IEEE 2019 PRIVACY PRESERVING WEIGHTED SIMILARITY SEARCH SCHEME FOR ENCRYPTED DATA

Abstract:

Cloud computing has become increasingly popular among individuals and enterprises because of the benefits it provides by outsourcing their data to cloud servers. However, the security of the outsourced data has become a major concern. For privacy concerns, searchable encryption, which supports searching over encrypted data, has been proposed and developed rapidly in secure Boolean search and similarity search. However, different users may have different requirements on their queries, which mean different weighted searches. This problem can be solved perfectly in the plaintext domain, but hard to be addressed over encrypted data. In this study, the authors use locality-sensitive hashing (LSH) and searchable symmetric encryption (SSE) to deal with a privacy preserving weighted similarity search. In the authors' scheme, data users can generate a search request and set the weight for each attribute according to their requirements. They treat the LSH values as keywords and mix them into the framework of SSE. They use homomorphic encryption to securely address the weight problem and return the top-k data without revealing any weight information of data users. They formally analysed the security strength of their scheme. Extensive experiments on actual datasets showed that their scheme is extremely effective and efficient.