

Accepted Manuscript

Expressive Query over Outsourced Encrypted Data

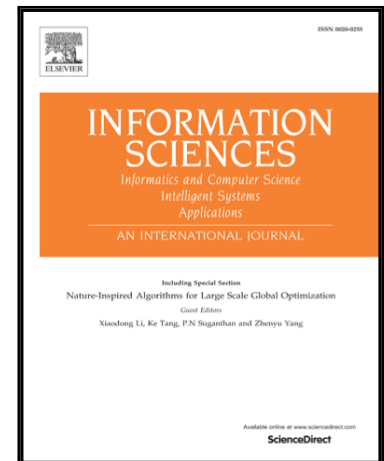
Yang Yang, Ximeng Liu, Robert Deng

PII: S0020-0255(18)30098-7
DOI: [10.1016/j.ins.2018.02.017](https://doi.org/10.1016/j.ins.2018.02.017)
Reference: INS 13422

To appear in: *Information Sciences*

Received date: 18 July 2017
Revised date: 25 November 2017
Accepted date: 8 February 2018

Please cite this article as: Yang Yang, Ximeng Liu, Robert Deng, Expressive Query over Outsourced Encrypted Data, *Information Sciences* (2018), doi: [10.1016/j.ins.2018.02.017](https://doi.org/10.1016/j.ins.2018.02.017)



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Highlights

- Expressive search query patterns: The system supports versatile search query patterns, such as the single/conjunctive keyword queries which are the most common search queries in data retrieval, the equality and multi-dimensional range queries which enable flexible numeric type data search, the subset queries which determine whether an encrypted element belongs to a specific set, and the boolean queries which support keyword search in which the keywords are connected by boolean operators “AND-OR-NOT”.
- Ranked search: In our system, a data owner defines a weightage for each keyword according to the keyword importance during data encryption. To conduct keyword search over encrypted documents, a data user sets different preference scores for the queried keywords and uses a trapdoor generation algorithm to generate a query trapdoor. Upon receiving the query trapdoor, the cloud server computes the relevance scores of the search results in an encrypted form and returns the top-k results to the data user.
- Flexible user authorization and revocation: The system allows a data owner to delegate his search privileges to data users while without revealing his secret key. The privilege delegation is constrained by a predefined time period and it expires automatically beyond the time period. The system enables the data owner to revoke the delegation within the validity time period in case a data user is found behaving maliciously.
- Multi-domain data retrieval: The system enables a data user to independently generate a query trapdoor. Another advantage of the system is that, upon authorization, a data user can conduct multi-domain search, i.e., use a single query trapdoor to search over encrypted documents from multiple data owners. On the contrary, in existing schemes in the literature, a data user has to generate n different trapdoors to search over encrypted documents from n data owners.

Download English Version:

<https://daneshyari.com/en/article/6856537>

Download Persian Version:

<https://daneshyari.com/article/6856537>

[Daneshyari.com](https://daneshyari.com)