International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN (P): 2249-6831; ISSN (E): 2249-7943
Vol. 8, Issue 4, Oct 2018, 13-20

TRANS STELLAR
•Journal Publications •Research Consultancy

PRIVACY PRESERVING FOR NUMERIC DATA QUERY IN CLOUD COMPUTING

B. SPANDANA[1], S. ZAHOOR-UL-HUQ[2] & P. PENCHALA PRASAD[3]

[1]*Student, Department of Computer Science and Engineering, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India*

[2]*Professor, Department of Computer Science and Engineering, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India*

[3]*Assistant Professor, Department of Computer Science and Engineering, G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India*

ABSTRACT

In the present situation, organizations and individuals are outsourcing database to limit their exertion and to get a minimal effort benefit. Keeping in mind the end goal to give the adequate usefulness to SQL inquiries, numerous safe database plans have been proposed. Be that as it may, such plans are defenseless against protection spillage to cloud server. For numerical range request (>, <, etcetra) these disregard to give sufficient security protection. A part of the challenges confronted are the security spillage of factual traits, get to examples et cetera. In like manner the expanded number of inquiries will discharge more data to the cloud server. We have considered a portion of these examination works and dissected the most ideal approaches to go to the coveted level of security protection on account of distributed computing. We have proposed two cloud engineering for secure database, with a progression of crossing point conventions that give protection safeguarding to different numeric related range questions. Security examination demonstrates that security of numerical data is firmly ensured against cloud suppliers in our proposed conspire.

KEYWORDS: ***Database***, ***Range Query***, ***Privacy Preserving*** & ***Cloud Computing***

Received: Jul 11, 2018; **Accepted:** Aug 01, 2018; **Published:** Sep 17, 2018; **Paper Id.:** IJCSEITROCT20183

Original Article

1. INTRODUCTION

In the current conditions, it can be seen that the cloud has taken the control over the IT business with its multitudinous favourable circumstances. Distributed computing is suggested as SaaS (Software as a Service) since it renders the applications as organizations over the Web and the equipment and frameworks programming in the server farms that offer those organizations. The equipment of the server farm and programming is known as a cloud. Today the mists can be open/open and likewise private. Private mists are related to the inward datacenters of a business or other affiliation, not made open to the general open. Distributed computing in this way can be compacted as a mix of SaaS and utility figuring, booting out the server farm (little + medium assessed).

Security is the main worry of the distributed computing. Cloud customers stand up to security perils both from outside and inside the cloud. Because of the security concerns, the cloud specialist organization is expected semi-trust (genuine yet inquisitive.), It turns into a basic issue to put touchy administration into the cloud, so encryption or obscurity is required before outsourcing delicate information -, for example, a database framework.

A cloud customer, for example, an IT undertaking, needs to outsource its database to the cloud, which contains profitable and touchy data (e.g. exchange records, account data, infection data), and after that entrance to the database (e.g. SELECT, UPDATE, and so on.). Because of the suspicion that cloud supplier is straightforward, however inquisitive, the cloud may attempt his/her best to acquire private data for his/her own advantages. Much more terrible, the cloud could forward such delicate data to the business contenders revenue driven, which is an unsuitable working danger.

Protecting the data from the server itself is the expert of the fundamental issues related with it. The server will by definition control the "base layer" of the item stack, which sufficiently circumvents most known security techniques.

