International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Two-Cloud Design for Secure Database to give Protection Conservation to different Numeric-Related Range Queries

Yeshwanth Rao Bhandayker
System Programmer Analyst, FINANCE: Trading Application Vanguard, Malvern, PA - 19355

Abstract: ***Enterprises and people rearrange database to acknowledge beneficial as well as minimal effort applications and managements. So regarding offer sufficient effectiveness to SQL questions, lots of safe and secure database strategies have been recommended. In any case, such strategies are defenseless versus security spillage to cloud server. The essential reason is that database is assisted in and taken care of in cloud server, which is outside the capability to control of information proprietors. For the mathematical range question (" >", "<", and so forth.), those strategies can't offer ample security assurance versus down to earth problems, e.g., protection spillage of quantifiable buildings, get to design. Besides, expanded variety of questions will unavoidably release more data to the cloud server. In this paper, we recommend a two-cloud layout for safe database, with a development of convergence conventions that give protection conservation to different numeric-related range questions. Security investigation shows that security of numerical information is certainly guaranteed versus cloud distributors in our proposed plan.***

Index Terms: Cloud, database, protection, queries

I. INTRODUCTION

A. System Architecture

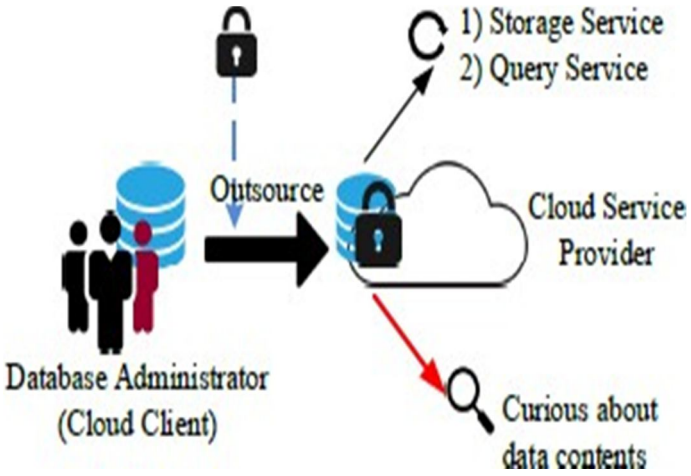

Figure - 1

The growing industry of cloud has give a service standard of storage/computation outsourcing helps to decrease customers' burden of IT infrastructure maintenance, and minimize the expense for both the enterprises and also private users Nonetheless, due to the privacy concerns that the cloud company is presumed semi-trust (honest-but curious.), it ends up being an essential issue to put delicate service into the cloud, so file encryption or obfuscation are required before contracting out delicate data - such as database system - to cloud. The typical situation for out sourced database is explained in Fig. 1 as that in Crypt A cloud client, such as an IT business, wishes to outsource its database to the cloud, which has beneficial and also sensitive details (e.g. transaction records, account details, disease info), and then access to the database (e.g. SELECT, UPDATE, etc.) Because of the presumption that cloud service provider is honest-but-curious the cloud may try his/her best to get personal information for his/her very own advantages. Even worse, the cloud could ahead such sensitive information to the business rivals for profit, which is an inappropriate operating risk.Besides data personal privacy, clients' frequent queries will certainly and gradually reveal some exclusive info on data statistic residential properties.

Therefore, information and queries of the outsouced database need to be safeguarded versus the cloud service provider. One straightforward technique to minimize the security danger of personal privacy leak is to secure the exclusive information and hide the query/access patterns. Regrettably, asfar as we know, couple of academia looks into satisfy both residential or commercial properties so far. Crypt is the very first effort to provide a safe and secure remote database application, which assures the standard discretion and also personal privacy demand, and gives varied SQL queries over encrypted data as well. Crypt uses a collection of cryptographic tools to attain these security capability. Especially, order preserving security is used to realize numeric related range query processes. From the viewpoint of query functionality, CryptDB supports most sort of mathematical SQL queries with such cryptology. However, such privacy leakage hasn't been well attended to thoroughly, because OPE is reasonably weak to supply adequate personal privacy assurance. Some certain objective cryptology like order preserving encryption(OPE) will reveal some exclusive info to the cloud service provider normally: As it is created to maintain the order on cipher texts to make sure that it can be used to conduct range queries, the order information of the data, the statistical buildings obtained there from, such as the information distribution, and the gain access to pattern will be dripped. Can we design a new database system to provide range queries with stronger personal privacy warranty? From the work in, the personal privacy can be maintained against the cloud, if the sensitive expertise is segmented right into two components, as well as distributed to two non- colluding clouds. In the literature, the authors likewise present a two-party system to design a protected knn query scheme, which makes it possible for the customer to query k most comparable records from the cloud securely.

