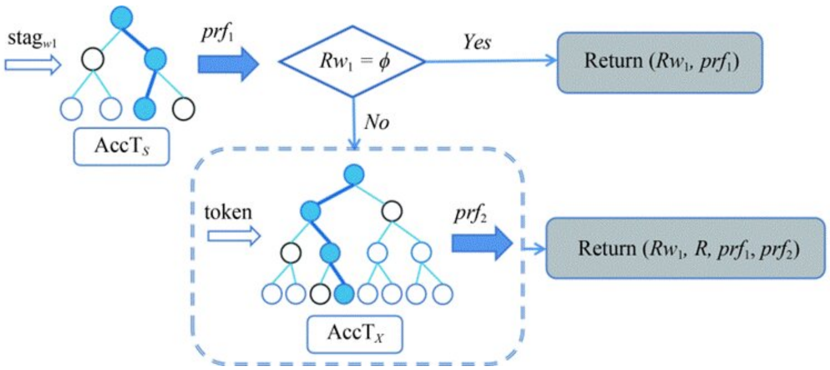
TechXplore

Verifiable searchable symmetric encryption for conjunctive keyword queries in cloud storage

May 26 2022



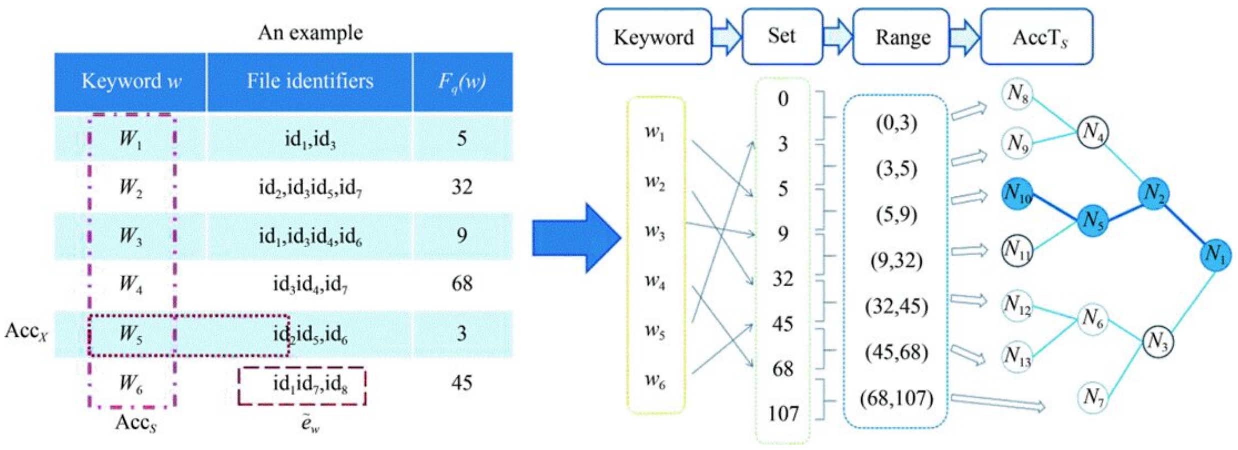
Overview of the proof generation procedure. Credit: Higher Education Press

Searchable symmetric encryption (SSE) has been introduced to enable secure outsourcing of encrypted databases to cloud storage, while maintaining searchable features. Of the various SSE schemes, most assume the server is honest but curious, while the server may be trustless in the real world.

Considering a malicious server not honestly performing the queries, verifiable SSE (VSSE) schemes are constructed to ensure the verifiability of the search results. However, existing VSSE constructions only focus on single-keyword search or incur heavy computational cost during verification.

To address this challenge, a research team led by Joseph K. Liu published their new research on 02 April 2022 in *Frontiers of Computer Science*.

The team proposes a new VSSE construction supporting conjunctive keyword queries, which can be treated as an improvement of a recent VSSE solution. The proposed VSSE scheme is based on a privacy-preserving hash-based accumulator, leveraging a well-established cryptographic primitive, Symmetric Hidden Vector Encryption (SHVE). The VSSE scheme enables both correctness and completeness verifiability for the result without pairing operations, thus greatly reducing the computational cost in the verification process.



An example

Keyword w	File identifiers	$F_q(w)$
W_1	id_1, id_3	5
W_2	$id_2, id_3 id_5, id_7$	32
W_3	$id_1, id_3 id_4, id_6$	9
W_4	$id_3 id_4, id_7$	68
W_5	$id_2 id_5, id_6$	3
W_6	$id_1 id_7, id_8$	45

The process from the keyword to an accumulator. Credit: Higher Education Press

More information: Qingqing Gan et al, Verifiable searchable symmetric encryption for conjunctive keyword queries in cloud storage, *Frontiers of Computer Science* (2022). DOI: 10.1007/s11704-021-0601-8

Provided by Higher Education Press

Citation: Verifiable searchable symmetric encryption for conjunctive keyword queries in cloud storage (2022, May 26) retrieved 25 April 2024 from https://techxplore.com/news/2022-05-searchable-symmetric-encryption-conjunctive-keyword.html