ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Privacy Preserving Technique in Two Cloud Secure Database for Related SQL Range

P.Purushothaman[1.], A.Gopalakrishnan, M.E[2]., Dr. R.Umamaheshwari, M.E., Ph.D.,[3]

Research Scholar, Dept. of Computer Science, Gnanamani College of Technology, Tamilnadu, India [1]

Assistant Professor, Dept of Computer Science, Gnanamani College of Technology, Tamilnadu, India [2]

HOD (CS), Gnanamani College of Technology, Namakkal, Tamilnadu, India[3]

ABSTRACT: Industries and individuals outsource database to realize convenient and low-cost applications and services. In order to provide sufficient functionality for SQL queries, many secure database schemes have been proposed. However, such schemes are vulnerable to privacy leakage to cloud server. The main reason is that database is hosted and processed in cloud server, which is beyond the control of data owners. For the numerical range query (">", "<", etc.), those schemes cannot provide sufficient privacy protection against practical challenges, e.g., privacy leakage of statistical properties, access pattern. Furthermore, increased number of queries will inevitably leak more information to the cloud server. In this paper, we propose a two-cloud architecture for secure database, with a series of intersection protocols that provide privacy preservation to various numeric- related range queries. Security analysis shows that privacy of numerical information is strongly protected against cloud providers in our proposed scheme.

KEYWORDS: Data Owner, Privacy Protection, Two Cloud Architecture.

I. INTRODUCTION

The growing industry of cloud has provided a service paradigm of storage/computation outsourcing helps to reduce users' burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users. However, due to the privacy concerns that the cloud service provider is assumed semi-trust (honest-but curious.), it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are needed before outsourcing sensitive data - such as database system - to cloud.

The typical scenario for out sourced database is Crypt DB: A cloud client, such as an IT enterprise, wants to outsource its database to the cloud, which contains valuable and sensitive information (e.g. transaction records, account information, disease information), and then access to the database (e.g. SELECT, UPDATE, etc.). Due to the assumption that cloud provider is honest-but-curious, the cloud might try his/her best to obtain private information for his/her own benefits. Even worse, the cloud could forward such sensitive information to the business competitors for profit, which is an unacceptable operating risk.

II. LITERATURE REVIEW

Wei Li, KaipingXue, YingjieXue "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage "TO satisfy requirements of data storage and high performance computation, cloud computing has drawn extensive attentions from both academic and industry. Cloud storage is an important service of cloud computing, which provides services for data owners to outsource data to store in cloud via Internet.

Jiawei Yuan, Shucheng Yu "Flexible and Publicly Verifiable Aggregation Query for Outsourced Databases in Cloud" For securing databases outsourced to the cloud, it is important to allow cloud users to verify that their queries to the cloud-hosted databases are correctly executed by the cloud. Existing solutions on this issue suffer from a high communication cost, a heavy storage overhead or an overwhelming computational cost on clients. Besides, only

DOI: 10.15680/IJIRCCE.2018.0603072

simple SQL queries (e.g., selection query, projection query, weighted sum query, etc) are supported in existing solutions.

Xiaofeng Chen, Jin Li, JianWeng "Verifiable Computation over Large Database with Incremental Updates" With the availability of cloud services, the techniques for securely outsourcing the prohibitively expensive computations are getting widespread attention in the scientific community. That is, the clients with resource-constraint devices can outsource the heavy computation workloads into the untrusted cloud servers and enjoy the unlimited computing resources in a pay-per-use manner.

Arnaud Castelltort and Anne Laurent "Fuzzy Queries over NoSQL Graph Databases: Perspectives for Extending the Cypher Language" When querying databases, users often wish to express vague concepts, as for instance asking for the cheap hotels. This has been extensively studied in the case of relational databases. In this paper, we propose to study how such useful techniques can be adapted to No SQL graph databases where the role of fuzziness is crucial. e indeed among the fastest-

III. EXISTING SYSTEM

In this section, we firstly give an overview of our existing two-cloud scheme, and then present the detailed interaction protocols to realize range query with privacy preservation on outsourced encrypted database.

In our scheme, two clouds (refer to Cloud A and Cloud B, respectively) have been assigned distinct tasks in the database system: Cloud A provides the main storage service and stores the encrypted database. Meanwhile, Cloud B executes the main computation task, to figure out whether each numerical record satisfies the client's query request with its own security key. With the assumption of no collusion between two clouds, the knowledge of application logic can be partitioned into two parts in our proposed scheme, where each one part is only known to one cloud. As we will analyze in this paper, one single part of knowledge cannot reveal privacy of the data and the query.

