Volume 5, Issue 4, October 2018 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Privacy Preserving for Numeric Data Query in Cloud Computing

P. Kiran Kumar
Assistant Professor,
Department of Computer Science and Engineering
Sri Indu College of Engineering & Technology
Ibrahmipatnam (T.S) [INDIA]
Email: prasadch204@gmail.com

S. Soundraya
PG Scholar
Sri Indu College of Engineering & Technology
Ibrahmipatnam (T.S) [INDIA]
Email: soundharyareshma579@gmail.com

N. Ashwini
PG Scholar,
Sri Indu College of Engineering & Technology
Ibrahmipatnam (T.S) [INDIA]
Email: ashwinin528@gmail.com

Y. Kavya Sri
PG Scholar
Sri Indu College of Engineering & Technology
Ibrahmipatnam (T.S) [INDIA]
Email: sri.kavya.008@gmail.com

ABSTRACT

In this paper we propose cloud environment for secure database with a series of intersection that provide privacy preservation to various numeric-related range queries.

Outsource database to realize convenient and low-cost applications and services. Querying many applications to provide sufficient functionality for database schemes. Privacy leakage to cloud server vulnerable process beyond the owners control cannot provide privacy protection.

Keywords:— *database, querying, privacy preservation*

I. INTRODUCTION

The increasing growth of cloud has provide a service for storage and outsourcing to reduce it infrastructure maintenance and reduce the cost for both the privacy concerns that the cloud service provider is assumed semi-trust it becomes a critical issue to put sensitive service in the cloud, so encryption or decryption are needed before outsourcing sensitive data such as database system to cloud.

A cloud client such as an IT enterprise wants to outsource its database to the cloud, which contains valuable and sensitive information and then access to the database. Due to the assumption that cloud provider is the honest one, the cloud might try her best to obtain private information for their benefits. Even worse the cloud forward such sensitive information to the business competitors for profit, which is an unacceptable operating risk.

The outsources data of the cloud clied have the following challenges:

1. Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers.
2. The data privacy clients frequent queries will gradually reveal some private information on data statistic properties.
3. Data and queries of the outsources database should be protected against the cloud service provider.

The above approach to mitigate the security risk of private data and hide the query/ access patters. The preserving encryption is utilized to realize numeric related range query processes. The perspective of query

functionality crypt support most kinds of numerical queries with such cryptography. Privacy preserving and well query processed with relatively privacy assurance and confidentiality.

II. OBJECTIVE

Security risk of privacy leakage is to encrypt the private data and hide supported numerical related data for query processing and functionality. Privacy leakage and cryptology and the order primitive encryptions and sufficient privacy assurance.

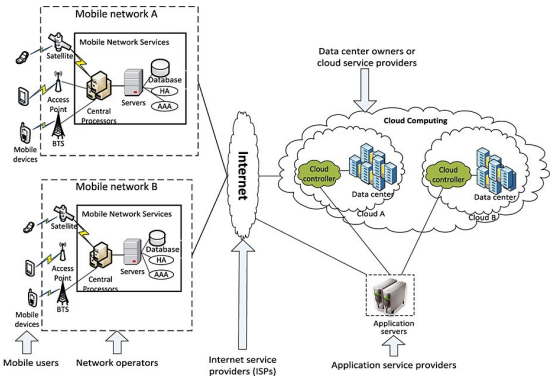

Figure 1: Cloud Computing Terminology

Cloud sensitive data are partitioned with non and distributed to two colluding clouds. In this we introduce two distributed clouds and access pattern will be leaked. The data base system to provide range queries with stronger privacy guaranty of security.

The greedy method or divide and conquer method may be used repeatedly to secure information for single and isolated part of the knowledge and each of the cloud data base service architecture, we propose the series of integration protocols for client to conduct numeric data query includes common query statements, such as greater than, less than or between values linearly selected.

