Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving

Ailuri Venkatrami Reddy[1], Racharla Ramya[2]

[1,2]*Assistant Professor, Department of IT*
[1,2]*Malla Reddy Engineering College (A), Hyderabad, Telangana, India.*

Abstract

In the present scenario businesses and people are outsourcing database to accomplish helpful administrations and minimal effort applications. These are buried in the cloud server, which is outside the ability to control of the data proprietor. The SQL Queries require a few secure database schemes for its undeniable working, yet this at long last prompts privacy spillage to the cloud server. For numerical range inquiry (>,< , and so forth.) these neglect to give adequate security insurance. A portion of the difficulties faced are privacy leakage of statistical attributes, access patterns and so on. Likewise, increased number of queries will release more information to the cloud server. Thus, regarding these issues numerous works have been done by various researchers. We have studied some of these research works and analyzed the best possible ways to come to the desired level of privacy preservation in the case of cloud computing. Some of the works studied are the fuzzy logic, range queries, CryptDB order preserving encryption and multi-cloud architecture.

Keywords *— cloud computing, database, privacy preserving, range query*

1. 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 an service. Cloud computing [1] is alluded to as SaaS (Software as a Service) since it renders the applications as administrations over the Web and the hardware and systems software in the data centres that offer those administrations. The hardware of data centre and software is called a cloud Today the clouds can be open/public and in addition private. Private clouds are associated to the inner datacenters of a business or other association, not made accessible to the overall public. Cloud computing in this manner can be compressed as a blend of saas and utility computing, booting out the data centre (little + medium estimated). Security is the chief concern of the cloud computing. Cloud clients confront security dangers both from outside and inside the cloud. Shielding the information from the server itself is the pro of the main issues related with it. The server will by definition control the "bottom layer" of the product stack, which adequately goes around most known security methods. As said the cloud server is accepted as semi-trusted (honest-but-curious). CryptDB [5], a framework that gives confidentiality to applications that utilize database administration frameworks (DBMSes). CryptDB permits to perform queries over

Copyright © 2020 Authors

encrypted data, likewise the SQL's very much characterized set of operators, and queries over encrypted data. CryptDB tends to the hazard of an inquisitive database administrator (DBA) who endeavors to learn private information (e.g., health books, financial articulations, individual data) by keeping an eye on the DBMS server by keeping the DBA from learning private information. It uses a few instruments to accomplish this security functionality. One of the devices being the Order preserving encryption (OPE) [11, 12] is generally utilized as a part of databases to process SQL Questions over encrypted information. It permits to perform order operations on ciphertext like the plaintext for e.g. data server can fabricate index perform range queries [10] and sort the encrypted information like the plaintext. Regardless of going to the security reason well, despite everything it uncovers the order of the ciphertext. Therefore, the objective of security protection of the outsourced information to a cloud server is refined by partitioning the sensitive knowledge into two parts and store them in two non-colluding clouds.

Moreover, a secure database service architecture is acknowledged by utilizing two non-colluding clouds in which the information learning and query rationale is divided into two clouds. Henceforth, perceiving just a single cloud can't help uncovering private data. Other than a progression of intersection protocols to give numeric-related SQL range queries [1] with privacy preservation is additionally executed and it won't uncover order related data to any of the two non-colluding clouds.

2. System Architecture

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. It 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). In our scheme, the knowledge of stored database and queries is partitioned into two parts, respectively stored in one cloud. The mechanism guarantees that knowing either of these two parts cannot obtain any useful privacy information.

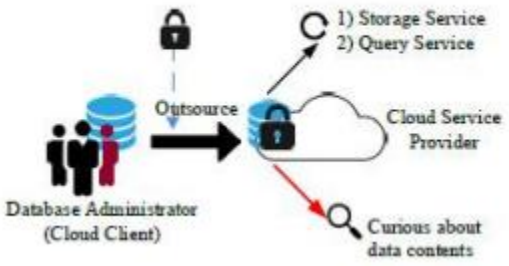

Figure 1. Outsource Database and Services

Copyright © 2020 Authors

As shown in to conduct a secure database, data are encrypted and outsourced to be stored in one cloud (Cloud A), and the private keys are stored in the other one (Cloud B). For each query, the corresponding knowledge includes the data contents and the relative processing logic. We utilize a prototype of knowledge partition, dividing application logic into two parts, which is bristly proposed by Bohli et al. In [16]. The application logic, as a secret knowledge, is partitioned into two parts, each of which is only known to one cloud. This prototype. Intuitively, this two-cloud architecture increases some complexity to some extent, and we will analyze and point out that this overhead is acceptable.

3. Related Work

This Paper analyzes recent research related to single or multiple cloud security and addresses possible solutions. Research on using multi-cloud providers to maintain security has been found to receive less attention from the research community than using individual clouds. This work aims to promote the use of multiple clouds thanks to its ability to reduce security risks affecting the user of cloud computing. We present new preprocessing techniques that allow obtaining interactive query times in large text collections (100 GB of text, served by a single machine). Consider two similarity measures, one in which the query terms coincide with similar terms in the collection (for example Algorithm of algorithm matches or vice versa) and one in which the query terms coincide with terms with a similar prefix in the collection (for example, Alori corresponds to the algorithm). The latter is important when we want to show the results instantly after each keystroke (search while writing). All the algorithms have been completely integrated into the complete search engine.

In this Paper, we define and solve the search for keywords classified as effective but protected on data encrypted in the cloud. We use order preserving symmetric encryption to protect data in the cloud. Although many research techniques are available, they do not offer efficient search results. For example, the search results generated 40 records and in those 30 records are relevant and the remaining 10 records generate irrelevant data. This paper focuses mainly on research methods that will improve the effectiveness of research. We use search methods based on keywords and concepts to retrieve relevant search criteria. This method will restore documents based on broader conceptual entities, which will improve the efficiency of the search.

4. 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

 Copyright © 2020 Authors

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, It 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.

5. Conclusion

In this paper, we presented a two-cloud architecture with an intersection for outsourced database service, which ensures the privacy preservation of data contents and SQL range 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 architecture are efficient. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

References

[1] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom "Cloud Computing Security: From Single to Multi-Clouds" in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, 2012, pp. 5490–5499.

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

 Copyright © 2020 Authors

[3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proceedings of the 30th IEEE International Conference on Distributed Computing Systems (ICDCS2010). IEEE, 2010, pp. 253–262.

[4] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212– 224, 2013.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data. ACM, 2004, pp.563–574.

[6] H. T. Dinah, 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, "Crypt: protecting confidentiality with encrypted query processing," in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp.85–100.

[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.

Copyright © 2020 Authors