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

Singani Venkateswarlu[1], C.Md. Gulzar[2]
[1]PG Scholar, Dept. Of CSE, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, A.P.
[2]Associative Professor, Dept. Of CSE, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, A.P.

ABSTRACT

A 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. In most of the organization, database management is the key component in the case of information infrastructure. In place of database management in-house, the computing industry has moved on the latest trend of outsourcing the database. The principle reason is that database is facilitated and handled in cloud server, which is outside the ability to control of information proprietors. In the database management, one of the necessary requirementsis to provide security to the database by holding the information confidential. But when the database is encrypted there exist the problem of processing queries. Furthermore enhance the security while ensuring practicality and the logical and mathematical queries those plans can't give adequate security assurance against possible difficulties. Moreover, expanded number of queries will definitely release more data to the cloud server. The SQL Queries require a few secure database schemes for it sun deniable working, yet this at long last prompts privacy spillage to the cloud server. For numerical range queries (>, <) these neglect to give adequate security insurance. Security examination demonstrates that security of numerical data is firmly ensured against cloud suppliers in our proposed scheme. 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, we propose an enhanced two-cloud architecture for secure database, with a series of intersection protocols that provide privacy preservation to various numeric-related range queries e.g. some numeric-related (>, < , =, Between, and Average etc).

I.INTRODUCTION

In modern era it can be seen that cloud has taken the control over the IT business with its various points of interest. It holds the likelihood to change a broad portion of the IT business, making programming significantly additional engaging as an administration. Distributed computing is implied to as SaaS (Software as a Service)[7] since it renders the applications as organizations over the Web and the equipment and frameworks programming in the multiple server that offer those organizations. The hardware of multiple server and software is known as a cloud [7]. Private clouds are related to the inward

datacenters of a business or other affiliation, not made available to the general purpose. Cloud registering in this way can be compacted as a mix of saas and utility registering, booting out the multiple servers. Security is the main worry of the distributed computing[1]. Cloud customers go up against security threats both from outside and inside the cloud. Protecting the data from the server itself is the main of the principle issues related with it. The server will by description control the "base layer" of the product stack, which effectively goes around most known security methods. As said the cloud server is accepted as semi-trusted. A framework that gives privacy to applications that uses database management frameworks (DBMSes) is known as CryptDB [9]. It permits to execute queries over encrypted data, similarly the SQL is extremely characterized the operators and queries over encrypted data. CryptDB tends to the hazard of an inquisitive database administrator (DBA) who going on to learn private information (e.g., medical data, financial data, individual data etc.) by keeping an attention on the DBMS server. The DBA try to learn private information by using different methods and security functionality. One of the procedure being the Order preserving encryption (OPE) [08][11] is generally used as a part of databases to process SQL queries over encrypted data. It permits to perform order operations on cipher text like the plaintext for e.g. Data server can build index to execute range queries [3] and sort the encrypted data like the plaintext. In spite of the security reason well, even though everything it uncovers the order of the cipher text. Hence the purpose of security protection of the outsourced data to a cloud server is developed by partitioning the sensitive information into two parts and store them in two different clouds. Furthermore, a secure database service architecture is known by utilizing two non-colluding clouds in which the information knowledge and query pattern is divided into two clouds.So each cloud knows only its respective data and they are non-colluding so both of them know only part of the pattern of queries. By firing out queries on a single cloud we can't be find out any private data. Other than an evolution of intersection protocols for a client to conduct numeric related SQL range queries e.g (>, < , =, Between, and Average etc)with privacy protection is additionally executed and it will never find out any order related information from any of the two non-colluding clouds.

III. SYSTEM ARCHITECTURE, SECURITY ASSUMPTION AND SECURITY REQUIREMENTS

A. 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. Fig. 1 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. 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).

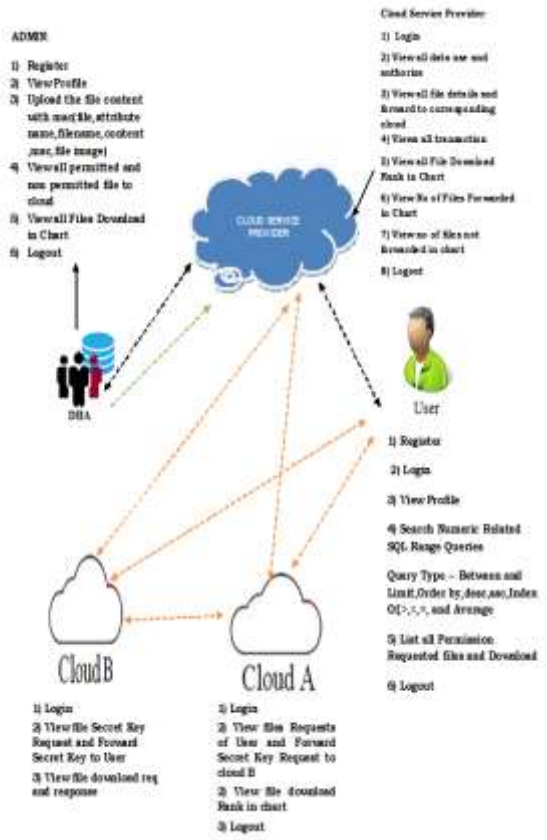

Figure 1: System Architecture

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. As shown in Fig. 2(a), 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. The application logic, as a secret knowledge, is partitioned into two parts, each of which is only known to one cloud. This prototype is shown in Fig. 1.

