Searchable Symmetric Encryption (SSE)

Dr. Geong Sen Poh

Cryptography Laboratory, MIMOS

Email: gspoh@mimos.my

Abstract:

Searchable symmetric encryption schemes enable a party to store his data in a storage provided by a storage provider in an encrypted form, while at the same time allowing the storage provider to perform queries on the data in a privacy-preserving manner. This issue has become the focus of active research recently due to the advancement of cloud storage solutions. Therefore, the aim of this work is to examine the many proposals of searchable symmetric encryption and the issues that are to be addressed. Firstly the different approaches taken and their properties are discussed and categorized. Secondly the security models are studied together with a few example schemes. The efficiency and practicality of the many proposals are analyzed, and finally some open problems are discussed.

Keywords: searchable symmetric encryption, cloud storage.