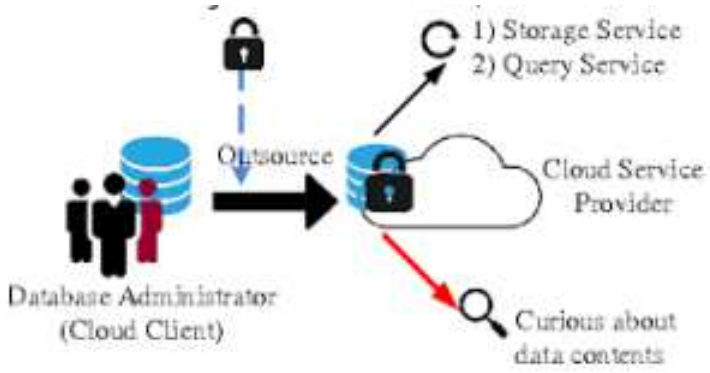

Figure 1: Outsourced Database, Service and Privacy Risk

One clear way to deal with alleviate the security danger of protection spillage is to encode the private information and shroud the question/get to designs. CryptDB is utilized for such reason. CryptDB, a system that offers privacy to applications that use database organization structures. CryptDB licenses to perform questions over the scrambled information, in like manner the SQL's especially portrayed arrangement of administrators, and inquiries over encoded information.

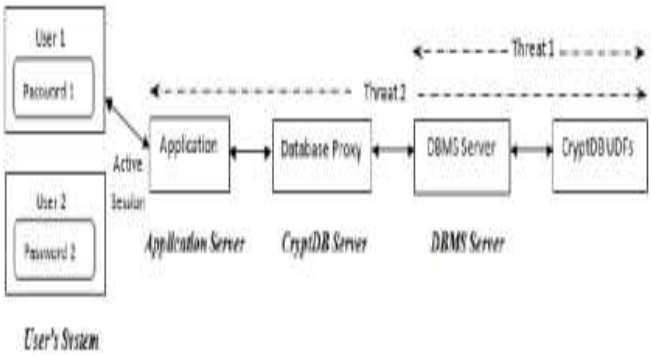

Figure 2: CryptDB Architecture

CryptDB watches out for the danger of a curious Database chairman (DBA) who attempts to learn private data (e.g., wellbeing books, budgetary explanations, singular information) by watching out for the DBMS server by shielding the DBA from learning private data. It utilizes a couple of instruments to achieve this security usefulness. One of the gadgets being the Order protecting encryption (OPE) is for the most part used as a piece of databases to process SQL Queries over scrambled data. It grants to perform, arrange tasks on ciphertext like the plaintext for e.g. information server can manufacture file and sort the scrambled data like the plaintext. Notwithstanding setting off to the security reason

well, in spite of everything, it reveals the request of the ciphertext, the determination of the measurable properties, for example, the information dissemination and the entrance design. In this manner the target of security insurance of the outsourced data to a cloud server is refined by apportioning the delicate learning into two sections and stores them in two non-intriguing mists. Also a protected database benefit design is recognized by using two non-conniving mists in which the data learning and inquiry reason are partitioned into two mists. Hereafter, seeing only a solitary cloud can't help reveal private information. Other than a movement of crossing point conventions to give numeric-related SQL run questions with protection safeguarding is furthermore executed and it won't reveal arrange related information to any of the two non-conniving mists.

2. SYSTEM ARCHITECTURE

Our proposed secure database framework incorporates a database executive, and two non intriguing mists. In this model, the database executive can be actualized on a customer's side from the viewpoint of cloud benefit. The two mists (allude to Cloud A and Cloud B), as the server's side, give the capacity and the calculation benefit. The two mists cooperate to react each question asked from the customer/approved clients (accessibility). For security concerns, these two mists are thought to be non-plotting with each other, and they will take after the crossing point conventions to protect the security of information and questions (protection). In our plan, the learning of put away database and questions is apportioned into two sections, individually put away in one cloud. The instrument ensures that knowing both of these two sections can't get any helpful security data. To lead a protected database, information is scrambled and outsourced to be put away in one (Cloud A), and the private keys are put away in the other one (Cloud B).

