Simple index based symmetric searchable encryption with result verifiability

Dhruti SHARMA, Devesh JINWALA

Frontiers of Computer Science, DOI: 10.1007/s11704-019-9125-x

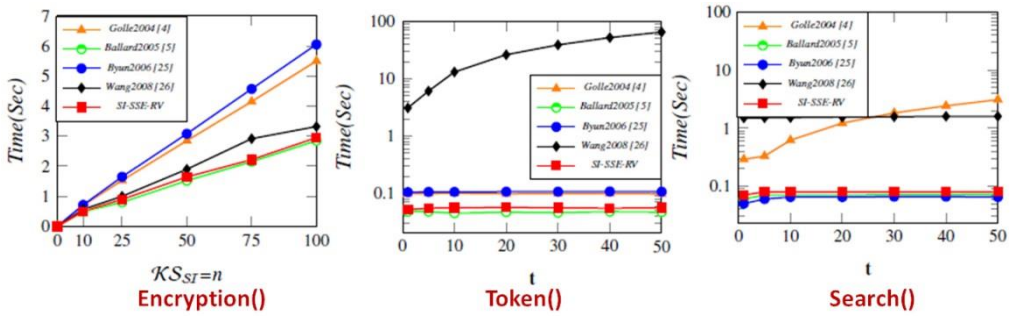
Problems & Ideas

- **Problems:**
  - The existing verification enabled Inverted Index (II) based Symmetric Searchable Encryption (SSE) schemes have following limitations
    - Support to static data collection or put additional computational overhead linear to the number of documents at server for dynamic data collection
    - Work for the prefixed set of keywords
    - Offer inefficient multi-keyword search
  - The existing Simple Index (SI) based SSE schemes do not offer result verification.
- **Idea:**
  - Define a Simple Index based SSE scheme that offers
    - Result verification - through server generated proof component
    - Multi-keyword Search - through token for conjunctive query
    - Support to dynamic data update - without any computational burden on server
- **Proposed Scheme:**

  Simple Index based Symmetric Searchable Encryption with Result Verifiability (SI-SSE-RV)

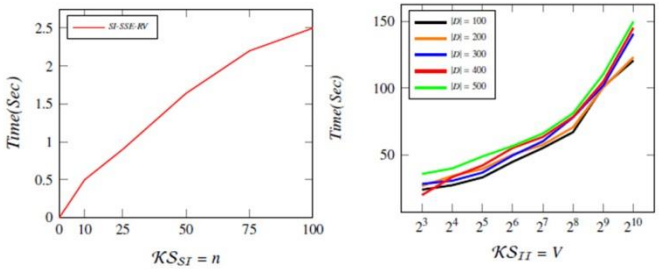
Main Contributions

Simulation Results for SI-SSE-RV as compared to SI-based schemes



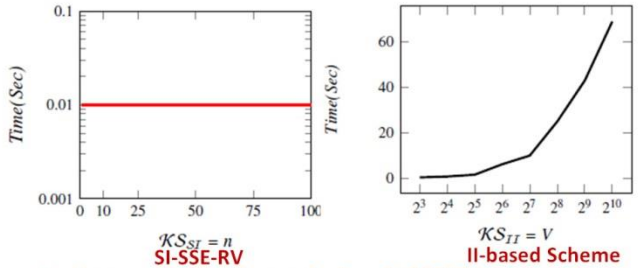
The proposed SI-SSE-RV with almost same storage-computational overhead as that in [5], offers an additional utility of search result verification besides conjunctive keyword search provided by [5].

Computational overhead for Index Generation



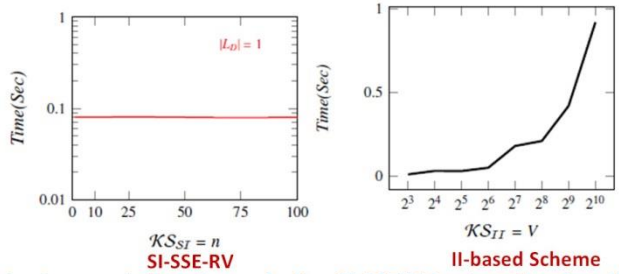
Practically, Number of keywords in II (V) >> Number of keywords in SI (n). Thus, the proposed Encryption() Algorithm is much more efficient than IndexGen() algorithm of II-based scheme.

Computational Overhead for Proof Component Computation



With constant computational complexity, SI-SSE-RV puts optimal overhead on server as compared to overhead linear to V incurred by II-based scheme.

Computational Overhead for Result Verification



With constant computational complexity, SI-SSE-RV puts optimal verification overhead on Client as compared to overhead linear to V incurred by II-based scheme.