ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Confidential and Essential Two-Cloud Secure Database for Numeric-Related SQL Range Queries

Professor, M.E.Sanap[1] , Komal Bhujbal[2], Shital Gadekar[3] , Nitin Gaikwad[4] , Shubham Ghodke[5]

Associate Professor, Department of Computer Engineering, SAE, Kondhwa, Pune, Maharashtra, India[1]

U.G Students, Dept. of Computer Engineering, SAE College, Kondhwa, Pune, Maharashtra, India[2,3,4,5]

ABSTRACT: Business and people outsource database to acknowledge helpful and minimal effort applications and administrations. To give adequate usefulness to SQL queries, many secure database plans have been proposed. Be that as it may, such plans are helpless against security spillage to cloud server. The principle reason is that database is facilitated and prepared in cloud server, which is outside the ability to control of information proprietors. For the numerical range queries (">", "<", and so forth.), those plans can't give adequate security insurance against reasonable difficulties, e.g., protection spillage of measurable properties, get to design. Besides, expanded number of questions will unavoidably release more data to the cloud server. In this paper, we propose for secure database a two-cloud architecture, with a progression of convergence conventions that give protection safeguarding to different numeric-related range questions. Security investigation demonstrates that security of numerical data is emphatically ensuredin our proposed scheme against cloud providers.

KEYWORDS: database, range query, privacy preserving, cloud computing.

I. INTRODUCTION

The developing business of cloud has givean administration worldview of capacity/calculation outsourcing diminishes clients' weight of IT foundation support, and decrease the cost for both the ventures and individual clients. In any case, because of the security worries that the cloud specialist organization is accepted semi-trust (fair but curious.), it turns into a basic issue to put delicate administration into the cloud, so encryption or confusion are required before outsourcing touchy information -, for example, database framework - to cloud. One direct way to deal with alleviate the security danger of protection spillage is to encode the private information and shroud the inquiry/get to designs. Sadly, to the extent we know, few scholarly world explores fulfill the two properties up until this point. Crypt DB 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 encoded information also. Crypt DB utilizes a progression of cryptographic devices to accomplish these security usefulness. For that reason range inquiry has been proposed. In any case, such existing extent question plans are not appropriate for handy secure database because of high stockpiling overhead to keep up the comparing cipher text. In existing framework there is bolster for more than and not as much as operations. In proposed work we are supporting more operations, for example, "Entirety/AVG". Also, in proposed framework, we are really demonstrating the assault on one of the mists. But since of the aggressor can assault on single cloud at once and data is put away on two mists the assailant will be not able recover any development from single cloud.

II. RELATEDWORK

In [1] authors show the issue of information security in cloud information stockpiling, which is basically a dispersed stockpiling framework. To accomplish the affirmations of cloud information uprightness and accessibility and uphold the nature of tried and true distributed storage benefit for clients, we propose a viable and adaptable appropriated plot with express unique information bolster, includingaffix, erase and square refresh. We depend on deletion rectifying

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

code in the document dispersion planning to give excess equality vectors and assurance the information constancy. The reconciliation of information mistake limitation and capacity rightness protection in our plan accomplishes, by using the homomorphic token with disseminated check of deletion coded information i.e., at whatever point information defilement has been distinguished amid the capacity accuracy confirmation over the circulated servers, we can nearly ensure the synchronous recognizable proof of the acting mischievously server(s). Considering the time,the related online weight of clients and calculation assets, we likewise give the expansion of the proposed principle plan to help outsider reviewing, where clients can securely designate the respectability checking undertakings to outsider inspectors and be effortless to utilize the distributed storage administrations.In [2] authors show the Combined GDH and TGDH has been proposed which can improve the safe gathering sharing utilizing mystery keys among assemble individuals. In existing plan utilizing single key for amass sharing. The proposed conspire utilize different keys which abuses deviated keys. Utilizing bunch key understanding plan which successfully convey the mystery key to various subgroups. The calculation stack is dispersed among numerous subgroups and furthermore bolster forward and in reverse mystery. The gathering key refreshed when subgroup participation changes (join, leave) happens. At the point when the quantity of subgroup expands, O(n) steps is truly tedious to construct a tree. In [3] authors introduced Relational Cloud, a scalable relational database-as-a-service for cloud computing environments. Relational Cloud overcomes three significant challenges: efficient multi-tenancy, elastic scalability, and database privacy. For multi-tenancy, we developed a novel resource estimation and non-linear optimization-based consolidation technique. For scalability, we use a graph-based partitioning method to spread large databases across many machines. For privacy, we developed the notion of adjustable privacy and showed how using different levels of encryption layered as an “onion” can enable SQL queries to be processed over encrypted data. The key insight here is for the client to provide only the minimum decryption capabilities required by any given query. In [4] paper shows that the primitive of verifiable database with efficient updates is useful to solve theverifiable outsourcing of storage problem. However, the existing schemes cannot satisfy the property of incremental update, i.e., the client must re-compute the new ciphertext and the updated tokens from scratch each time. In this paper, we first introduce the notion of verifiable database with incremental updates (Inc.-VDB) that can lead to huge efficiency gain when the database undergoes frequently while small modifications. We have proposed additionally a general Inc.-VDB structure by fusing the primitive of vector responsibility and the scramble then-incremental MAC method of encryption. In [6] authors have proposed a new threshold multi-authority CP-ABE access control scheme, named TMACS, in public cloud storage, in which all AAs jointly manage the whole attribute share and set the master key α. Taking advantage of (t, n) threshold secret sharing, by interacting with any t AAs, a legal user can generate his/her secret key. we also construct a hybrid scheme that is more suitable for the real scenario, in which attributes different authority-sets and multiple authorities come from of the whole attribute set in an authority-set jointly maintain a subset. This enhanced scheme addresses not only attributes coming from different authorities but also system-level and security robustness.