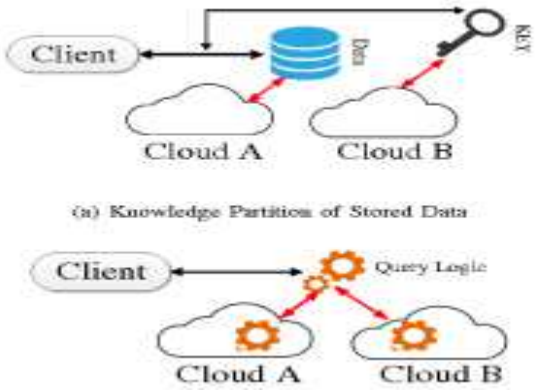

Figure 3: Two Cloud Database and Architecture

For each inquiry, the comparing learning incorporates the information substance and the relative handling rationale. We use a model of information segment, partitioning application rationale into two sections, which is right off the bat proposed by Bohli et al. in. The application rationale, as mystery information, is divided into two sections, every one of which is just known to one cloud. Instinctively, this cloud engineering expands some many-sided quality to some degree, and we will investigate and call attention to that this overhead is worthy.

3. LITERATURE REVIEW

Wei Li, Kaiping Xue, Yingjie Xue "TMACS: A Robust and Verifiable Threshold Multi Authority Access Control System in Public Cloud Storage" to fulfil the prerequisites of information stockpiling and elite calculation, distributed computing has drawn broad considerations from both scholarly and industry. Distributed storage is a critical administration

of distributed computing, which gives administrations to information proprietors to outsource information to store in cloud by means of web.

Jiawei Yuan, Shucheng Yu "Adaptable and Publicly Verifiable Aggregation Query for Outsourced Databases in Cloud" For anchoring databases outsourced to the cloud, it is essential to permit cloud clients to confirm that their inquiries to the cloud facilitated databases are effectively executed by the cloud. Existing arrangements on this issue experience the ill effects of a high correspondence cost, a substantial stockpiling overhead or a staggering computational cost on customers. Plus, just basic SQL questions (e.g., choice inquiry, projection question, weighted total question, and so on) are upheld in existing arrangements.

Xiaofeng Chen, Jin Li, Jian Weng "Irrefutable Computation over Large Database with Incremental Updates" With the accessibility of cloud benefits, the procedures for safely outsourcing the restrictively costly calculations are getting far reaching consideration in mainstream researchers. That is, the customers with asset imperative gadgets can outsource the overwhelming calculation workloads into the untrusted cloud servers and appreciate the boundless figuring assets in a compensation for each utilization way.

Arnaud Castelltort and Anne Laurent "Fluffy Queries over No SQL Graph Databases: Perspectives for Extending the Cipher Language" When questioning databases, clients regularly wish to express ambiguous ideas, with respect to occurrence requesting the shoddy lodgings. This has been broadly considered on account of social databases. In this paper, we propose to examine how such valuable strategies can be adjusted to No SQL diagram databases where the part of fluffiness is vital.

4. PRELIMINARIES AND DEFINITIONS

Paillier Cryptographic Algorithm

There are different cryptographic procedures to help numeric-related tasks (e.g. expansion, increase, XOR) upon the encryption field. Paillier cryptosystem [41] is a standout amongst the most prevalent procedures that give expansion homomorphic, which implies: in the event that two whole numbers and b are scrambled with a same key k into two ciphertexts (be meant as Ek(a) and Ek (b)), there exists a task (allude to as "⊗"), to such an extent that Ek(a)⊗Ek(b)= Ek(a+b). Paillier cryptographic calculation is made out of the accompanying stages: key age, encryption and decoding.

Key Age: Two extensive and autonomous prime numbers p and q are haphazardly chosen. At that point we process n = p•q and μ=λ−1 mod n, where λ is the minimum basic numerous of p and q, and generally λ = lcm (p −1, q −1). The general population key (PK) is n, and the private key (SK) is (λ, μ).

Encryption: Give m a chance to be the whole number to be encoded. Right off the bat, we select an arbitrary number ∈ Z∗ n2, and after that the ciphertext of m can be figured as takes after: E(m;r)=(n+1)m •rn mod n2.

Decryption: Let the ciphertext c = E(m;r). The plaintext m can be recouped as takes after: m =(cλ mod n2) −1 n •μ mod n.

