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 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 then multiple users can access the data. The scheme uses attribute based encryption that allows user to access the selective subset of data from cloud without revealing his/her access rights to the cloud server. The 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 practical in real-world applications.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium i3 Processor.
- Hard Disk : 500 GB.
- Monitor : 15’’ LED
- Input Devices : Keyboard, Mouse
- Ram : 4 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 10.
- Coding Language : Java
- Web Framework : Flask

REFERENCE:

P. Chaudhari and M. L. Das, "Privacy Preserving Searchable Encryption with Fine-Grained Access Control," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 753-762, 1 April-June 2021, doi: 10.1109/TCC.2019.2892116.