II. EXISTING SYSTEM

From the viewpoint of protection affirmation, below the details include for perpetuity put away information (i.e., database), yet in addition every transitory inquiry request for (i.e., inquiries). Additionally as well as imperatively, as the presumption in some current jobs, we expect that the two mists An and also B are non-conniving: Cloud A pursues the convention to include expected complication to protect protection versus cloud B, so cloud B can't obtain additional personal information in the collaborations with Cloud A. No personal information is conveyed past the extents of conventions.

III. PROPOSED SYSTEM

In this segment, we right off the bat give a layout of our suggested two-cloud strategy, and later existing the factor by factor cooperation conventions to acknowledge run question with protection conservation on redistributed clambered database The proposed tool can save the protection of info as well as inquiry needs versus each of the two hazes. Specifically, Cloud A simply realizes the inquiry request for kind and also the last documents, yet due to sham points linking, Cloud A can't precisely comprehend the at long last fulfilled checklist collection for each and every single need. On the other hand, in order to protect against Cloud A from releasing several specific-purpose query requests to purposely to seek more understanding concerning the data, we present a token based plan, which can restrict the number of products and also the series of columns that Cloud A can only refine. For Cloud B, it knows the pleased indexes of each single request, but after the proposed procedures, it does not know the connection of the matching products. Moreover, Cloud B can barely differentiate whether two got columns are generated from several columns in the original database.

IV. IMPLEMENTATION

Paillier Cryptographic Algorithm There are various cryptographic techniques to sustain numeric-related operations (e.g. addition, reproduction, XOR) upon the file encryption field. Paillier crypto system [41] is among the most popular methods that gives enhancement homomorphic, which suggests: if two integers an as well as b are secured with an exact same crucial k right into two cipher texts (be represented as Ek(a) and also Ek(b)), there exists a procedure (refer to as "⊗"), such that Ek(a) ⊗ Ek(b) = Ek(a + b). Paillier cryptographic algorithm is made up of the list below phases: essential generation, encryption and decryption. ◦ Key generation. Two big and also independent prime numbers p and randomly selected.Then we compute n = p - q and also μ = λ − 1 mod n, where λ is the least common multiple of p and also q, and generally λ = lcm(p − 1, q − 1). The publickey (PK) is n, and also the private trick (SK) is (λ, μ). ◦ File encryption. Let m be the integer to be encrypted.Firstly, we select a random numberr.

∈ Z ∗ n2, and afterwards the ciphertext of m can be calculated as adheres to: E(m; r) = (n + 1) m - r n modn2.(1)◦ Decryption.Lettheciphertextc.

= E(m; r). The plain text m can be recovered as.

adheres to: m = (c λ mod n 2) − 1 n - μ mod n. Paillier cryptosystem holds additive homomorphic in group Z+ n, which corresponds to the reproduction procedure in the security 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) One more home can be summed up as adheres to: Em2(m1; r1) =-LRB-(n +1) m1rn1) m2.

=(n + 1) m1 - m2 (r1 m2) n =E(m1 - m2; r m2 1.).

Numeric-Related SQL Queries The Structured Query Language (SQL) is a specified purpose shows language, which is utilized to take care of information in a relational database system, which has ended up being a standard of the ANSI as well as ISO in 1986 [42] and 1987 [43] specifically. A query operation can request arbitrary data with a statement to describe the desired information. The asked for data can be several columns of several tables in the database, as well as it can also be aggregated results from the original data (such as sum, average, count of the data.). To acquire the wanted data, the query includes some declarations to explain the demand, e.g. some numeric-related (" >", "<"," BETWEEN"). For clearness, we refer to those query requests as numeric-related SQL queries in the rest of the paper. Based upon the presented two-cloud style, we additionally propose a collection of communication methods between the client and the two clouds, which can recognize numeric-related SQL queries, and also please personal privacy needs. It must be noted that, aside from the query procedure, there are various other SQL operations (e.g. update, place) which change the data. The personal privacy issue for such situations can be relolved with other existing techniques, such as ORAM (Oblivious RAM) [38], [44], [45], which is beyond the extent of our paper. In this paper, we concentrate on applying query procedure with personal privacy preserving

