Latent Information towards Various Numerical Related SQL Queries

[1]J.Vaishnavi, [2]Dr. Aruna Varanasi, [3]Dr. Prasanta Kumar Sahoo
[1,2,3]Dept. of CST, Sreenidhi Institute of Science and Technology, JNTUH University, Telangana, India

Abstract
In present situation many multinationals and people utilize database to understand suitable administrations and minimal effort applications. So, to implement sufficient performance for SQL queries, various safe database programs have been proposed. Though, such schemes are unsafe to privacy leakage to cloud server. The databases are covered inside the cloud server, which is over the control of information proprietors. The SQL Queries require a few secure collection of data scheme for its clear working, yet sometimes this prompts privacy spillage to the cloud server.For the numerical range request (“>”, “<”, and so on.), these plans can’t give sufficient security assurance against reasonable difficulties. Moreover, increased number of queries will necessarily leak more data to the cloud server. Thus numerous work have been done by various researchers regarding these issues. We have studied some of these research works and determined the best possible ways to come to the desired level of privacy preservation in the case of cloud computing. Few works which were studied are the fuzzy logic, range queries, CryptDB order preserving encryption and multi-cloud architecture.

Keywords
Database, Information, Cloud Server

I. Introduction

In the present state as it can be seen that the cloud has taken the command over the IT work with its countless advantages. It holds the opportunity to change a thorough segment of the IT trade, making system substantially more agreeable as a service. Distributed computing is alluded as SaaS (Software as a Service) as it executes the applications as control over the net and the equipment and programming frameworks in the server farms that offer those organizations.
The hardware of data centre and software is called a cloud. The clouds can be in public and private. Private clouds are combined to the inner datacenters of a company or other corporation, which is not made available to the public. In this manner Cloud computing can be compressed as a mixture of saas and function computing, booting out the data centre.The major concern of cloud computing is the security. Cloud clients meet the security dangers which arise both from outside and inside the cloud.Protecting the data from the server is itself main issue. Because of the responsibility of the protection the cloud specialist co-op is thought to be semi-put stock in (legitimate however inquisitive.), it turns into a noteworthy issue to put the touchy information into the cloud, so encryption or obscurity are required before sending delicate information.

CryptDB, is a structure that offers security to the applications that utilize the database organization plans (DBMSes). It offers agreement to perform questions over scrambled data,in that expansion the SQL’s are characterized set of administrators, and inquiries over encoded information. It prompts go out on a limb of an inquisitive database executive (DBA) who endeavors to learn private data (e.g., well being books, budgetary explanations, singular information) by watching out for the DBMS server and by shielding the DBA from learning private data. To achieve this security execution it utilizes a couple of instruments.

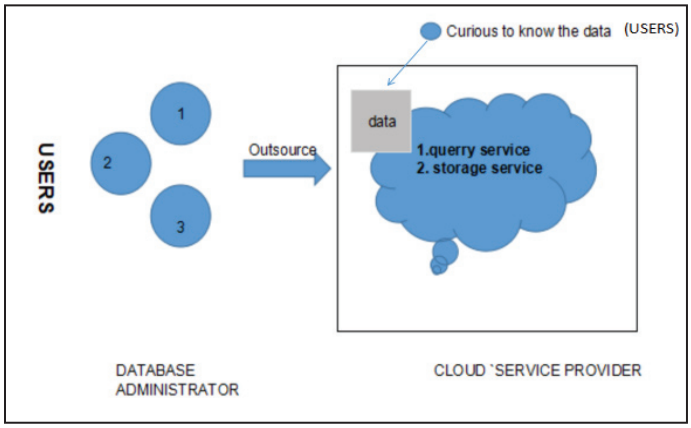

Fig. 1: Architecture

Few devices being the Order Preserving Encryption (OPE) is generally used as a part of databases to process SQL queries over encrypted data. It gives permission to perform operations in an order on ciphertext like the plaintext for e.g. data server can build index perform range queries and arrange the encrypted data like the plaintext. For security reason in spite of everything it uncovers the order of the ciphertext.

