing the encrypted data and provides various database services to user. The arbitration center works as trusted third party to deal with the dispute between the user and the CSP.

V. TECHNIQUES

Merkle B Tree

An MB-tree works like a B+-tree. An MBT is combination of MHT and B+ Tree and also consists of ordinary B+-tree nodes that are expanded with one hash value associated with every pointer entry. The hash values concerned with entries on leaf nodes are computed on the database records themselves. The hash values concerned with index node entries are computed on the concatenation of the hash values of their children. After computing all hash values, the data owner has to sign the hash of the root using the private key.

To answer a range query the server builds a verification object (VO) by initiating two top-down B+-tree like traversals, one to find the left-most and one the right-most query result. At the leaf level, the data implied in the nodes between the two discovered boundary leaves are returned, as in the normal B+-tree. The server also necessity to include in the VO the hash values of the entries contained in each index node that is visited by the lower and upper boundary traversals of the tree, except the hashes to the right (left) of the pointers that are traversed until the lower (upper) boundary traversals. At the leaf level, the server puts only the answers to the query, along with the hash values of the remaining entries to the left and to the right parts of the boundary leaves. The result is also enhanced with one tuple to the left and one to the right of the lower-bound and upper-bound of the query result respectively, for completeness verification. Finally, the signed root of the tree is inserted as well.

VI. CONCLUSION AND FUTURE WORK

In this paper, we can achieve auditing of outsourced database in cloud computing. We constructed dynamic audit services for untrusted and outsourced storages. We can achieve the verifiability of search result. We also prove that our scheme can achieve the desired security goals.

REFERENCES

1. J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, “Verifiable Auditing for Outsourced Database in Cloud Computing,” IEEE Trans. Comput., vol. 64, no. 11, pp. 3293–3303, 2015.
2. M. Xie, H. Wang, and J. Yin, “Integrity auditing of outsourced data,” Very large data bases, pp. 782–793, 2007.

DOI10.17148/IJARCCE.2017.65108

3. J. Yuan and S. Yu, "Flexible and publicly verifiable aggregation query for outsourced databases in cloud," 2013 IEEE Conf. Commun. Netw. Secur. CNS 2013, pp. 520–524, 2013.
4. F. Li, M. Hadjileftheriou, G. Kollios, and L. Reyzin, "Authenticated index structures for outsourced databases," Handb. Database Secur. Appl. Trends, pp. 115–136, 2008.
5. G. Ateniese et al., "Provable data possession at untrusted stores," ACM Conf. Comput. Shilpa jain and Sourabh jain ,'Energy Efficient Maximum Lifetime Ad-Hoc Routing (EEMLAR)', international Journal of Computer Networks and Wireless Communications, Vol.2, Issue 4, pp. 450-455, 2012.
6. 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.
7. F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in Proc. ACM SIGMOD Int. Conf. Manag. Data, 2006, pp. 121–132.
8. A. Juels and B. S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 584–597.
9. Q. Chai and G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in Proc. IEEE Int. Conf. Commun., 2012, pp. 917–922.
10. H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H.Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A Study of UserFriendly Hash Comparison Schemes," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114, 2009
11. Zheng-Fei Wang, Ai-Guo Tang, "Implementation of Encrypted Data for Outsourced Database", In Proc. of Second International Conference on Computational Intelligence and Natural Computing (CINC), IEEE, 2010, pp. 150-153.
12. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. 29th IEEE Int. Conf. Comput. Commun., 2010, pp. 525–533.

BIOGRAPHY

Darshan Tatyaso Kavathekar is currently pursing M. Tech in Computer Science and Engineering (Specialization in Information Technology) Walchand College of Engineering Sangli, Shivaji University. He received Bachelor degree in 2015 from ADCET, Ashta, MS, India. His research interests are Cloud Computing, Algorithms, Information Security, etc.

DOI10.17148/IJARCCE.2017.65108