Publicly verifiable Boolean query over outsourced Encrypted Data

Abstract:

The great flexibility and economic savings of cloud computing motivate companies and individuals to outsource their data to cloud servers. By outsourcing a dataset to the cloud, the data owner or other valid data users can then issue the cloud informational queries that are answered according to the dataset.

Existing system:

In the existing system Cash et al. Presented a SSE scheme supporting conjunction queries over static data. Based on Cash et al. Work, Jarecki et al. proposed a scheme that allowed data owners to authorize third parties and to execute private information retrieval on the outsourced database. Faber et al. extended the search capabilities of the system from by supporting range queries, substring queries, wildcard queries, and so on. Moreover, they also extended their techniques to the more involved multi-client SSE scenarios studied in. However, they did not consider the update process and the integrity query verification comparing with our scheme.

Disadvantages:

1. Existing systems do not consider the verification problem of the search result.
2. Security levels has to be improved

Proposed system:

We propose a publicly verifiable dynamic searchable symmetric encryption scheme based on the accumulation tree. We first construct an accumulation tree based on encrypted data and then outsource both of them to the cloud. Next, during the search operation, the cloud generates the corresponding proof according to the query result by mapping Boolean query operations to set operations, while keeping privacy-preservation and achieving the verification requirements: freshness, authenticity, and completeness. Finally, we extend our scheme by dividing the accumulation tree into different small accumulation trees to make our scheme scalable.

Advantages:

1. Our scheme can keep the privacy-preserving of private information retrieval.

2. The performance demonstrates our scheme is scalable.

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