Thus the goal of security protection of the expanded data to a cloud server is precise by dividing the sensitive knowledge into two parts and store them in two non-colluding clouds.

Additionally a safe database service architecture is confirmed by using two non-colluding clouds in which the information learning and query rationale is divided into two clouds. Henceforth, perceiving just a single cloud can’t help uncover private data. Other than a progression of intersection protocols to give numeric-related SQL range queries with privacy preservation is additionally executed and it won’t uncover order related data to any of the two non-colluding clouds.

A. Motivation

Confidentiality is the best essential aspect in the cloud and the other information storage services. Numerous makers tackled security assurance, yet private information can’t be completely ensured by some system. Every person has some hidden and isolated documents which they won’t share to anyone likewise all companies have abundant secret data, which they won’t convey the data to anyone. On the off chance that any of the data is released the association’s setback is certain shot. With the objective that we are turning on insurance of the delicate data. Display day advancement furthermore tackles protection safeguarding in the cloud servers.

II. Related Work

John Daugman, and Piotr Zielinski have proposed a speed scan calculation for an expansive fuzzy database that stores iris codes or information with a relative parallel structure.The confused type of iris codes and their extreme depth is controlled by new process, Beacon Guided Search (BGS), which does as such by scattering an extensive number of "reference points" in the hunt clear. BGS is significantly fast than the existing ES with an irrelevant loss of accuracy. It takes considerably very limited memory and it doesn't trust at the time of caching information in the storage, this is the way of taking out the requirement for composite storage administration. The preprocessing is fundamental and lively. It holds up to 30% piece mistakes in the question and furthermore up to seven cyclic revolutions. The wealth memory put is close to nothing and expeditiously affordable– it supports dynamic upkeep, enabling straightforward requesting of new books.

R.A.Popa, C. Redfield, N.Zeldovich and H.Balakrishnan proposed CryptDB, a structure to protect the secret data in databases from the curious cloud server itself and the application server's agreement. Essentially, CryptDB includes making use of the range queries effectively, refining the encrypted data utilizing a new SQL-aware encryption system.It confines the information revealed to the untrusted database server. Although fulfilling the task of insurance shielding, still a couple of data is revealed all the while.

Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu proposed Order Preserving Encryption for Numeric Data that empowers any correlation task to be direct associated on scrambled data. Query results delivered are sound and finish.OPES (Order Preserving Encryption Scheme) allows relational operations to be connected particularly on encrypted data without decrypting the operands. In this manner, adjust and go request and furthermore the MAX, MIN, and COUNT , GROUP BY and ORDER BY questions can be particularly arranged over scrambled data. OPES comes about are right and don't contain false positives, an incentive in a section can be altered or another esteem can be embedded in a segment without requiring changes in the encryption of different qualities and it can be easily joined with existing database systems. Encryption of non-numeric data, for instance, factor length strings aren't done by OPES. Likewise while applying SUM or AVG to a gathering the qualities ought to be decoded.

J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, N. Marnau, proposed the Security and privacy-enhancing multicloud architecture. This paper works as an overview paper where it talked about the security in open cloud and in multiple cloud. In this paper he writers also discussed about the high potential for security prospects in cloud computing. Homomorphic encryption and secure multiparty calculation protocols were encouraging in both technical security and regulatory compliance. However there is no single unique way to deal with cultivate both security and legal compliance in an omni applicable way. The bounds of these methodologies originated from their restricted applicability and high multifaceted nature being used.

III. System Architecture

Our system architecture involves a database administrator and two non intransitive clouds.Here, the database administrator can be executed on a customer's side in the clouds point of view. The two clouds (Cloud A and Cloud B), act as the server's side which provides the storage and the computation service briefly describes the architecture of our secure database system in our device.