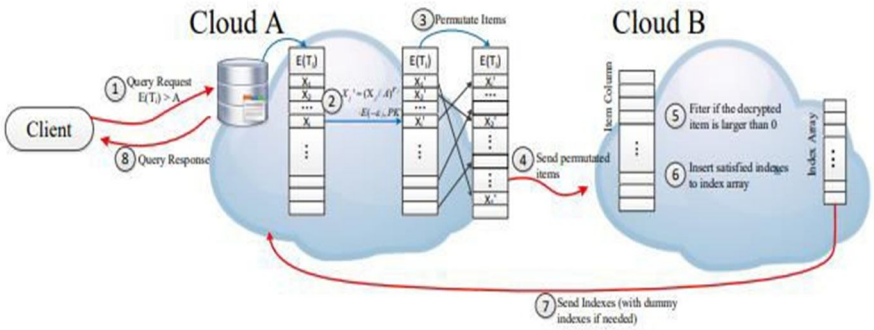

Figure - 2

V. CONCLUSION

In this paper, we offered a two-cloud style with a collection of interaction procedures for outsourced database solution, which guarantees the personal privacy preservation of information materials, statistical properties and query pattern. At the exact same time, with the assistance of range queries, it not just safeguards the discretion of fixed data, but also addresses potential personal privacy leakage in analytical residential or commercial properties or after lot of query processes. Security evaluation reveals that our plan can meet the privacy-preservation requirements. Furthermore, efficiency assessment outcome shows that our suggested system is reliable. In our future job, we will consider to even more improve the security while making certain functionality, as well as we will expand our proposed scheme to sustain even 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 queryprocessing,” in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp. 85–100.
[8] 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] Anusha Medavaka, P. Shireesha, “A Survey on TraffiCop Android Application” in “Journal of Advances in Science and Technology”, Vol. 14, Issue No. 2, September-2017 [ISSN : 2230-9659]
[10] Anusha Medavaka, Dr. P. Niranjan, P. Shireesha, “USER SPECIFIC SEARCH HISTORIES AND ORGANIZING PROBLEMS” in “International Journal of

Advanced Computer Technology (IJACT)", Vol. 3, Issue No. 6 , 2014[ISSN : 2319-7900]
[11] Yeshwanth Rao Bhandayker , "Artificial Intelligence and Big Data for Computer Cyber Security systems" in "Journal of Advances in Science and Technology", Vol. 12, Issue No. 24, November-2016 [ISSN : 2230-9659]
[12] Sugandhi Maheshwaram, "A Comprehensive Review on the Implementation of Big Data Solutions" in "International Journal of Information Technology and Management", Vol. XI, Issue No. XVII, November-2016 [ISSN : 2249-4510]
[13] Sugandhi Maheshwaram , "An Overview of Open Research Issues in Big Data Analytics" in "Journal of Advances in Science and Technology", Vol. 14, Issue No. 2, September-2017 [ISSN : 2230-9659]
[14] Yeshwanth Rao Bhandayker, "Security Mechanisms for Providing Security to the Network" in "International Journal of Information Technology and Management", Vol. 12, Issue No. 1, February-2017, [ISSN : 2249-4510]
[15] Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications", Volume 1, Issue 1, Jan-Mar 2014 [ISSN : 2349-0020]
[16] Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1,Jan-Mar 2014 [ISSN : 2349-0020].
[17] Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management", Volume VI, Issue I, Feb 2014 [ISSN : 2249-4510]
[18] Anusha Medavaka, P. Shireesha, "Analysis and Usage of Spam Detection Method in Mail Filtering System" in "International Journal of Information Technology and Management", Vol. 12, Issue No. 1, February-2017 [ISSN : 2249-4510]
[19] Anusha Medavaka, P. Shireesha, "Review on Secure Routing Protocols in MANETs" in "International Journal of Information Technology and Management", Vol. VIII, Issue No. XII, May-2015 [ISSN : 2249-4510]
[20] Anusha Medavaka, P. Shireesha, "Classification Techniques for Improving Efficiency and Effectiveness of Hierarchical Clustering for the Given Data Set" in "International Journal of Information Technology and Management", Vol. X, Issue No. XV, May-2016 [ISSN : 2249-4510]
[21] Anusha Medavaka , P. Shireesha, "Optimal framework to Wireless Rechargeable Sensor Network based Joint Spatial of the Mobile Node" in "Journal of Advances in Science and Technology", Vol. XI, Issue No. XXII, May-2016 [ISSN : 2230-9659]
[22] Anusha Medavaka,"Enhanced Classification Framework on Social Networks" in "Journal of Advances in Science and Technology", Vol. IX, Issue No. XIX, May-2015 [ISSN : 2230-9659]