2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

TWO-CLOUD PRIVACY DATABASE FOR ARITHMETIC-RELATED SQL RANGE QUERIES USING AES ENCRYPTION

[1]CH.SWETHA [2]MR.V.RAVIKUMAR VEMULA

[1] M.Tech Student, Department of Computer Science and Engineering, Chaitanya Institute of Technology and Science Kishanpura,Hanamkonda,Warangal -506001, (.TS).India

[2]Associate Professor, Department of Computer Science and Engineering , Chaitanya Institute of Technology and Science kishanpura,Hanamkonda,Warangal -506001, (TS).India

[1]Swethachennaboina515@gmail.com, [2]ravikumar.vemula@hotmail.com

Abstract:

Undertakings and individuals redistribute database to recognize profitable and negligible exertion applications and organizations. To give sufficient handiness to SQL questions, many secure database plans have been proposed. Regardless, such plans are defenseless against security spillage to cloud server. The basic reason is that database is encouraged and took care of in cloud server, which is outside the capacity to control of data owners. For the numerical range question (">", "<, etc.), those plans can't give sufficient security affirmation against rational challenges, e.g., insurance spillage of quantifiable properties, get the chance to structure. Furthermore, extended number of request will unavoidably discharge more information to the cloud server. In this paper, we propose a two-cloud plan for secure database, with a movement of combination shows that give assurance protection to various numeric-related range questions. Security examination exhibits that security of numerical information is unequivocally guaranteed against cloud providers in our proposed arrangement.

I.INTRODUCTION

The developing business of cloud has give an administration worldview of capacity/calculation redistributing diminishes clients' weight of IT framework upkeep, and decrease the expense for both the undertakings and individual clients However, because of the protection worries that the cloud specialist organization is accepted semi-trust (legitimate yet inquisitive.), it turns into a basic issue to place touchy administration into the cloud, so encryption or confusion are required before re-appropriating delicate information -, for example, database framework - to cloud. The run of the mill situation for redistributed database is portrayed in Fig. 1 as that in Crypt A cloud customer, for example, an IT undertaking, needs to redistribute its database to the cloud, which contains important and delicate data (for example exchange records, account data, malady data), and after that entrance to the database (for example SELECT, UPDATE, and so forth.) Due to the presumption that cloud supplier is straightforward however inquisitive the cloud may attempt his/her best to get private data for his/her own advantages. Far more terrible, the cloud could advance such delicate data to the business contenders revenue driven, which is an inadmissible working danger. Other than information security, customers' regular inquiries will definitely and bit by bit uncover some private data on information measurement properties. Along these lines, information and inquiries of the outsouced database ought to be ensured against the cloud specialist co-op. One clear way to deal with relieve the security danger of protection spillage is to encode the private information and shroud the question/get to designs. Sadly, apparently, couple of the scholarly world inquires about fulfill the two properties up until now. Sepulcher is the main endeavor to give a safe remote database application, which ensures the fundamental secrecy and protection prerequisite, and gives different SQL inquiries over scrambled information also. Grave uses a progression of cryptographic devices to accomplish these security usefulness. Particularly, request protecting encryption is used to acknowledge numericrelated range inquiry forms. From the point of view of inquiry usefulness, CryptDB bolsters most sorts of numerical SQL questions with such cryptology. In any case, such protection spillage hasn't been very much tended to altogether, since OPE is moderately powerless to give adequate security confirmation. Some particular reason cryptology like request protecting encryption(OPE) will uncover some private data to the cloud specialist co-op normally: As it is intended to save the request on figure messages with the goal that it tends to be utilized to lead range questions, the request data of the information, the factual properties got there from, for example, the information dissemination, and the entrance example will be spilled. Would we be able to plan another database framework to give range inquiries more grounded protection certification? From the work in, the protection can be saved against the cloud, if the touchy learning is apportioned into two sections, and disseminated to two non-conniving mists. In the writing, the writers additionally acquaint a two-party framework with plan a protected knn inquiry conspire, which empowers the customer to question k most comparable records from the cloud safely.

