Non-Colluding Cloud Architecture for Privacy Preserving in Database Service

Ishwarya S, SubiaNaureen, Suman Sariga M. S, Jyothi. T
Department of information science and engineering, GSSSIETW, Mysuru, Karnataka, India

ABSTRACT

In the present scenario, businesses and people are outsourcing database to accomplish helpful administrations and minimal effort applications. To provide sufficient functionality for SQL queries, many secure database schemes have been proposed. However, the proposed 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.), the schemes cannot provide sufficient privacy protection against the practical challenges. A portion of the difficulties faced are privacy leakage of statistical attributes and access patterns. 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: Cloud Computing, Database, Privacy Preserving, Range Query

I. INTRODUCTION

In the present circumstances as it can be seen cloud has taken the control over the IT business with its innumerable advantages. It holds the possibility to change an extensive segment of the IT business, making software considerably more appealing as a service. The growing industry of cloud has provide 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. Security is the chief concern of the cloud computing. Cloud clients confront security dangers both from outside and inside the cloud. However, due to the privacy concerns that the cloud service provider is assumed semi-trust, it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are needed before outsourcing sensitive data to cloud.

The privacy challenge of outsourced database is two-hold.

1) Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers.
2) The data and queries of the outsourced database should be protected against the cloud service provider.

This divide-and-conquer mechanism can know any private information from one single isolated part of the knowledge. In this paper, a secure two-cloud database service architecture is introduced, where the two clouds are non-colluding and both of them knows only part of knowledge. Based on this architecture, a series of interaction protocols for a client to conduct numeric-related query over encrypted data from remote cloud servers is proposed. The numeric-related query includes common query statements, such as greater than, less than, and between.

II. PROBLEM STATEMENT

A. Existing System

In existing system, the perspective for privacy assurance and the data not only include permanently stored information that is the database, but also each temporary query request.

Additionally and importantly, as the assumption in some existing works, we assume that the two clouds A and B are non-colluding: Cloud A follows the protocol to add required obfuscation to protect privacy against cloud B, so that cloud B cannot obtain additional private information in the interactions with Cloud A. No private information is delivered beyond the scopes of protocols.

Disadvantages

a. While providing efficient cross server storage verification and data availability insurance, the entire focus is on static or archival data.
b. The capability of handling dynamic data remains unclear, which inevitably limits full applicability in Server storage scenarios.

B. Proposed System

In the proposed system the two-cloud scheme, the detailed interaction protocols will be provided to realize range query with privacy preservation on outsourced encrypted database. The proposed mechanism can preserve the privacy of data and query requests against each of the two clouds.

Specifically, Cloud A only knows the query request type and the final indexes, but due to dummy items appending, Cloud A cannot accurately understand the finally satisfied index set for each single request. For Cloud B, it knows the satisfied indexes of each single request, but after the proposed operations, it does not know the relationship of the corresponding items. Moreover, Cloud B can hardly distinguish whether two received columns are generated from one or more columns in the original database.

III. LITERATURE SURVEY

[1] Two- Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving.
Kaiping Xue, , Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu, and Peilin Hong.

This paper deals withClient Module, Storage Service Module,Query Service Moduleand Cloud Service Provider Module. It also ensures the privacy preservation of data contents, statistical properties and query patternwith the support of range queries.

[2] Achieving Collaborative Cloud Data Storage byKey-Escrow-Free Multi-Authority CP-ABE Scheme with Dual-Revocation.
Nyamsuren Vaanchig, Hu Xiong, Wei Chen, and Zhiguang Qin.

The Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE) is an data access control for large-scale collaborative cloud storage service is addressed in this paper.

[3] Privacy Preserving Data Storage Technique in Cloud Computing.
Dr.K.Kartheeban, A.Durai Murugan.

This paper shows how exactly the privacy is preserved and availability of information in cloud computing. The distribution of information among the multiple available Cloud service providers is done in order to preserve the privacy.

[4] RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage.

K. Xue, Y. Xue, J. Hong,W. Li, H. Yue, D. S.Wei, and P. Hong.

This paper is based on how to achieve a robust and efficient access control for public cloud storage.The Ciphertext-Policy Attribute-Based En-Cryption (CP-ABE) is the methodology used in this paper.

[5] “CryptDB: protecting confidentiality with encrypted query processing.
R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan.

In this, paper the proposed CryptDB, a framework to defend the private information in databases. CryptDB fundamentally includes utilizing the range queries productively finished the encrypted information utilizing a novel SQL-aware encryption system.