Due to cost-efficiency and less hands-on management, data owners are outsourcing their data to the cloud which can provide access to the data as a service. However, by outsourcing their data to the cloud, the data owners lose control over their data as the cloud provider becomes a third party service provider. At first, encrypting the data by the owner and then exporting it to the cloud seems to be a good approach. However, there is a potential efficiency problem with the outsourced encrypted data when the data owner revokes some of the users' access privileges. An existing solution to this problem is based on symmetric key encryption scheme but it is not secure when a revoked user rejoins the system with different access privileges to the same data record.

The main contribution in this paper can be summarized as follows:

1. Non-colluding cloud architecture and a secure data base service in which data is stored in one cloud, while reveal any private numeric data querying. With privacy preservation and especially information related to any two colluding clouds.

2. Series of intersection to numeric related query processing and cryptographic performance analysis.

III. PROCESS INVESTIGATIONS

Order preserving encryption has numeric related data querying and provide structured database. The data hiding in the Ciphertext and data with security terms and idea of secure data utilization to revel an amount of critical expected private boundary of each user cloud.

Select query:

SELECT *column_name(s)*
FROM *table_name*
WHERE *column_name* BETWEEN *value1*
AND *value2;*

Some of the most fundamental DDL commands discussed during following hours include the following:

CREATE TABLE
ALTER TABLE
DROP TABLE
CREATE INDEX
ALTER INDEX
DROP INDEX
CREATE VIEW
DROP VIEW

Data control commands in SQL allow you to control access to data within the database. These DCL commands are normally used to create objects related to user access and also control the distribution of privileges among users. Some data control commands are as follows:

ALTER PASSWORD
GRANT
REVOKE
CREATE SYNONYM

BETWEEN…AND operators in SQL are used to select in-between values from the given range/ values. It is used in a WHERE clause in SELECT, UPDATE and DELETE statements/queries. Syntax for SQL BETWEEN…AND operators are given as per column names.

With the popularity of cloud computing technology, the clients usually store a mass of data in the cloud server. Because of the untrusted cloud servers, the massive data query raises privacy concerns. To prevent sensitive data on the cloud from hostile attacking, and obtain the query result timely, users usually use the searchable encryption technology to store encrypted data on the cloud. In the prior work, there are many privacy-preserving schemes for cloud computing, but the verification of these schemes cannot be ensured. Due to software errors, communication transmission failure or the dishonest features of the public cloud servers, only part of the data set was searched. So the integrity is also an urgent problem to be solved. In this paper, we propose a verifiable range query processing scheme with the ability to verify the correctness of query result. The key idea of this paper is to add additional information to a complete binary tree, which is used to organize indexing elements. The result returned by the cloud server will be accompanied by validation information so that the user can verify whether the result is complete. Finally, we confirm that the storage overhead of the verifiable scheme is Multi cloud data architecture and protection of data from outsourced data base. The replication of patterns among various store clients and partition of applications on to fragments and data storage in term of data accessed from multi-cloucal data d can get private information in multi cloud. The privacy of the statistical data property and query pattern and data access to the server stability.

[column_name] – Any one of the column names in the table. [Operator] – Any one of the following (>, <, =, >=, <=, NOT, LIKE etc) [Value] – User defined value.

The symbols which are used to perform logical and mathematical operations in SQL are called SQL operators. There are three types of Operators used in SQL. They are, Arithmetic operators, Relational operators and Logical operators

The clouds data exchange works with the data clients and authorized users for privacy concerns two clouds are summed to the non -colluding with each other and they will follow the intersection to preserve privacy of data and queries(privacy). We utilize a partition in to two parts which firstly applicable to logic of query in terms of

view and partitioned into two parts each of which is only known to cloud and two-cloud architecture increase some

Basic Table structures in cloud :

There are some rules about entities: each entity can have up to 252 properties but the size of an entity with all of the properties and values cannot exceed 1 MB. Table storage entities support the following data types: Byte array, Boolean, DateTime, Double, GUID, Int32, Int64 and String (up to 64KB in size). There are an additional three required system properties that must exist on every entity: PartitionKey, RowKey and TimeStamp. The partition key is way to group entities within a table and control the scalability of the table which we will touch on in a bit. The row key is a unique identifier for an entity within a given partition. The combination of partition key and row key is the unique identifier for an entity within a table, comparable to a primary key in a relational database. The Timestamp property represents the last time the entity was modified and is managed by the Storage sub -system. Any change you make to Timestamp will be ignored.

