Privacy Preserving in Database Service using Non-Colluding Cloud Architecture

Pravin S. Ghatode¹, Trupti P. Tajne², Sweta D. Kuthe³

¹Assistant Professor, Department of Master of Computer Applications, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India
²³PG Scholar, Department of Master of Computer Applications, G. H. Raisoni College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

In the present scenario, businesses and people are outsourcing database to accomplish helpful administrations and minimal effort applications. To provide sufficient functionality for SQL queries, many secure database schemes have been proposed. However, the proposed 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.), the schemes cannot provide sufficient privacy protection against the practical challenges. Portions of the difficulties faced are privacy leakage of statistical attributes and access patterns. Furthermore, increased number of queries will inevitably leak more information to the cloud server. In this paper, we propose a two-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 Computing, Database, Privacy Preserving, Range Query

I. INTRODUCTION

In the present circumstances as it can be seen cloud has taken the control over the IT business with its innumerable advantages. It holds the possibility to change an extensive segment of the IT business, making software considerably more appealing as a service. 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 users. Security is the chief concern of the cloud computing. Cloud clients confront security dangers both from outside and inside the cloud. However, due to the privacy concerns that the cloud service provider is assumed semi-trust, it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are needed before outsourcing sensitive data to cloud.

The privacy challenge of outsourced database is two-fold.

1) Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers.

2) The data and queries of the outsourced database should be protected against the cloud service provider.
This divide-and-conquer mechanism can know any private information from one single isolated part of the knowledge. In this paper, a secure two-cloud database service architecture is introduced, where the two clouds are non-colluding and both of them knows only part of knowledge. Based on this architecture, a series of interaction protocols for a client to conduct numeric-related query over encrypted data from remote cloud servers is proposed. The numeric-related query includes common query statements, such as greater than, less than, and between.

II. PROBLEM STATEMENT

A. Existing System

In existing system, the perspective for privacy assurance and the data not only include permanently stored information that is the database, but also each temporary query request.

Additionally and importantly, as the assumption in some existing works, we assume that the two clouds A and B are non-colluding: Cloud A follows the protocol to add required obfuscation to protect privacy against cloud B, so that cloud B cannot obtain additional private information in the interactions with Cloud A. No private information is delivered beyond the scopes of protocols.

Disadvantages

a. While providing efficient cross server storage verification and data availability insurance, the entire focus is on static or archival data.
b. The capability of handling dynamic data remains unclear, which inevitably limits full applicability in Server storage scenarios.

B. Proposed System

In the proposed system the two-cloud scheme, the detailed interaction protocols will be provided to realize range query with privacy preservation on outsourced encrypted database. The proposed mechanism can preserve the privacy of data and query requests against each of the two clouds.

Specifically, Cloud A only knows the query request type and the final indexes, but due to dummy items appending, Cloud A cannot accurately understand the finally satisfied index set for each single request.

For Cloud B, it knows the satisfied indexes of each single request, but after the proposed operations, it does not know the relationship of the corresponding items. Moreover, Cloud B can hardly distinguish whether two received columns are generated from one or more columns in the original database.

III. LITERATURE SURVEY


This paper deals with Client Module, Storage Service Module, Query Service Module and Cloud Service Provider Module. It also ensures the privacy preservation of data contents, statistical properties and query pattern with the support of range queries.


The Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE) is an data access control for large-scale collaborative cloud storage service is addressed in this paper.

This paper shows how exactly the privacy is preserved and availability of information in cloud computing. The distribution of information among the multiple available Cloud service providers is done in order to preserve the privacy.

[4] RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage. K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong.

This paper is based on how to achieve a robust and efficient access control for public cloud storage. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is the methodology used in this paper.


In this paper, the proposed CryptDB, a framework to defend the private information in databases. CryptDB fundamentally includes utilizing the range queries productively finished the encrypted information utilizing a novel SQL-aware encryption system.

IV. METHODS AND MATERIAL

This section describes the potential threats and the privacy requirements when the database is outsourced to public cloud. The stored data contents and the query processes. Although there are many data encryption schemes, some fail to provide sufficient privacy preservation after statistical analysis. Repeated and large-amount query processes not only leak the access patterns, but also disclose the stored encrypted data progressively.

The privacy issues we consider in this paper are as follows:

1. Potential Threats and Privacy Requirements.
2. Data contents Module.
3. Query pattern Module.
4. Privacy of Item Values Modules.

1. Potential Threats and Privacy Requirements

This section describes the potential threats and the privacy requirements when the database is outsourced to public cloud. The stored data contents and the query processes. Although there are many data encryption schemes, some fail to provide sufficient privacy preservation after statistical analysis. Repeated and large-amount query processes not only leak the access patterns, but also disclose the stored encrypted data progressively.

2. Data contents Module

Besides the static properties can disclose the private information of data contents, such properties themselves are already sensitive and private for the client. Order Preserving Encryption (OPE), which is widely used in constructing the secure database, with support of range queries, directly exposes the statistical information in the encryption field. Furthermore, the leakage of statistic properties is part of the nature of outsourced cloud database service: the cloud can learn the statistical properties (like order) by repeated query requests. As an example, Fig. 3 describes such an attack: After two simple queries over one same column, the order relationship of some data in certain column can be determined. There are also some other direct and indirect scenarios to leak statistical properties. In this way, even though the order property is not exposed to the semi-trusted
cloud at the beginning, the cloud can gradually find out the order information after many query requests.

3. Query Pattern Module

The query pattern also contains privacy information, as they can reveal the client’s purpose of the query. Even worse, such pattern can leak some statistical properties, as discussed above. Based on the above discussion, we assert that an outsourced secure database providing numeric-related queries should prevent the following private information from being obtained by the honest-but-curious clouds.

4. Privacy of Item Values Modules

An ideal scheme is required to make nothing of the statistical properties be leaked to the curious clouds. However, the privacy leakage of statistical properties in a practical outsourced database system is inevitable, as returning subset of data rather than universe requires knowledge for filtering. For instance, if the client wants to retrieve a from the outsourced database, a cloud server without any knowledge of the order can only return all items of the database to the client, which is not usable.

V. CONCLUSION

In the presented two-cloud architecture a series of interaction protocols for outsourced database service is provided, 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 it can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that the proposed scheme is efficient. In the future work, it is required to enhance the security while ensuring practicality, and to extend the proposed scheme to support more operations, such as “SUM/AVG”.

VI. REFERENCES


Cite this article as:

Journal URL : http://ijsrst.com/IJSRST196291