IV. METHODS AND MATERIAL

This section describes the potential threats and the privacy requirements when the database is outsourced to public cloud. The stored data contents and the query processes. Although there are many data encryption schemes, some fail to provide sufficient privacy preservation after statistical analysis. Repeated and large-amount query processes not only leak the access patterns, but also disclose the stored encrypted data progressively.
The privacy issues we consider in this paper are as follows:

1. Potential Threats and Privacy Requirements.
2. Data contents Module.
3. Query pattern Module.
4. Privacy of Item Values Modules

1. Potential Threats and Privacy Requirements

This section describes the potential threats and the privacy requirements when the database is outsourced to public cloud. The stored data contents and the query processes. Although there are many data encryption schemes, some fail to provide sufficient privacy preservation after statistical analysis: Repeated and large-amount query processes not only leak the access patterns, but also disclose the stored encrypted data progressively.

2. Data contents Module

Besides the static properties can disclose the private information of data contents, such properties themselves are already sensitive and private for the client. Order Preserving Encryption (OPE), which is widely used in constructing the secure database, with support of range queries, directly exposes the statistical information in the encryption field. Furthermore, the leakage of statistic properties is part of the nature of outsourced cloud database service: the cloud can learn the statistical properties (like order) by repeated query requests. As an example, Fig. 3 describes such an attack: After two simple queries over one same column, the order relationship of some data in certain column can be determined. There are also some other direct and indirect scenarios to leak statistical properties. In this way, even though the order property is not exposed to the semi-trusted cloud at the beginning, the cloud can gradually find out the order information after many query requests.

3. Query Pattern Module

The query pattern also contains privacy information, as they can reveal the client’s purpose of the query. Even worse, such pattern can leak some statistical properties, as discussed above. Based on the above discussion, we assert that an outsourced secure database providing numeric-related queries should prevent the following private information from being obtained by the honest-but-curious clouds.

4. Privacy of Item Values Modules

An ideal scheme is required to make nothing of the statistical properties be leaked to the curious clouds. However, the privacy leakage of statistical properties in a practical outsourced database system is inevitable, as returning subset of data rather than universe requires knowledge for filtering. For instance, if the client wants to retrieve a from the outsourced database, a cloud server without any knowledge of the order can only return all items of the database to the client, which is not usable.

V. RESULT AND DISCUSSION

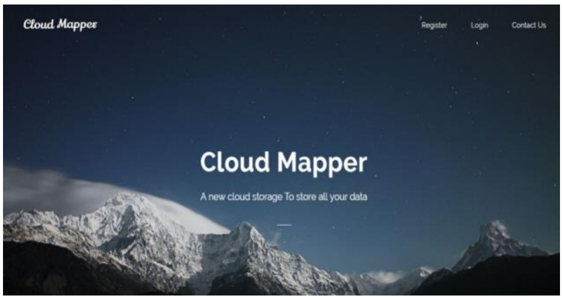


Figure 1. Home page

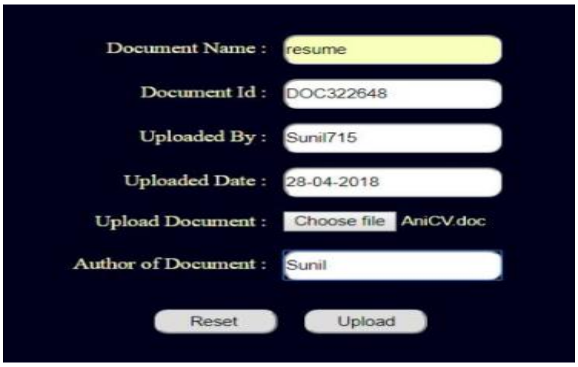
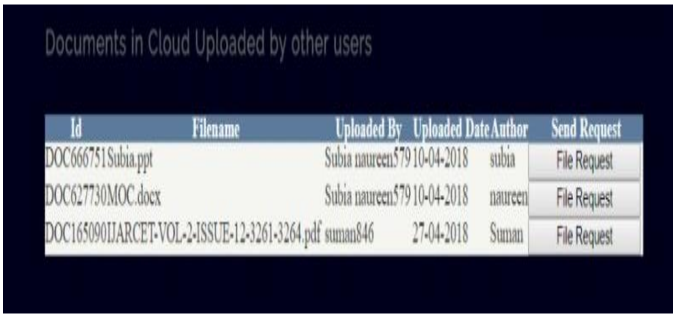
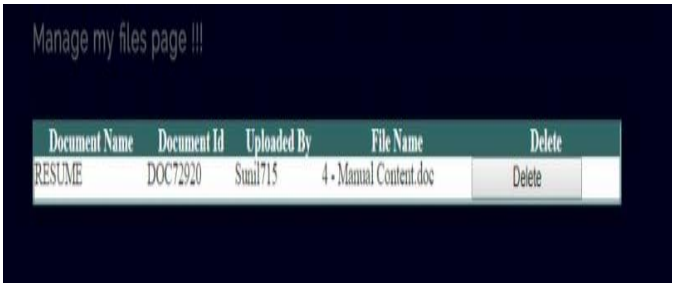

