Two Cloud Storage Database Numeric Related Queries for Privacy Protection

Dr. Deepak Sharma
HOD, Computer Engineering Department
K. J. Somaiya College of Engineering
Mumbai, India

Harita Kundalia
Department of Computer Engineering
K. J. Somaiya College of Engineering
Mumbai, India

***Abstract*— Strong encryption is known to offer assistance to data security. In spite of the way that encryption can make the data secure in data move exceptionally still, sometimes this encoded data obviously should be decoded. As of now at this very point, it so happens that the data gets powerless against attacks finally achieving sabotaged data security. This is where two cloud secure capacity comes into the picture, subsequently, it offers the ability to figure required characteristics from different encoded data sources with no social occasion choosing their secret data. Reasonably two cloud secure capacity is wherein we send the mixed data to a TTP. The TTP by then reestablishes the last needed result. As no accepted untouchable exists no question, two cloud secure capacity is the thing that's to come to offering induction to data in this manner similarly giving strong security affirmation. For example, expect there are a lot of players who wish to enroll the typical of their singular vocations.**

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

I. INTRODUCTION

The growing trade of cloud has give a service paradigm of storage/computation outsourcing helps to cut back users' burden of IT infrastructure maintenance, and reduce the price for each the enterprises and individual users. However, because of the privacy issues that the cloud service supplier is assumed semi-trust (honest-butcurious.), it becomes a crucial issue to place sensitive service into the cloud, therefore coding or obfuscation are required before outsoucing sensitive information - adore info system - to cloud. within the gift circumstances because it is seen cloud has taken the management over the IT business with its unnumbered advantages. It holds the chance to vary an intensive phase of the IT business, creating software significantly additional appealing as associate service. Cloud computing is alluded to as SaaS (Software as a Service) since it renders the applications as administrations over the online and also the hardware and computer programme within the data centres that provide those administrations. The hardware of knowledge centre and software is termed a cloud. nowadays the clouds is open/public and additionally private. non-public clouds are associated to the inner datacenters of a business or alternative association, not created accessible to the general public. Cloud computing during this manner is compressed as a mix of saas and utility computing, booting out the info centre (little + medium estimated). Security is that the chief concern of the cloud computing. Cloud purchasers confront security dangers each from outside and within the cloud. The privacy is preserved against the cloud, if the sensitive data is divided into two parts, and distributed to 2 non-colluding clouds. within the literature, the authors conjointly introduce a two-party system to style a secure knn query scheme, that permits the consumer to question k most similar records from the cloud securely. This divide-and-conquer mechanism will grasp any personal information from one singe isolated a part of the knowledge, and every of each clouds solely is aware of its own part. during this paper, we tend to introduce a secure two-cloud information service architecture, wherever the 2 clouds are non-colluding and both of them is aware of solely a part of knowledge. supported this architecture, we tend to any propose a series of interaction protocols for a consumer to conduct numeric-related question over encrypted information from remote cloud servers. The numeric-related query includes common query statements, love larger than, less than, between.

II. LITERATURE SURVEY

Yin Yang, Hongwei Li, Mi Wen, Hongwei Luo, and Rongxing Luss, planned a positioned territory question (RRQ) plot [10], that support every reach inquiry and positioned search. discerned on the homomorphic Paillier cryptosystem, we have a tendency to tend to use two super-expanding arrangements to feature up to three-d watchwords. the primary is employed to feature up to a minimum of 1 buyer' or merchant' multidimensional catchphrases to a gathered variety. future one is claimed to making a summary range by gathering the collected amounts of all vendors. Security examination shows that RRQ will do the privacy of watchwords, affirmation, information reliability, and question protection.

Regardless, meanwhile loads of confusing pre-sifting rules, for the model, "and", "our", "not" isn't done by the RRQ system. R.A.Popa, C. Redfield, N.Zeldovich, and H.Balakrishnan planned CryptDB, a system to safeguard the personal information in information bases from at first the curious cloud worker itself and besides the appliance worker' deals. CryptDB is additionally a general sense incorporates victimisation the reach queries gainfully completed the encoded information employing a distinctive SQL-mindful cryptography framework. It restricts the knowledge open to the untrusted information base worker. nevertheless fulfilling the task of security protecting, still, hardly any data is revealed all the whereas. Rakesh Agrawal, Hun Kiernan, Ramakrishnan Srikant, Yirong Xu planned Order protective cryptography for Numeric information [11] that empowers Associate in Nursingy examination activity to be clearly concerning unstuck data.

