Secure KNN query on Encrypted Cloud Data with Multiple Keys

Abstract:

Cloud computing has become an increasingly popular service for its flexibility and scalability, which motivates many organizations, institutions and companies to prefer to outsource data services to cloud platform. At the same time, much attention has been paid to cope with the special security and privacy problems in outsourced cloud. On one hand, to protect the data confidentiality, the data owner (DO) encrypt the sensitive information of his outsourced data, such as income level, health records, personal photos before the dataset is uploaded to the cloud . On the other hand, data owner may plan to rely on cloud platform for querying of the datasets stored in cloud, not just for storage and management.

Existing system:

Existing works primarily concern the following aspects: traditional SQL query ,textual query range search top-*k* query and *k*-NN query .In this section, we mainly review some recent achievements on secure *k*-NN query. In previous works, some schemes have been proposed to solve secure *k*-NN computation on encrypted cloud data which can be mainly classified into two categories based on whether the key of data owner is sharing with others or not: key-sharing scheme and key-confidentiality scheme.

Disadvantages:

1. Security levels has to be improved
2. Key Maintenance and sharing time consuming and for encryption and decryption cost will be increased.

Proposed system:

we propose a novel scheme for secure *k*-NN query on encrypted cloud data with multiple keys, in which they DO and each QU all hold their own different keys, and do not share them with each other; meanwhile, the DO encrypts and decrypts outsourced data using the key of his own.

Our scheme is constructed by a distributed two trapdoors public-key cryptosystem (DT-PKC) and a set of protocols of secure two-party computation, which not only preserves the data confidentiality and query privacy but also supports the offline data owner. Our extensive theoretical and experimental evaluations demonstrate the effectiveness of our scheme in terms of security and performance.

Advantages:

1. Application performance and security has been improved.
2. Key maintenance has become less effort.

SYSTEM REQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –III
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X
- Front End : HTML, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.
- Database : MySQL 5.0
- Database Connectivity : JDBC