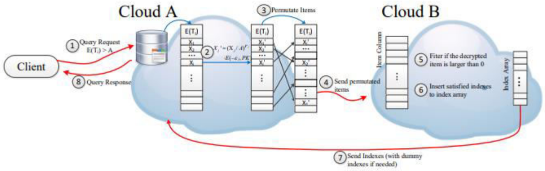
II.EXISTING SYSTEM:

From the perspective of security insistence, here the data consolidate forever set away information (i.e., database), yet likewise every brief request (i.e., questions). Besides and vitally, as the assumption in some present works, we expect that the two fogs An and B are non-scheming: Cloud A seeks after the show to add anticipated that disarray should verify assurance against cloud B, so cloud B can't gain additional private information in the coordinated efforts with Cloud A. No private information is passed on past the degrees of shows

III.PROPOSED SYSTEM:

In this segment, we right off the bat give a diagram of our proposed two-cloud plan, and afterward present the point by point cooperation conventions to acknowledge run question with protection conservation on redistributed scrambled database. The proposed instrument can save the protection of information and inquiry demands against every one of the two mists. In particular, Cloud A just realizes the inquiry ask for sort and the last records, yet because of sham things annexing, Cloud A can't precisely comprehend the at long last fulfilled list set for each single demand. Meanwhile, in order to prevent Cloud A from launching multiple specific-purpose query requests to deliberately to seek more knowledge about the data, we introduce a token based scheme, which can restrict the number of items and the range of columns that Cloud A can only process. 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..

Architecture:


Cloud A
Cloud B
Client
1 Query Request E(T_i) > A
8 Query Response
E(T_i)
X_1
X_2
X_i
2 X_i' = (X_i / A)^r · E(-ε_i, PK)
3 Permutate Items
4 Send permutated items
Item Column
5 Fiter if the decrypted item is larger than 0
6 Insert satisfied indexes to index array
Index Array
7 Send Indexes (with dummy indexes if needed)

Algorithm:

Paillier Cryptographic Algorithm There are various cryptographic techniques to support numeric-related operations (e.g. addition, multiplication, XOR) upon the encryption field. Paillier cryptosystem [41] is one of the most popular techniques that provides addition homomorphic, which means: if two integers a and b are encrypted with a same key k into two ciphertexts (be denoted as Ek(a) and Ek(b)), there exists an operation (refer to as "⊗"), such that Ek(a) ⊗ Ek(b) = Ek(a + b)

Paillier cryptographic algorithm is composed of the following phases: key generation, encryption and decryption. ◦ Key generation. Two large and independent prime numbers p and q are randomly selected. Then we compute n = p • q and µ = λ −1 mod n, where λ is the least common multiple of p and q, and commonly λ = lcm(p−1, q−1). The public key (PK) is n, and the private key (SK) is (λ, µ). ◦ Encryption. Let m be the integer to be encrypted. Firstly, we select a random number r ∈ Z ∗ n2 , and then the ciphertext of m can be computed as follows: E(m; r) = (n + 1)m • r n mod n 2 . (1) ◦ Decryption. Let the ciphertext c = E(m; r). The plaintext m can be recovered as follows: m = (c λ mod n 2) − 1 n • µ mod n.Paillier cryptosystem holds additive homomorphic in group Z + n , which corresponds to the multiplication operation in the encryption field in Zn2 . The following equation illustrates the homomorphic property of Paillier cryptosystem. E(m1; r1) • E(m2; r2) =(n + 1)m1 r n 1 • (n + 1)m2 r n 2 =(n + 1)m1+m2 (r1 • r2) n =E(m1 + m2; r1 • r2) (3) Another property can be be summarized as follows: E m2 (m1; r1) =((n + 1)m1 r n 1) m2 =(n + 1)m1•m2 (r1 m2) n =E(m1 • m2; r m2 1).

IV.IMPLEMENATATION:

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.

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.

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.

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.CONCLUSION:

In this paper, we presented 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. 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".

VI.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.

[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- on Security and Privacy (SP'13). IEEE, 2013, pp. 463–477.