B. Security Assumption

Following the general assumption of many related works in public cloud, we assume the clouds to be honest-but-curious: On one hand, both of the two clouds will respond with correct information in the interactions of our proposed scheme (honest); on the other hand, the clouds try their best to obtain private information from the data that they process (curious). From the perspective of privacy assurance, here the data not only include permanently stored information (i.e., database), but also each temporary query request (i.e., queries). 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.

C. Potential Threats and Privacy Requirements

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 mainly include data

contents, statistical properties, and query pattern as follows:

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 and meanwhile the values are encrypted with some other encryption techniques. 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.

Statistical Properties: 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.

Query Pattern: 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. 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:

Data Contents: The data contents includes item values and column names, which are the raw data that should be protected against any potential adversaries.

Statistical Properties: It includes the order of data and their probability distributions, some of which include ">", "<", "=", "BETWEEN", and "AVERAGE"etc.

Query Pattern: Each query should be kept private against the honest-but-curious clouds and any unauthorized parties. The secrecy of such pattern should be well preserved even after many query processes.

IV. OUR PROPOSED TWO-CLOUD SCHEME

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. Based on the two-cloud architecture, our scheme provides an approach to query numeric-related data with privacy preservation. The client can retrieve the desired data from the cloud, when the query predicates contain operators like ">", "<" and "BETWEEN"

for one column, or even diverse condition combinations over one or more columns. For example, the client wants to retrieve items from the table, whose column Ti should be greater than a constant a (i.e., SELECT _ FROM table WHERE Ti > a). In our scheme, it is resolved by figuring out the sign of each value of (Ti(j)-a), in which j traverses all rows of the whole table. If the result is greater than 0, the relevant item satisfies the query predicate. These procedures are executed in the encryption field, so that the privacy is strongly preserved. Meanwhile, each column name Ti must be encrypted.

The Structured Query Language (SQL) is a specified purpose programming language, which is used to manage data in a relational database system, which has become a standard of the ANSI and ISO in 1986 and 1987 respectively. A query operation can request arbitrary data with a statement to describe the desired data. The requested data can be several columns of one or more tables in the database, and it can also be aggregated results from the original data (such as sum, average, and count of the datum.). To obtain the desired data, the query contains some statements to describe the requirement, e.g. some numeric-related (“>”, “<”, “=”, “BETWEEN”, “AVERAGE”etc.). Based on the introduced two-cloud architecture, we further propose a series of interaction protocols between the client and the two clouds, which can realize numeric-related SQL queries, and satisfy privacy requirements. It should be noted that, apart from the query operation, there are other SQL operations (e.g. update, insert) which modify the data. The privacy issue for such cases can be resolved with other existing approaches, such as ORAM (Oblivious RAM), which is beyond the scope of our paper. In this paper, we focus on implementing query operation with privacy preserving.

V.Conclusion

Present two-cloud data source service structure. Two atmosphere are non-colluding namely cloud-A and cloud-B and both of them know only part of knowledge. Series of connections methods for a customer to perform numeric-related question (“>”, “<”, “=”, “BETWEEN”, “AVERAGE”etc.) over secured information from distant reasoning web servers. The two atmosphere work together to react each question demand. For comfort concerns, these atmosphere follow the methods to protect comfort of information and concerns.

VI.REFERENCE

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., “A view of cloud computing,” Communications of the ACM.

[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.

[3] K. Xue and P. Hong, “A dynamic secure group sharing framework in public cloud computing,” IEEE Transactions on Cloud Computing.

[4] J.W. Rittinghouse and J. F. Ran some, Cloud computing: implementation, management, and security. CRC press, 2016.

[5] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems.

[6] 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.
[7] 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.
[8] 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.
[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] F. Hao, J. Daugman, and P. Zielinski, "A fast search algorithm for a large fuzzy database," IEEE Transactions on Information Forensics and Security, vol. 3, no. 2, pp. 203–212, 2008.
[11] A. Castelltort and A. Laurent, "Fuzzy queries over NoSQL graph databases: perspectives for extending the cypher language," in International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems. Springer, 2014, pp. 384– 395.
[12] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keywordsearch over encrypted data in cloud computing," in Proceedings ofthe 29th IEEE International Conference on ComputerCommunications (INFOCOM2010). IEEE, 2010, pp. 1–5.
[13] 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.
[14] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.
[15] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multikey word fuzzy search over encrypted data in the cloud," in Proceedings of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM2014). IEEE, 2014, pp. 2112–2120.
[16] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Transactions on Computers, vol. 62, no. 11, pp. 2266– 2277, 2013.
[17] 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.
[18] Z. 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.
[19] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, "Secure Knn computation on encrypted databases," in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. ACM,
2009, pp. 139–152.
[20] 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.
[21] 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.
[22] D. Boneh and B. Waters, "Conjunctive, subset, and range queries onencrypted data," in Theory of Cryptography. Springer, 2007, pp. 535–554.
[23] E. Shi, J. Bethencourt, T. H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in IEEE Symposium onSecurity and Privacy (SP'07). IEEE, 2007, pp. 350–364

About Authors:

SINGANI VENKATESWARLU is current pursuing M.Tech in CSE. dept., Dr.K.V.Subba Reddy Institute of Technology, Kurnool, AP.

C.MD. Gulzar, Associative Professor & HOD (CSE), Dr.K.V.Subba Reddy Institute of Technology, Kurnool, AP.