Paillier cryptosystem holds added substance homomorphic in assemble Z+ n, which compares to the augmentation task in the encryption field in Zn2. The accompanying condition delineates the homomorphic property of Paillier cryptosystem. E(m1;r1)• E(m2;r2) = (n+1)m1rn 1 •(n+1)m2rn 2 = (n+1)m1+m2(r1 •r2)n = E(m1+m2;r1 •r2)

Another property can be outlined as takes after: Em2(m1;r1) = ((n+1)m1rn 1)m2 = (n+1)m1•m2(r1m2)n =

E(m1•m2;rm2 1).

As the irregular number r does not influence the aftereffect of decoding in Paillier encryption, can be viewed as the result of m1 and m2 in the encryption field. Whatever is left of this paper, we utilize E(m, PK) to signify the encryption aftereffect of the plaintext m with PK, and D(X, SK) to indicate the unscrambling result. We utilize capital letters like "X" to signify scrambled outcomes (ciphertext), and lowercase letters like "x" to mean decoded comes about (plaintext). The irregular number r ∈ Z∗ n is discarded in the discourse of our plan. For number examination, the indication of a plaintext number in Paillier cryptosystem is characterized as takes after: each took an interest plaintext whole number x is thought to be x < n/2. At that point for lucidity, the indication of x is characterized to be certain if 0 < x < n/2, and the sign is characterized to be negative if x > n/2. Subsequently, the number juggling subtraction of self-assertive two whole numbers (xi−xj) won't surpass the limit n/2 ifxi>xj, and the subtraction will surpass n/2 ifxi<xj.

Numeric-Related SQL Queries

The Structured Query Language (SQL) is a predefined reason programming dialect, which is utilized to oversee information in a social database framework, which has turned into a standard of the ANSI and ISO in 1986 and 1987 individually. An inquiry task can ask for discretionary information with an announcement to portray the coveted information. The asked for information can be a few sections of at least one table in the database, and it can likewise be collected outcomes from the first information, (for example, entirety, normal, and check of the datum.). To get the coveted information, the inquiry contains a few explanations to depict the prerequisite, e.g. some numeric related (">", "<", "BETWEEN", and so on) for clearness, we allude to those questions asked for as numeric related SQL inquiries in whatever remains of the paper. In view of the presented two cloud engineering, we additionally propose a progression of connection conventions between the customer and the two mists, which can understand numeric related SQL questions, and fulfil protection necessities. It ought to be noticed that, aside from the question task, there are other SQL activities (e.g. refresh, embed) which change the information. The security issue for such cases can be settled with other existing methodologies, for example, ORAM (Oblivious RAM) which is past the extent of our paper. In this paper, we center around actualizing inquiry task with security protecting.

5. SECURITY ANALYSIS

In this area, we will center around the protection conservation in the outsourced inquiry forms against two genuine however inquisitive mists.

Security Proof Theorem 1

Cloud A can't acquire any data from the client's question and the put away encoded database as long as Paillier cryptosystem is semantically secure, and Cloud An and B are non-plotting. Evidence: In these means, since every one of the information got by Cloud An is scrambled and the calculation steps are altogether performed in the ciphertext space, and due to the semantic security of Paillier cryptosystem, Cloud A can't find any private data from these three stages except if Cloud B connives with it.

Theorem 2: Cloud B can't gather any private data from Cloud A's contribution insofar as blinding elements are appropriately created, and Cloud An and B are non plotting.

Privacy Preservation in Repeated Queries

The mists could gather increasingly factual data subsequent to getting rehashed inquiry asks for and producing the comparing reactions towards the database (e.g. Figure 3). Notwithstanding, we will exhibit that our plan can decrease the security spillage significantly in this situation. 1) For Cloud A: Repeated question solicitations will make Cloud A take in more and more about the security data, while in our plan, this capacity is confined as takes after. On one hand, numerous inquiry demands are traversing various sections, and basic question demands are only a piece of normal database question demands. In such a circumstance, Cloud An exclusive gets the last file result (with fakers, alternatively) from Cloud B sifted with numerous conditions, it can't get the first correlation consequence of every one segment. Then again, Cloud B reacts Cloud an in view of the token got from the customer, and there have two different ways to ensure the security.

