Multi Cloud Particle Analysis With Series Interaction

OUDAYAKUMAR. K , GEETHA. S
DEPARTMENT OF PHYSICS,
SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE,
PUDUCHERRY – 605 107. INDIA
udaya742004@gmail.com, geetha.ssv@gmail.com

ABSTRACT—Industries and individuals outsource database to realize convenient and low-cost applications and services. In order to provide sufficient functionality for SQL queries, many secure database schemes have been proposed. However, such schemes are vulnerable to privacy leakage to cloud server. The main reason is that database is hosted and processed in cloud server, which is beyond the control of data owners. For the numerical range query (“>”, “<”, etc.), those schemes cannot provide sufficient privacy protection against practical challenges, e.g., privacy leakage of statistical properties, access pattern. Furthermore, increased number of queries will inevitably leak more information to the cloud server. In our paper, we propose a multi-cloud architecture for secure database, with a series of intersection protocols that provide privacy preservation to various numeric-related range queries. Security analysis shows that privacy of numerical information is strongly protected against cloud providers in our proposed scheme.

Keywords: cloud server, privacy, SQL Queries,

INTRODUCTION

Introduction to Network Security

Managing security means understanding the risks and deciding how much risk is acceptable. Different levels of security are appropriate for different organizations. No network is 100 percent secure, so don’t aim for that level of protection. If you try to stay up¬-to¬-date on every new threat and every virus, you’ll soon be a quivering ball of anxiety and stress. Look for the major vulnerabilities that you can address with your existing resources.

We all know the numerous advantages of computer networks and the Internet. Connecting your network to the Internet provides access to an enormous amount of information and allows you to share information on an incredible scale. However, the communal nature of the Internet, which creates so many benefits, also offers malicious users easy access to numerous targets. The Internet is only as secure as the networks it connects, so we all have a responsibility to ensure the safety of our networks.

Why Is Network Security Important?

The good neighbor policy. Your mistakes can be someone else’s headaches. If your network is insecure and someone takes control of one of your computers, they can use that machine to launch denial of service attacks on innocent third parties. They can also flood the Web with spam.

Patron privacy. Obviously, patron records are of paramount importance. Trust between the library and its clients can be irreparably harmed if these records are compromised.

Money and time. Tracking down a virus or a worm and eliminating it from your network is frustrating and time-¬consuming. You often have to rebuild your machines from the ground up, re¬installing the operating system and software and restoring data from backup tapes. Lax security can lead to weeks of wasted time spent patching your network and fixing the wreckage.

Subdomain:

The growing industry of cloud has provide a service paradigm of storage/computation outsourcing helps to reduce users' burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual user]. However, due to the privacy concerns that the cloud service provider is assumed semi-trust (honest-but-curious.), it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are needed before outsourcing sensitive data - such as database system - to cloud

The typical scenario for outsourced database is described in Fig. 1 as that in CryptDB. 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, UPDATE, etc.) Due to the assumption that cloud provider is honest-but-curious the cloud might try his/her best to obtain private information for his/her own benefits. Even worse, the cloud could forward such sensitive information to the business competitors for profit, which is an unacceptable operating risk.

The privacy challenge of outsourced database is two-hold.

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 gradually reveal some private information on data statistic properties. Thus, data and queries of the outsourced database should be protected against the cloud service provider.

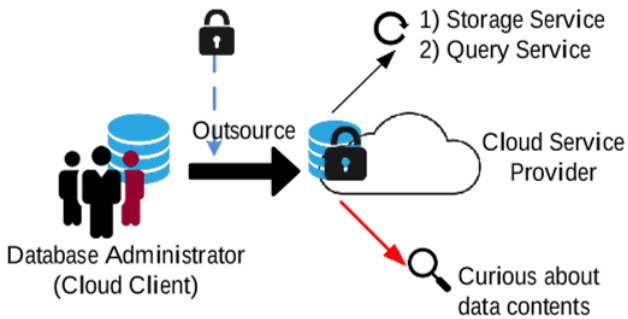

Fig. 1. Outsourced database, service and the privacy risk

The main contribution of our paper can be summarized as follows: 1) We propose a two non-colluding cloud architecture to conduct a secure database service, in which the data is stored in one cloud, while the knowledge of query pattern is well partitioned into two parts, and knowing only one cannot reveal any private information; 2) 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.

