

**Keyword Search with Access Control over Encrypted Cloud Data**

**Abstract:**

In this paper, we study the problem of keyword search with access control (KSAC) over encrypted data in cloud computing. We first propose a scalable framework where user can use his attribute values and a search query to locally derive a search capability, and a file can be retrieved only when its keywords match the query and the user's attribute values can pass the policy check. Using this framework, we propose a novel scheme called KSAC, which enables keyword search with access control over encrypted data. KSAC utilizes a recent cryptographic primitive called hierarchical predicate encryption to enforce fine-grained access control and perform multi-field query search. Meanwhile, it also supports the search capability deviation, and achieves efficient access policy update as well as keyword update without compromising data privacy. To enhance the privacy, KSAC also plants noises in the query to hide users' access privileges. Intensive evaluations on real-world dataset are conducted to validate the applicability of the proposed scheme and demonstrate its protection for user's access privilege.