Zhao, Fangming; Nishide, Takashi; Sakurai, Kouichi
Multi-user keyword search scheme for secure data sharing with fine-grained access control.
(English) [Zbl 1365.94473]
Kim, Howon (ed.), Information security and cryptology – ICISC 2011. 14th international conference,

Summary: We consider the problem of searchable encryption scheme for the cryptographic cloud storage
in such a way that it can be efficiently and privately executed under the multi-user setting. Searchable
encryption schemes allow users to perform keyword searches on encrypted files to retrieve their interested
data without decryption. All existing such schemes only consider the straightforward search approach
where for searching one encrypted keyword, the cloud server must look round all encrypted files on the
storage to compare that encrypted keyword to each keyword index. Since the file number can be very
huge and the user may be unable to decrypt all files, that approach is not efficient and secure enough.
In this paper, we first propose a keyword search scheme for the cryptographic cloud storage based on
attribute-based cryptosystems. Our scheme presents a new keyword search notion: fine-grained access
control aware keyword search. By narrowing the search scope to the user’s decryptable files’ group before
executing the keyword search, our approach can both decrease information leakage from the query process
and be more efficient than other existing schemes.

For the entire collection see [Zbl 1248.68040].

MSC:
94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Keywords:
keyword search; multi-user; fine-grained and flexible access control; data sharing

Full Text: DOI