SYSTEM ARCHITECTURE

Secure database system includes a database administrator, and two non-colluding clouds. In this model, the database administrator can be implemented on a client's side from the perspective of cloud service. The two clouds (refer to Cloud A and Cloud B), as the server's side, provide the storage and the computation service. Fig. 2 briefly depicts the architecture of our outsourced secure database system in our scheme.

The two clouds work together to respond each query request from the client/authorized users (availability). For privacy concerns, these two clouds are assumed to be non-colluding with each other, and they will follow the intersection protocols to preserve privacy of data and queries (privacy).

In our scheme, the knowledge of stored database and queries is partitioned into two parts, respectively stored in one cloud. The mechanism guarantees that knowing either of these two parts cannot obtain any useful privacy information. As to conduct a secure database, data are encrypted and outsourced to be stored in one cloud (Cloud A), and the private keys are stored in the other one (Cloud B). For each query, the corresponding knowledge includes the data contents and the relative processing logic. We utilize a prototype of knowledge partition, dividing application logic into two parts

POTENTIAL THREATS AND PRIVACY REQUIREMENTS

The privacy issues we consider in our paper mainly include data contents, statistical properties, and query pattern as follows:

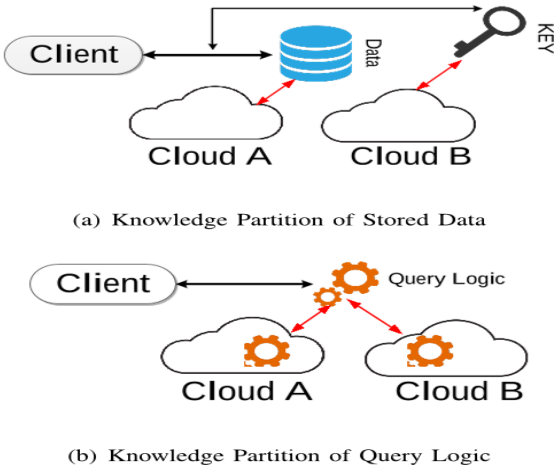

Fig.2. Two-cloud Database Architecture and Knowledge Partition Prototype

Data contents. The data contents includes item values and column names, which are the raw data that should be protected against any potential adversaries.

Statistical properties. It includes the order of data and their probability distributions, some of which include “>”, “<”, “=”, “BETWEEN”, etc.

Query pattern. Each query should be kept private against the honest-but-curious clouds and any unauthorized parties. The secrecy of such pattern should be well preserved even after many query processes.

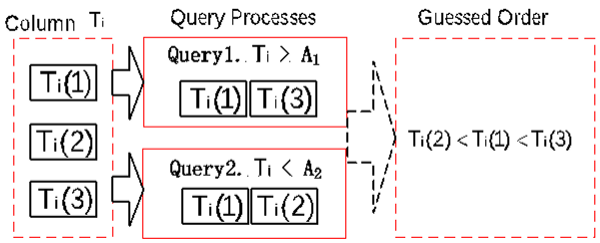

Fig. 3. Repeated Query Discloses Statistical Properties (For example, after two simple queries over one same column, the order relationship of some data in certain column can be determined.)

PAILLIER CRYPTOGRAPHIC ALGORITHM

There are various cryptographic techniques to support numeric-related operations (e.g. addition, multiplication, XOR) upon the encryption field. Paillier cryptosystem [41] is one of the most popular techniques that provides addition homomorphic, which means: if two integers a and b are encrypted with a same key k into two ciphertexts (be denoted as Ek(a) and Ek(b)), there exists an operation (refer to as "⊗"), such that

Ek(a) ⊗Ek(b) = Ek(a + b).