Question results created are sound (no bastard hits) and complete (no fake drops). OPES (Order conserving cryptography Scheme) empowers correlation tasks to be expressly associated on scrambled data, while not unscrambling the operands. As wishes are, equilibrium and reach requests and so the MAX, MIN, and COUNT, cluster BY, and Request BY queries are sometimes expressly discerned finished scrambled information. OPES results are right and don't contain bogus positives, Associate in Nursing incentive throughout a section is often adjusted or Associate in Nursingother worth is commonly embedded throughout a phase whereas not requiring changes at intervals the cryptography of varied qualities and it alright might even be merely amalgamate with existing information base structures.

III. ARCHITECTURE

This project we tend to are develop mistreatment J2EE. we tend to used cloud as google drobox that is for cloud storage. In out project have 5 modules are there. Admin module, information supplier module, Cloud user module, 2 clouds (i.e. Cloud A and Cloud B). In Admin module module admin controls permission to data provider and cloud user and and so forth In data provider module, Registration and For Login information supplier get admin Permission and displaced person transfer data and data to cloud and look at all files. In Cloud user module have Registration, login data user and find permission from admin and user access the cloud files uploaded by information provider. If user desires to access the files 1st he should send request to cloud A and might conjointly transfer the files shared by Cloud B. Cloud A, It checks the user' request and question to cloud b and Cloud B, It receives the query from cloud A and sends the key to the user and user can download that file.. The sequence within which they're going to follow one another are clearly delineate within the Figure.

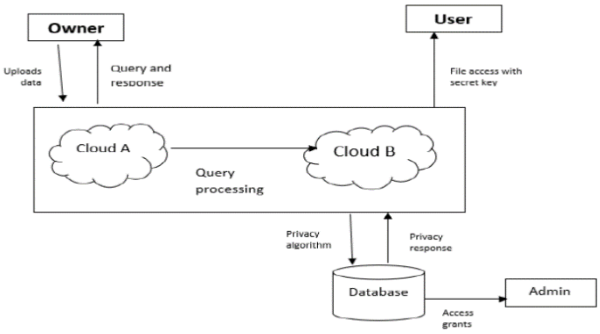

Fig-3.2: Architecture

IV. RESULTS AND CONCLUSION

1) Conclusions

We bestowed a two-cloud design with a series of interaction protocols for outsourced info service, that ensures the privacy preservation of knowledge contents, applied mathematics properties and question pattern. At constant time, with the support of vary queries, it not solely protects the confidentiality of static data, however additionally addresses potential privacy escape in statistical properties or when sizable amount of query processes. Security analysis shows that our theme will meet the privacy-preservation requirements. Furthermore, performance analysis result shows that our planned scheme is efficient. In our future work, we'll envisage to more enhance the safety whereas guaranteeing practicality, and we can extend our planned theme to support additional operations.

ACKNOWLEDGMENT

I would like to thank my mentor Dr. Deepak Sharma. through his guidance and vigilance, I've accomplished this, thank you sir.

REFERENCES

[1] Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu, and Peilin Hong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving", IEEE Transactions on Information Forensics and Security ,2017

[2] 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.

[3] 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.

[4] D. Zissis and D. Lekkas,"Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[5] 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, pp. 85–100, 2011.

[6] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, "Hosting services on an untrusted cloud," in Advances in CryptologyEUROCRYPT 2015. Springer, pp. 404–436, 2015.

[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, pp. 463–477, 2013.

[8] J.-M. Bofhli, 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] 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.

[10] Y. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving ranked range query in smart grid auction market," in 2014 IEEE International Conference on Communications (ICC2014). IEEE, Vol.2, No.4,April 2014.

[11] 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, pp.563–574, 2004.

[12] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, "Orderpreserving symmetric encryption," in Advances in Cryptology–EUROCRYPT 2009. Springer, pp. 224–241, 2009.

[13] 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, pp. 5490–5499, 2012.

[14] 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.

[15] Weiwei Kong, Yang Lei, Jing Ma (2017),"Data Security and Privacy Information Challenges in Cloud Computing", International Conference on Intelligent Networking and Collaborative Systems, IEEE.

[16] Hongbing Cheng, ChunmingRong, ManyunQian, and Weihong Wang (2018), "Accountable Privacy-Preserving Mechanism For Cloud Computing Based On Identity-Based Encryption", IEEE.