There is no direct table-specific limit to how much data you can store within a table. The size is restricted only by the allowable size of a Windows Azure Storage account which is currently 200 TB, or 100 TB if the storage account was created prior to June 7th, 2012. A storage account can hold any combination of Windows Azure Tables, BLOBs or Queues up to the allowable size of the account. There is a reason that there is a difference in the allowable size depending on when the storage account was created. Starting on that date, accounts are created on the newer infrastructure of Windows Azure Storage which drastically increased the throughput and scalability of the system.

Cloud storage structure:

The GetTableReference method of the CloudTableClientobject. This is just a reference for the client library to use, it hasn't made a call to the REST API yet at all. The next line, table. CreateIfNotExists (), will actually make the first call to the Table service REST API and, if a table named "sportingproducts" doesn't already exist within the storage account it will create it. Note that the call to CreateIfNotExists is idempotent, meaning we can call it multiple times and it will only ensure the table is created. If the table already existed no action would be taken and no data that might already exist within the table would be changed. After the table is created we write to the console the URL of the table. Remember that the table service, like all the Windows Azure Storage services, exists as a REST based API so every table has its own resource location, or URI. Calls against this table, such as inserts, selects, etc., are all sent to this URI.

IV. IMPLEMENTATION

Cloud data privacy assurance and integrations of our stored data perspective with in the interactions of private data process will provide private data delivered beyond the scope of each data partitions in cloud.

The privacy data contents include the description of each stored database option data with other mechanism for data and values of each record. The outsourced data initializing encryption and preservation of redundancy. The statistical properties and order of cloud gradually be exposed as scenarios of order of query requests.

Query processing contains the privacy information as they can reveal the clients purpose and the query pattern out put as per the statistical properties of stored data instances.

Data contents are included as column names and item values for each query pattern the private well preserved even after many query processing. Key generation an encryption for independent private key and ciphertext computed with cryptosystem additive homomorphic operation, clients query request with its own security key and assumption of analyze on privacy data and the query.

Proposed scheme is composed of table creation and query processing with query request, item set, index column and query response. The cloud architecture restricts for query numeric-related data with privacy preserving and client data retrieval. The query predicated and operators like "<",">" and BETWEEN for one column conditions combinations over one or more column in to the table. The operators is reversed and the predicators are combination is another one that combines predicates with Boolean expression with and operators are "V" and or Private cloud and specific cloud processing and index set of each single request and proposed operations like insert delete with index values. The table creation and query processing intersection procedure of query consists of query response and in the form of view of output on terminal. For each column of table the client and use of encrypt each column and numeric data representation.

The encrypted table is uploaded to cloud as the public key and private key with multiple tables in a database and table name encrypted in the same column names are encrypted. Query request of client with selective request modified to an encrypted query as following steps:

Encrypt the column name

Encrypt the range boundary value

Generate the taken

Send the query request

SELECT * FROM table where CONDITION

column computation and comparisons with integer values, rows shuffeling and temporary column creation or saved information. Index send by column values and item number are consistent as request authorization and decrypt the item as index in view or output.

The restrictions on the privacy and protection of cloud data will be a mapping item set.

The operators combination leads the multiple cloud invocation with concatenation and complex query procedures. The idea to realize the type complex query request and simple condition for logic gate and compute the intersection of them.