Paillier cryptographic algorithm is composed of the following phases: key generation, encryption and decryption.

Key generation.:Two large and independent prime numbers p and q are randomly selected.Then we compute n = p•qand μ = λ−1 mod n, where λ is the least common multiple of p and q, and commonly λ = lcm(p−1,q−1). The public key (PK) is n, and the private key (SK) is (λ,μ).

Encryption:Let mbe the integer to be encrypted. Firstly, we select a random number , and then the ciphertext of m can be computed as follows:

$$E(m;r) = (n + 1)^m \cdot r^n \bmod n^2.$$

Decryption:Let the ciphertextc = E(m;r). The plaintext m can be recovered as follows:

Numeric-Related Sql Queries

To obtain the desired data, the query contains some statements to describe the requirement, e.g. some numeric-related (">", "<", "=", "BETWEEN", etc.).

OUR PROPOSED TWO-CLOUD SCHEME

Our proposed scheme is composed of Table Creation and Query Protocol. The intersection procedure of Query Protocol consists of four parts: Query Request, Item Send, Index Send, and Query Response

Query Request: When the client wants to retrieve some data from the outsourced database, he/she firstly generates a

SQL query (e.g. "SELECT * FROM table WHERE Ti> a").

Encrypt the column name

Encrypt the range boundary value

Generate the token

Send the query request.

Then the client sends the encrypted query request to Cloud A as follows:

SELECT * FROM table WHERE E(Ti) > A,

Query Response:

1) Operator "<": When the operator in the query is "<", the operation of query request and item send are slightly modified based on the scheme for the operator ">".In the operation of query request, the form of the encrypted query is modified as follows:

SELECT *FROM table WHERE E(Ti) < A.

2) Operator "BETWEEN" and "=": When the operator in the query is "BETWEEN" (SELECT * FROM table WHERE TiBETWEEN a AND b), it is equivalent to an "AND" logic as follows:(Ti> a) ∧ (Ti< b). The operator "=" can be treated as a special case of "BETWEEN": the predicate "Ti= a" can be translated to: "Ti BETWEEN a − 1 AND a + 1", so it is also equivalent to an AND logic:

(Ti> a − 1) ∧ (Ti< a + 1).

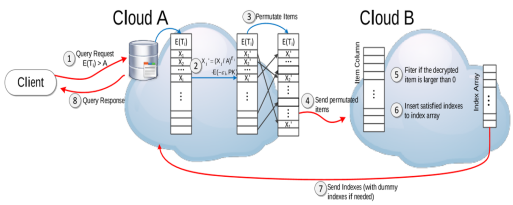

Fig. 4. The Query Protocol. The actions are performed in our designate orderd, which is marked up with circled number, like .

CONCLUSION:

In our paper, we presented a multi-cloud architecture with a series of interaction protocols for outsourced database service, which ensures the privacy preservation of data contents, statistical properties and query pattern. At the same time, with the support of range queries, 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. Security analysis shows that our scheme can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that our proposed scheme is efficient.

REFERENCES:

W. Li, K. Xue, Y. Xue, J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage", IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 5, pp. 1484-1496, May 2016.

K. Xue et al., "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage", IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 953-967, Apr. 2017

X. Yi, R. Paulet, E. Bertino, V. Varadharajan, "Practical approximate k nearest neighbor queries with location and query privacy", IEEE Trans. Knowl. Data Eng., vol. 28, no. 6, pp. 1546-1559, Jun. 2016.

Z. Xia, X. Wang, X. Sun, Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data", IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, Jan. 2016.

Y. Dou et al., " P 2 -SAS: Privacy-preserving centralized dynamic spectrum access system ", IEEE J. Sel. Areas Commune., vol. 35, no. 1, pp. 173-187, Jan. 2016.