

Searchable Encryption with Hybrid Index

Abstract

This invention relates an indexing method for a secret encryption scheme having a first database and a second database. The first database comprises a list of keyword-data pairs and the second database comprises encrypted data-label pairs where the labels computed by keywords are associated to the encrypted data. The method comprises receiving a document containing a keyword; determining a type of keyword in the document; in response to the keyword being a search token, searching the keywords in the first database that matches the keyword in the document and retrieving data paired with a keyword in the first database that matches the keyword in the document; recording a new entry indicator data associated to the keyword in the first database that matches the keyword in the document as A; searching the labels in the second database, for new added entry indicator associated to the labels greater than A, with the keyword in the document and retrieving encrypted data associated to label in the second database that matches the keyword in the document; returning a search result containing the data and encrypted data retrieved from the first and second databases; and updating the first and the second databases.

Figure 1 to accompany the abstract