IEEE 2019 PRIVACY PRESERVING SEARCHABLE ENCRYPTION WITH FINE-GRAINED ACCESS CONTROL

Abstract:

Searchable encryption facilitates cloud server to search over encrypted data without decrypting the data. Single keyword based searchable encryption enables a user to access only a subset of documents, which contains the keyword of the user's interest. In this paper we present a single keyword based searchable encryption scheme for the applications where multiple data owners upload their data and multiple users access the data. We use attribute based encryption scheme that allows user to access the selective subset of data from cloud without revealing his/her access rights to the cloud server. The proposed scheme is proven adaptively secure against chosen-keyword attack in the random oracle model. We have implemented the scheme on Google cloud instance and the performance of the scheme found feasible in real-world applications.

SHIELD TECHNOLOGIES,
2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64
Mail us: shieldtechnoblr@gmail.com / manager@shieldtechno.com
Contact: 9972364704 / 8073744810