Document Name : resume
Document Id : DOC322648
Uploaded By : Sunil715
Uploaded Date : 28-04-2018
Upload Document : Choose file AniCV.doc
Author of Document : Sunil

Figure 2. File upload page


Documents in Cloud Uploaded by other users

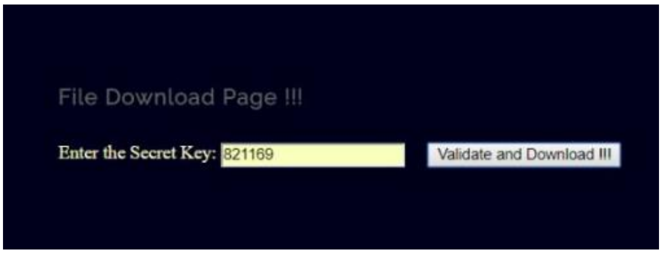
Id	Filename	Uploaded By	Uploaded Date	Author	Send Request
DOC666751Subia.ppt		Subia naureen579	10-04-2018	subia	File Request
DOC627730MOC.docx		Subia naureen579	10-04-2018	naureen	File Request
DOC165090IJARCET-VOL-2-ISSUE-12-3261-3264.pdf		suman846	27-04-2018	Suman	File Request

Figure 3. File Request Option to the Files Uploaded By Other Users


Manage my files page !!!

Document Name	Document Id	Uploaded By	File Name	Delete
RESUME	DOC72920	Sunil715	4 - Manual Content.doc	Delete

Figure 4. Manage files


File Download Page !!!

Enter the Secret Key: 821169

Figure 5. Download File

VI. CONCLUSION

In the presented two-cloud architecture a series of interaction protocols for outsourced database service is provided, 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 it can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that the proposed scheme is efficient. In the future work, it is required to enhance the security while ensuring practicality, and to extend the proposed scheme to support more operations, such as “SUM/AVG”.

VII. REFERENCES

[1] Nyamsuren Vaanchig, Hu Xiong, Wei Chen, and Zhiguang Qin “Achieving Collaborative Cloud Data Storage by Key-Escrow-Free Multi-Authority CP-ABE Scheme with Dual-Revocation”, 2018.

[2] J.W.Ritting house and J.F.Ransome,Cloud computing: implementation, management, and security. CRC press, 2016.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in 2014 IEEE 30th International Conference on Data Engineering. IEEE, 2014, pp. 664–675.

[10] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, “Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706–2716, 2016.

[11] Yu, Y. Liu, X. Yu, and K. Q. Pu, “Scalable distributed processing of k nearest neighbor queries over moving objects,” IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 5, pp. 1383–1396, 2015.

[12] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, “Practical approximate k nearest neighbor queries with location and query privacy,” IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 6, pp. 1546–1559, 2016.

[13] Z. Xia, X. Wang, X. 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, 2016.

[14] Z. Liu, X. Chen, J. Yang, C. Jia, and I.You, “New order preserving encryption model for outsourced databases in cloud environments,” Journal of Network and Computer Applications, vol. 59, pp. 198–207, 2016.

[15] X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, “Data mining with big data,” IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97–107, 2014.

[16] E. Stefanov and E. Shi, “Oblivistore: High performance oblivious cloud storage,” in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP’13). IEEE, 2013, pp. 253–267,

[17] J. Katz and Y. Lindell, Introduction to modern cryptography. CRC press, 2014.

[18] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, K. Ren, and S. Li, “P2SAS: Privacy-preserving centralized dynamic spectrum access system,” IEEE Journal on Selected Areas in Communications, 2016