University of Trento

Advanced Programming of Cryptographic Methods

Outsourced Sensitive Database

Graduate Student
Filippo De Grandi

Date: 19/11/2025

Contents

Description

In the era of cloud computing and big data, the need for secure and efficient methods to search over cloud-hosted confidential data has become increasingly critical. The scenario involves a client-server model, where the client is a smart device (e.g., a smartphone or IoT device) with limited computational and storage resources, and the server is a cloud service provider. The client has sensitive data and wants to outsource it to the server. The client needs to perform search operations over this data without revealing the content of the queries or the data itself. In particular, the client must be able to:

- Add new documents to the database on the server;
- Search for keywords within the database and retrieve the relevant documents;
- Maintain privacy by ensuring that the server cannot infer information about the client's data or queries, even when updates (additions or deletions) are performed.

The server, while providing storage and computational resources, is considered semi-trusted. This means that the server is honest but curious, it will follow the protocol correctly but may attempt to learn as much as possible about the client's data and queries. For instance, the server should not link new updates to previous search queries or infer information about deleted documents.

Requirements

Security Requirements

In this section, we outline the security requirements for the outsourced sensitive database system, focusing on confidentiality, privacy, integrity, and threat mitigation.

Confidentialiy

Data Confidentiality — SR 1

All outsourced documents must remain encrypted at all times; the server must not be able to read document contents.

Query Confidentiality — SR 2

The content of search queries (keywords) must remain hidden from the server.

Index Confidentiality — SR 3

Metadata such as keyword-document relations must also be encrypted or obfuscated.

Forward & Backward Privacy

Forward Privacy — SR 4

Newly added documents must not be linkable to past queries—i.e., after a keyword has been searched, the server cannot infer that a newly added document contains that keyword.

Backward Privacy — SR 5

After deleting a document, the server should not be able to return it in future searches nor infer previously associated keywords.

Leakage Minimization

Search Pattern Privacy — SR 6

The server should not be able to determine whether two search tokens correspond to the same keyword.

Access Pattern Privacy — SR 7

The server should not learn which documents match a query (requires ORAM or PIR if desired).

Update Pattern Privacy — SR 8

The server must not be able to link updates (new documents, deletions) to past queries.

Integrity & Freshness

Integrity of Search Results — SR 9

The server must not omit or alter returned encrypted documents; the client must be able to verify correctness (e.g., via MACs or authenticated data structures).

Index Integrity — SR 10

Any tampering with the encrypted index must be detectable.

Freshness Guarantees — SR 11

Returned results must reflect the most recent updates (no replay of outdated search results).

Authentication & Access Control

Authorized Client Access — SR 12

Only the legitimate client may upload documents, perform searches, or request updates.

Secure Client–Server Communication — SR 13

All communication must use secure channels (TLS), despite encryption at rest.

Threat Mitigation

Resistance to Traffic Analysis — SR 14

The system should minimize information leakage through message size, timing, or frequency.

Compromise Containment — SR 15

If the client device is compromised, the attacker should not be able to derive the plaintext or reveal past queries (e.g., key rotation or forward-secure key updates).

Functional Requirements

In this section, we outline the functional requirements for the outsourced sensitive database system.

Document Upload FR 1

The client must be able to upload encrypted documents to the server

Document Update FR 2

The client must be able to add new encrypted documents without reuploading or re-encrypting the entire dataset.

Document Deletion FR 3

The client must be able to delete previously outsourced documents in a way that prevents future retrieval.

Search Capability FR 4

The client must be able to issue search queries (via encrypted search tokens) for specific keywords.

Result Retrieval FR 5

The system must return a set of encrypted documents relevant to the search query.

Efficient Indexing FR 6

The server must maintain an encrypted index that supports efficient search and update operations.

Lightweight Client Operations FR 7

Most computation (e.g., index management, filtering) should occur server-side because the client device is resource constrained.

Non-Functional Requirements