

**VPSearch: Achieving Verifiability for Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data**

**Abstract:**

Although cloud computing offers elastic computation and storage resources, it poses challenges on verifiability of computations and data privacy. In this work we investigate verifiability for privacy-preserving multi-keyword search over outsourced documents. As the cloud server may return incorrect results due to system faults or incentive to reduce computation cost, it is critical to offer verifiability of search results and privacy protection for outsourced data at the same time. To fulfill these requirements, we design a Verifiable Privacy-preserving keyword Search scheme, called VPSearch, by integrating an adapted homomorphic MAC technique with a privacy-preserving multi-keyword search scheme. The proposed scheme enables the client to verify search results efficiently without storing a local copy of the outsourced data. We also propose a random challenge technique with ordering for verifying top-k search results, which can detect incorrect top-k results with probability close to 1. We provide detailed analysis on security, verifiability, privacy, and efficiency of the proposed scheme. Finally, we implement VPSearch using Matlab and evaluate its performance over three UCI bag-of-words data sets. Experiment results show that authentication tag generation incurs about 3% overhead only and a search query over 300,000 documents takes about 0.98 seconds on a laptop. To verify 300,000 similarity scores for one query, VPSearch costs only 0.29 seconds.