University of Trento

Advanced Programming of Cryptographic Methods

Outsourced Sensitive Database

Filippo De Grandi

Date: 27/11/2025

Contents

Description

In this scenario, a client with limited computational resources (such as a smartphone or IoT device) wishes to outsource sensitive documents to a cloud server. The client must later search over these outsourced documents without revealing the content of either the data or the search queries.

The server is honest-but-curious: it follows protocol but attempts to infer as much information as possible. The system must support secure document uploads, updates, deletions, and keyword searches while preventing the server from learning search patterns, access patterns, or update patterns.

Strong privacy guarantees (including forward and backward privacy) and efficient handling of encrypted data are required despite the client's limited capabilities.

Requirements

Functional Requirements

> SR 1 **Add documents** : The user must be able to add documents to the database

> SR 2 **Delete documents** : The user must be able to delete documents from the database

> SR 3 **Searching** : The database must return the documents related to the key words searched by the client.

> SR 4 **User search** : The user must be able to search using key words.

> SR 5 **Document keyword association** : The documents must be associated with specific keywords.

Security Requirements

> FR 1 **Non-revealing database** : The database must not leak sensitive information to the server or third-parties.

> FR 2 **User scope** : The user must be able to obtain only their personal documents.

> FR 3 **Data integrity** : The integrity of the information must be kept both during communication and inside the database.

> FR 4 **Authentication** : The users must be authenticated before communication and for sensitive operations.

> FR 5 **Secure queries** : The queries must reveal as little information as possible

Non-Functional Requirements

> NFR 1 **Compliance** : The system must comply with local regulations for sensitive data.

Technical Details

Architecture

Security Considerations