- Each token contains the particular segment number (CN) and the aggregate thing number in the table (N), which Cloud An unquestionable requirement work on precisely. Cloud An absolute necessity send the outcome to Cloud B precisely with these two numbers without alteration: If Cloud An increments or reductions CN or N, Cloud B will locate that unmatched with the token, and if Cloud A replaces anything in these CN segments, it will go out on a limb of reacting incorrectly result to customer, which can be expected not happening in light of the presumption that semi confided in mists are straightforward. 2) Each token has been marked with SK by customer, Cloud A can't alter any tokens or produce another one, and each token contains an alternate serial number and timestamp, so Cloud A can't lead the replay assault.
- For Cloud B: The name of each included segment is expelled before sending to Cloud B, and then, unique arbitrary whole numbers are chosen for everything in each question ask for by Cloud A. Accordingly, Cloud B can't recognize whether two past question demands are on a similar section, subsequently rehashed inquiries can't be used to expanding the exactness of request speculating. Also, in light of thing rearranged, Cloud B can't recognize one same thing from two past questions, despite the fact that the plaintext SQL inquiries are indistinguishable.

6. CONCLUSIONS

In this paper, we have contemplated the different procedures and conventions related with the protection safeguarding of the outsourced information to the outer cloud server. Arranged by the progress in this field a portion of the works incorporates the fluffy rationale, extend questions, arrange protecting encryption and multi cloud engineering. The fluffy rationale actualized the, Beacon Guided Search (BGS), which requires considerably less memory and no intricate stockpiling instrument. The Range Queries work by executing the RRQ can achieve classification of catchphrases, affirmation, information respectability and inquiry protection. At that point came the CryptDB which in a general sense incorporates using the range questions gainfully completed the encoded data using a novel SQL mindful encryption framework. Anyway a few information is as yet presented to the cloud server. The request protecting encryption is one of the instruments utilized by the CryptDB which empowers correlation tasks to be particularly associated on encoded data, without unscrambling the operands. However, encryption of non numeric data isn't conceivable with this instrument. Later the multi cloud design was presented which presented apportioning the touchy data and inquiry rationale into two diverse non-conspiring mists which don't have the learning about each other. Anyway, this design doesn't remain constant for inquiries, for example, SUM/AVG.

REFERENCES

1. *R. A. Popa, C. Redfield, N. Zeldovich,* and *H. Balakrishnan*, "*CryptDB: Protecting confidentiality with encrypted query processing*".
2. *C. Curino et al*. (*2011*). *Relational Cloud: A Database-as-a-Service for the Cloud*.
3. *D. Boneh, D. Gupta, I. Mironov,* and *A. Sahai*, "*Hosting services on an untrusted cloud,*" *in Advances in Cryptology*.
4. *X. Chen, J. Li, J. Weng, J. Ma,* and *W. Lou*, "*Verifiable computation over large database with incremental updates*".
5. *X. Chen, J. Li, X. Huang, J. Ma,* and *W. Lou*, "*New publicly verifiable databases with efficient updates*".
6. *S. Benabbas, R. Gennaro,* and *Y. Vahlis*, "*Verifiable delegation of computation over large datasets*".
7. *W. Li, K. Xue, Y. Xue,* and *J. Hong*, "*TMACS: A robust and verifiable threshold multi authority access control system in public cloud storage*".
8. *H. Kadhem, T. Amagasa,* and *H. Kitagawa*, "*MVOPES: Multi valued order preserving encryption scheme: A novel scheme for encrypting integer value to many different values*".
9. *Khanna, N., Behar, N.,* & *Yadav, N.* (*2016*). *Improved Algorithm for Dynamic Memory Allocation in Cloud Computing*.