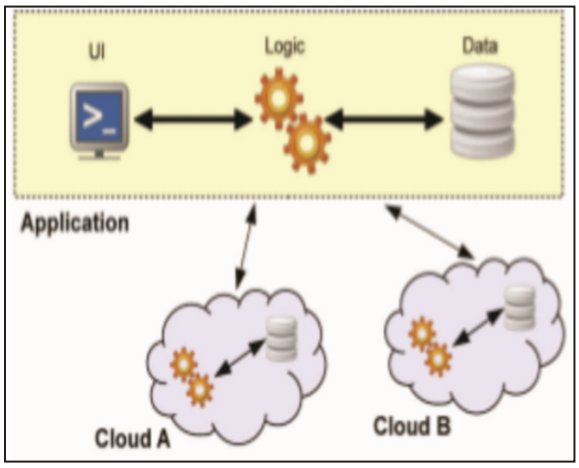

Fig. 2: Data is Stored in Two Clouds

The two clouds cooperate to react each query request from the customer/approved clients (accessibility). For protection concerns, these two clouds are thought to be non-conspiring with each other, and they will follow the convergence protocols to safeguard security of information and queries (security).

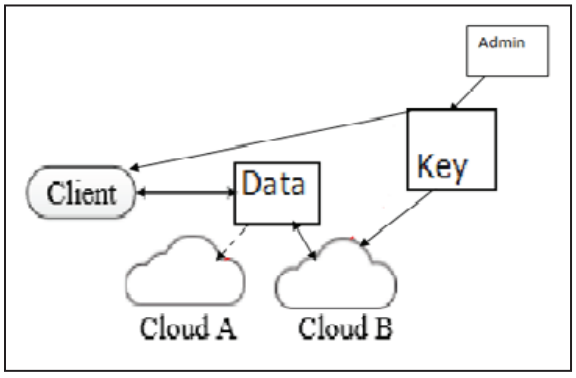

Fig. 3: Knowledge Partition of Stored Data

In our scheme,the knowledge of stored database and inquiries is divided into two sections, individually gathered in one cloud. The component ensures that knowing both of these two sections can't be used for protecting data. As in Fig 3.

To administer a safe database, information are scrambled and outsourced to store in Cloud A, and the private keys are put in the Cloud B. For each question, the corresponding information incorporates the information substance and the relative handling rationale. We use a model of information segment, isolating application rationale into two sections, which was first proposed by Bohli et al. The application rationale, as a secret learning, is divided into two sections, each of which is known to one cloud. This model is appeared in Fig. 4. Instinctively, this two-cloud design expands some complexity quality to some extent.

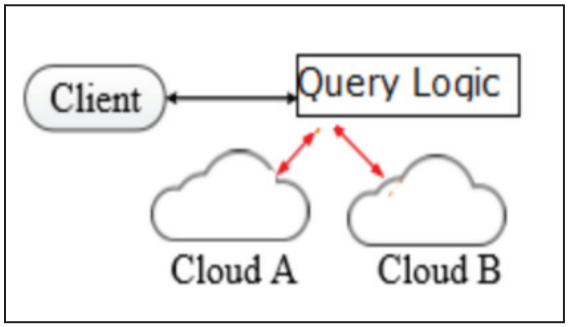

Fig. 4: Knowledge Partition of Query Data

IV. Algorithm

Here, we use Advanced Encryption Standard (AES) algorithm. AES is an Encryption standard chosen by National Institute of Standards and Technology (NIST) in 2001, USA to protect classified information.It is block cipher which operates on block size of 128 bis for encrypting and decrypting.Each round performs same operations.It basically repeats four major functions to encrypt data. It takes 128 bit block of data and key and gives cipher text as output. The functions are Sub Bytes, Shift Rows, Mix Columns, Add Key. This algorithm depends on the key size.

Table 1: Number of Rounds Taken for Key Sizes in Bits

Key Size (in bits)	Rounds
128	10
192	12
256	14

The larger the number of keys the more secure will be the data.

