Privacy-Preserving Outsourced Media Search

ABSTRACT

This work proposes a privacy-protection framework for an important application called outsourced media search. This scenario involves a data owner, a client, and an untrusted server, where the owner outsources a search service to the server. Due to lack of trust, the privacy of the client and the owner should be protected. The framework relies on multimedia hashing and symmetric encryption. It requires involved parties to participate in a privacy-enhancing protocol. Additional processing steps are carried out by the owner and the client: (i) before outsourcing low-level media features to the server, the owner has to one-way hash them, and partially encrypt each hash-value; (ii) the client completes the similarity search by re-ranking the most similar candidates received from the server. One-way hashing and encryption add ambiguity to data and make it difficult for the server to infer contents from database items and queries, so the privacy of both the owner and the client is enforced. The proposed framework realizes trade-offs among the strength of privacy enforcement, the quality of search, and complexity, because the information loss can be tuned during hashing and encryption. Extensive experiments demonstrate the effectiveness and the flexibility of the framework.

EXISTING SYSTEM

As a consequence, the management of multimedia data, e.g., storage and search,is typically outsourced to third parties. Outsourcing offers constant availability, fault tolerance, and gigantic processing power to both data owners and users. In this work, the outsourced scenario is tackled by a novel privacy-preserving framework based on robust hashing and partial encryption. In a nutshell, database items and queries are represented by content-based hash values; the hash value of each database item is divided into two parts, one of which is encrypted. The unencrypted part is used by the server for approximate indexing and search.

DISADVANTAGES

- Data owners might involuntarily confide sensitive information to third party server, especially when it is not trusted.
- Three-party scenario is more difficult than the conventional two-party scenario. So far most existing solutions only address the latter, and cannot be easily extended.
- One-way hashing and encryption add ambiguity to data and make it difficult for the server to infer contents from database items and queries.

PROPOSED SYSTEM

In this work, the outsourced scenario is tackled by a novel privacy-preserving framework based on robust hashing and partial encryption. In a nutshell, database items and queries are represented by content-based hash values; the hash value of each database item is divided into two parts, one of which is encrypted. The unencrypted part is used by the server for approximate indexing and search. The encrypted part is used by the client for refined candidate ranking. Figure 1 shows a flow chart of the proposal. Robust hashing is the key element for protecting the privacy of the owner and the client. Conventional low-level features sometimes enable the inferring of content , while the one wayness of hashing makes it hard to recover original content from hash values. This concept has been successfully used in a two-party protocol . In order to cope with the new scenario, another element is incorporated – partial encryption prevents the server from precisely “linking” queries and database items. At the server, a high level of ambiguity is maintained because similarity search can only be performed using unencrypted hash parts. That ambiguity must be such that similarity search remains possible and meaningful.

ADVANTAGES

- If search performance can be slightly sacrificed, the cost for privacy can be further reduced.
- Reducing the number of candidates by selecting the top matches at the server. Results show that good performance can be maintained with a small proportion of candidates.

- By tuning the number of returned candidates, flexible trade-offs can be achieved between privacy and communication cost.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net
- Tool : Visual Studio 2010
- Database : SQL SERVER 2008