III. PROPOSED SCHEDULINGALGORITHM

- Modified RSA Encoding/Decoding Recall the setup:

1. Select *p, q and r* any three prime nos. $p \neq q \neq r$
2. Calculate $n = p\ X\ q\ X\ r$ Its length is key length which is usually expressed in bits
3. Calculate $\emptyset(n) = (p-1)\ X\ (q-1)\ X\ (r-1)$
4. Calculate integer e such that
    - root of $n < e < \emptyset(n)$
    - $GCD(\emptyset(n), e)$ are co-prime
    - e is short bit length and small hamming weight
5. Compute X (to replace n)

• If $p>q$ then consider X such that $n - p < X < n$ *and* $GCD(X, n) = 1$
• If $p<q$ then consider X such that $n - q < X < n$ *and* $GCD(X, n) = 1$

6. Calculate d such that $d \equiv e-1 (mod\ \emptyset(n))$
7. Now the Public key PU = [e, X]
8. Now the Private key PR = [d, X]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

9. Consider plain text M, $M < n$
10. Find cipher of plain text by $C = M \ emod \ X$
11. Transmit the coded message to receiver by sender
12. Find plain text from cipher by receiver using $M = Cdmod \ X$

IV. PSEUDO CODE

Step 1: Choose three prime numbers p, q and r.
Step 2: Calculate n such that
n=pXqXr.
Step 3 : Calculate modulus,
$Ø\ (n) = (p-1)\ X\ (q-1)\ X\ (r-1)$
Step 4: Calculate integer e which is short bit length and small hamming weight
(root of $n < e < Ø\ (n)$ && $GCD(Ø\ (n), e)$ are co-prime)
Step 5: Compute X (to replace n)
if (p>q)
consider X such that$(n- p) < X < n$ and $GCD(X, n) = 1$
else if $(p<q)$
consider X such that $(n-q) < X < n$ and $GCD(X, n) = 1$
Step 6: Calculate d
$d \equiv e-1 (mod\ Ø\ (n))$
Step 7: PU = [e, X]

Step 8: PR = [d, X]
Step 9: If (M<n)
$(C = M \ emod \ X \&\& M = Cdmod \ X)$

V. SIMULATION RESULTS

1. Existing System

The typical scenario for outsourced database is described in Fig. 1 as that in CryptDB: A cloud client, such as an IT enterprise, wants to outsource its database to the cloud, which contains valuable and sensitive information (e.g. transaction records, account information, disease information), and then access to the database (e.g.SELECT, ALTER and UPDATE). Cloud provider is honest-but-curious due to the assumption that the cloud might try his/her best to obtain private information for his/her own benefits. For profit the cloud could forward such sensitive information to the business competitors, operating riskwhich is an unacceptable. The privacy challengeis two-hold of outsourced database. Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers; Besides data privacy, clients' frequent queries will inevitably and some private information on data statistic propertiesgradually reveal. Thus, data and queries of the outsourced database should be protected against the cloud service provider.

Weaknesses of Existing System:-In fig[1] shows existing graph, we are not sure that whether it is actually secure or not for the clients to deploy their essentialon cloud Servers.
As The Existing and Proposed System Graphfig[1] shows. From that we conclude that Proposed System is good as comparative to Existing System.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

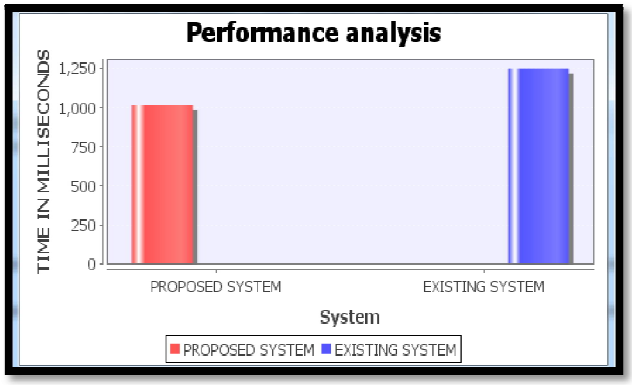

Fig.1. Existing System VS Proposed System

2. Proposed System

We propose two non-colluding cloud architecture to conduct a secure database service, in which the data is stored in one cloud and the query logic in second cloud and knowing only one cannot reveal any private information. We then present a series of intersection protocols to provide numeric-related SQL range query with privacy preservation, and especially, such protocols will not expose order-related information to any of the two non-colluding clouds.
Infig[1] shows proposed graphwe are supporting more operations, such as “SUM/AVG”. And in proposed system, we are actually showing the attack on one of the clouds. But because of the attacker can attack on single cloud at a time and information is stored on two clouds the attacker will be unable to retrieve any formation from single cloud.

VI. CONCLUSION

In this paper, we introduced a two-cloud design with a progression of communication conventions for outsourced database benefit, which guarantees the privacy preservation of statistical properties, information substance and query pattern. In the meantime, with the help of range queries, it ensures the classification of static information, but also addresses potential privacy leakage in statistical properties or after substantial number of inquiry forms. Security examination demonstrates that our plan can meet the protection safeguarding necessities. Moreover, execution assessment result demonstrates that our proposed scheme is proficient.

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. 1, 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. 2, pp. 459–470, 2014.
4. J.W. Rittinghouse and J. F. Ransome, “Cloud computing: implementation, management, and security”, CRC press, no.2, 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. 2, 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, pp. 3184–3195, 2016.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

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, 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, pp. 1484-1496, 2016.