**Verifiable Attribute-Based Search over Shared Cloud Data**

**OBJECTIVES**

1. To design novel security primitives for supporting verifiable attribute-based access control over shared cloud data.
2. To protect data content and access policy of outsourced databases in a zero-knowledge manner.
3. To propose query authentication algorithms and optimization techniques for various query types.
4. To develop a demonstration system to show the robustness and efficiency of our proposed techniques.

**HIGHLIGHTS**

**Problem Statement**

- Data owner outsources her database to a cloud service provider.
- Users need to ensure the integrity of query results from the following two perspectives:
  - **Soundness:** No records in results are tampered with and are truly the results with respect to their own roles.
  - **Completeness:** All records not in results are either non-results or inaccessible to users.
- Data are cryptographically enforced with fine-grained access control.
- Data content and access policy are protected in a zero-knowledge manner.

**System Architecture**

- Verifiable attribute-based search services over shared cloud data.
- **Client side:** attribute-based search and result verification.
- **Server side:** query processing and VO construction.

**SELECTED PUBLICATIONS**