A. Working

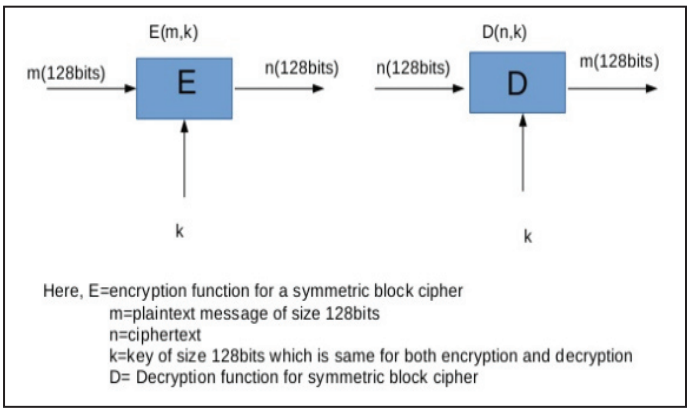

Fig. 3: Working of AES Algorithm

B. High-level Description of the Algorithm

KeyExpansion—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

Initial round key addition:

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

9, 11 or 13 rounds:

SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
MixColumns—a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
AddRoundKey
Final round (making 10, 12 or 14 rounds in total):
SubBytes
ShiftRows
AddRoundKey

V. Algorithm 2

Random Key Generator is used to generate keys randomly.RSA is the first public key algorithm.It uses two different keys for encryption and decryption.This algorithm can be used for public key generators and digital signature purpose also.

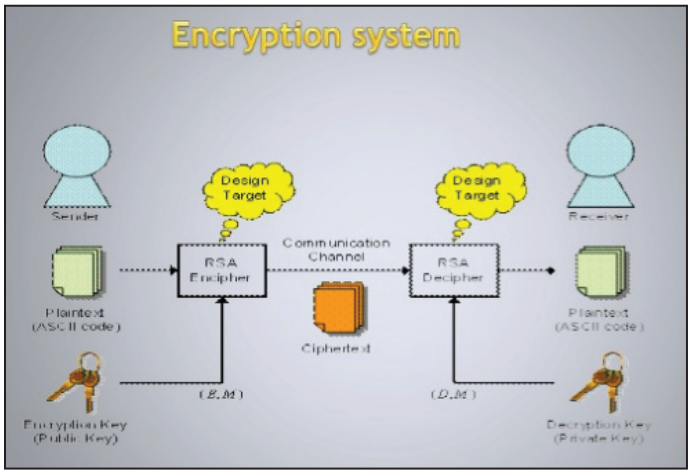

Fig. 4: Encryption System

The keys which are used for encryption and decryption are public and private keys.Public keys are stored in such away that the public can easily get access to those keys. The sender of message encrypt the data using receiver's public key and the receiver decrypt using its own private key. That is the reason no one can intercept the data except the receiver.

Steps For RSA Algorithm:

Step 1: We select the two largest prime numbers P and Q to calculate the key.
Step 2: Calculate the system modulus -N of P and Q which is common for both public and private keys.

N=P*Q

Step 3: Calculate encryption key (E) by taking the factors of (P-1)*(Q-1). We choose E such that E should not divide by any factor of (P-1)*(Q-1).
Step 4: Calculate decryption key (D) such that
(E*D) mod (P-1)(Q-1)=1
(P-1)(Q-1) * K+1= value1, value 2,....
When k= 1,2,3,4,.....
Step 5: Encryption

$$CT=PT^{E} Mod\ N$$

Step 6: Decryption

$$PT=CT^{D} Mod\ N$$

VI. Conclusion

In this paper we concluded it by providing a dual cloud with a series of interaction protocols and 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. We used RSA algorithm for key generation and AES algorithm for encryption and decryption of files.By using these algorithms the cloud can be highly secured.

References

[1] Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu, 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, 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, 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, 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, A. Sahai,"Hosting services on an untrusted cloud", In Advances in Cryptology EUROCRYPT 2015. Springer, pp. 404–436, 2015.
[7] R. A. Popa, F. H. Li, 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, 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, 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, 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, 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, A. Oneill, "Orderpreserving symmetric encryption," In Advances in Cryptology–EUROCRYPT 2009. Springer, pp. 224–241, 2009.
[13] M. A. AlZain, E. Pardede, B. Soh, 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.