Disadvantages

- Discrimination may cause a much more information loss
- Data extracting time consumption is more.
- Sensitive attributes does not prevent unethical.
- Less security for data transformation

IV. PROPOSED SYSTEM

Our proposed secure database system includes a database administrator, and two non-colluding clouds. In this model, the database administrator can be implemented on a client's side from the perspective of cloud service. The two clouds (refer to Cloud A and Cloud B), as the server's side, provide the storage and the computation service. Briefly depicts the architecture of our outsourced secure database system in our scheme.

The two clouds work together to respond each query request from the client/authorized users (availability). For privacy concerns, these two clouds are assumed to be non-colluding with each other, and they will follow the intersection protocols to preserve privacy of data and queries (privacy).

Advantages

- High security provide.
- It is easy to maintain the database storage.
- Two cloud service clouds provide secure for users.

V. METHODOLOGIES

- CLOUDS STORAGE
- DATA CONTENTS
- SERVICE KEY ASSUMPTION

DOI: 10.15680/IJIRCCE.2018.0603072

CLOUDS STORAGE

We propose two cloud management systems using intelligent traffic clouds to overcome the issues we've described so far. With the support of cloud computing technologies, it will go far beyond other multi agent traffic management systems, addressing issues such as infinite system scalability, an appropriate agent management scheme, reducing the upfront investment and risk for users, and minimizing the total cost of ownership.

DATA CONTENTS

The privacy of data contents includes (1) The definition and description of each column (column name) in the table of the stored database, and(2) The values of each record in the table. Some related works have mainly focused on this issue, in which the column names are blinded (such as Crypt DB) and meanwhile the values are encrypted with some other encryption techniques (such as Order Preserving Encryption) and some deterministic encryption schemes, so that the adversaries cannot easily and directly guess the meaning of the column, or the values of the data. However, in an outsourced database, utilizing encryption alone, without other mechanisms, is far from being enough to preserve the privacy of the data contents. With the development of data analysis, by extracting features from data and queries, classification technique can help understand the definition of columns, and then breach of confidentiality of data contents.

SERVICE KEY ASSUMPTION

Cloud Computing moves the application software and databases to the large data centers to maintain security. The management security data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this two cloud, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed crypto analyze scheme with two salient features, opposing to its predecessors. By utilizing the homomorphism key token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s) and responses.

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented two-cloud architecture with a series of interaction protocols for outsourced database service, which ensures the privacy preservation of data contents, statistical properties and query pattern. At the same time, with the support of range queries, it not only protects the confidentiality of static data, but also addresses potential privacy leakage in statistical properties or after large number of query processes. Security analysis shows that our scheme can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that our proposed scheme is efficient.

In our future work, we will consider to further enhance the security while ensuring practicality, and we will extend our proposed scheme to support more operations, such as "SUM/AVG".

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
2. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
3. K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.
4. J.W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security. CRC press, 2016.
5. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.
6. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.
7. R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp. 85–100.

DOI: 10.15680/IJIRCCE.2018.0603072

8. C. Curino, E. P. Jones, R. A. Popa, N. Malviya et al., “Relational cloud: A database-as-a-service for the cloud,” 2011, http://hdl.handle.net/1721. 1/62241.
9. D. Boneh, D. Gupta, I. Mironov, and A. Sahai, “Hosting services on an untrusted cloud,” in Advances in Cryptology-EUROCRYPT 2015. Springer, 2015, pp. 404–436.
10. X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” IEEE Transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.
11. X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.
12. S. Benabbas, R. Gennaro, and Y. Vahlis, “Verifiable delegation of computation over large datasets,” in Annual Cryptology Conference. Springer, 2011, pp. 111–131.
13. W. Li, K. Xue, Y. Xue, and J. Hong, “TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016.
14. K. Xue, Y. Xue, J. Hong,W. Li, H. Yue, D. S.Wei, and P. Hong, “RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.
15. R. A. Popa, F. H. Li, and N. Zeldovich, “An ideal-security protocol for order-preserving encoding,” in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP’13). IEEE, 2013, pp. 463–477.