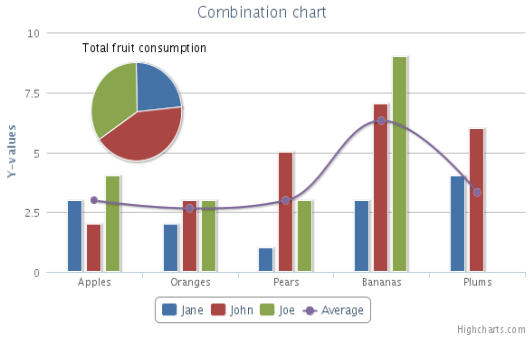

Figure 2: Example of Combination Cart

Security terminology: The privacy preservation in the outsourced query processing against the privacy analysis of security due to repeated queries. Cloud cannot obtain any information from the users query and the stored encryption database as cryptosystem is semantically secure and cloud combination of non-colluding data. An cloud data cannot infer any private information from any two clouds as long as the view is combinational and factor is consistent data.

Ordering the scheme for cloud data return values to database client usage will preserve the boundary values. The data boundary values for any query a SELECT * FROM table WHERE condition is preserved by two non-colluding data clouds as view.

Complex query operations and combination generally exposes the final combination of individually and the appends query. Cloud privacy information foe executing the query predicate and proposed scheme each column is encrypted as un know distinguisher as privacy information.

Two clouds receive and data encrypted data with the different data clouds and relative low. The security for query processing restrict for data aggregation and insertion query with multiple query processing.

As mentioned in the code example above, the best possible query to run is one that includes both partition key and row key as this is the primary key for an entity. In the code sample, we knew the category and the SKU for what we were looking for so the query will be the fastest we can achieve. It might not always be the possible for you to know both keys, so it is best to understand the flow of how you will access this data in order to get the best performance. This category partition approach might be acceptable if, for the vast majority of time, the flow of our data-access starts at the category. For instance, the approach above may make sense if the flow of our solution was to retrieve all of the products within a category to display on a product page and then a user can select an individual product where we already know the category.

All entities with the same partition key within the same table are guaranteed to be accessed via the same partition server. A partition server knows about all the data that exists within one or more partitions.

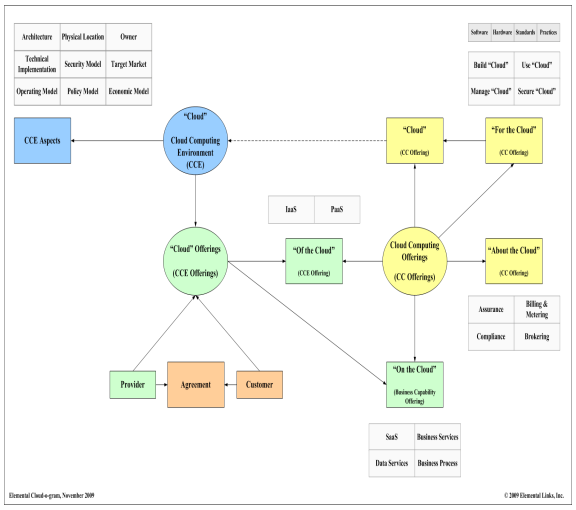

Figure 3: Data Storage in Cloud

The number of partitions a partition server is responsible for depends on how much data is within the partitions and how often they are being accessed. It is very important to choose the correct partitioning scheme. You may need to try multiple options to see what works best for you, or even store the same data in different ways in order to optimize the system for your scenarios. This is not unlike when companies use a data warehouse to store the same data as their transactional systems in a manner which is easier to build analytical queries from. One of the things to keep in mind when using Table Storage is that, in some cases, your query may not complete on a single call to the REST based API. There are a lot of reasons this might occur, such as when the query crosses multiple partition servers or the amount of data coming back is quite large. When this happens, the storage service will return continuation tokens with the query results. These continuation tokens can then be used to continue the query by making additional calls.

V. CONCLUSIONS

In this paper, we presented a cloud with interaction and outsourced database service, which ensures the privacy preservation of data contents, statistical properties and

query pattern. An range queries with static data and addresses the privacy leakage after large number of query processes. Security analysis with out sourced data in terms of view and query output. Future work, we will consider the future enhance the security while ensuring practically and extract proposed scheme for performance increase in terms of output query and view of data in all operations.

REFERENCES:

[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] 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.

[5] J. W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security. CRC press, 2016.

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

[7] 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

[8] 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.

* * * * *