香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

Verifiable Attribute-Based Search over Shared Cloud Data

PI : Prof. XU Jianliang

PC : Prof. JIA Xiaohua (CityU)

Funding Scheme: **Collaborative Research Fund**

Project Ref. No.: **C1008-16G**

Amount Awarded (to HKBU): **HK$ 1,020,000**

Project Period: **Jun 2017 - May 2020**

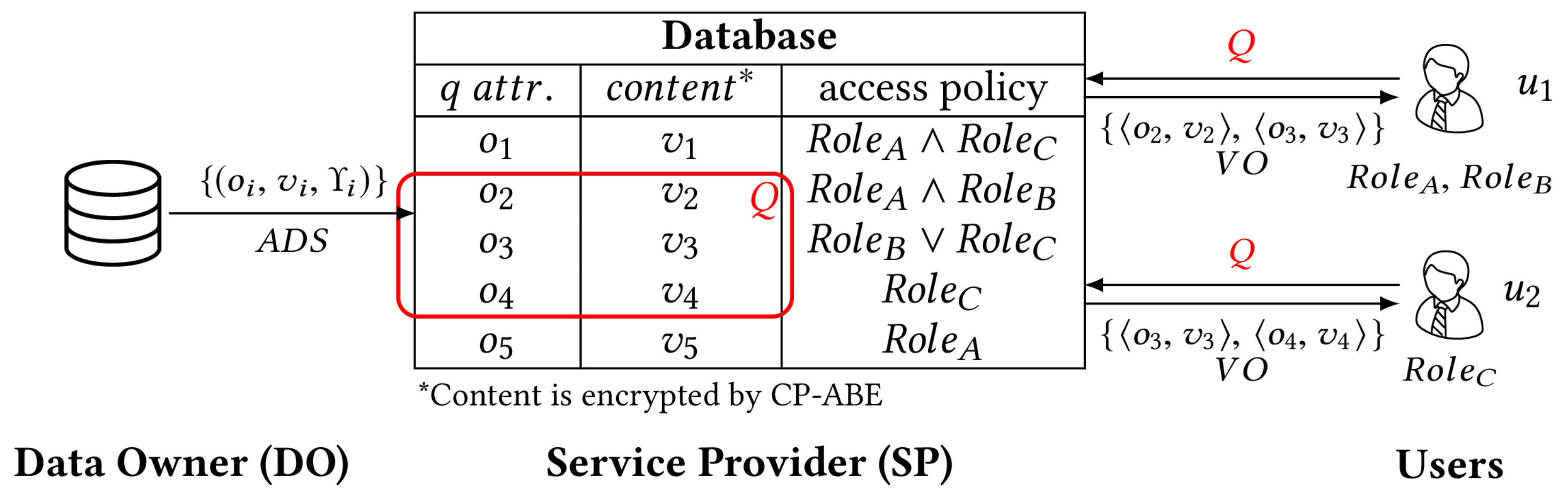
OBJECTIVES

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


$\{(o_i, v_i, \Upsilon_i)\}$
ADS
Q
Q
Q
u_1
$\{\langle o_2, v_2\rangle, \langle o_3, v_3\rangle\}$
VO
$Role_A, Role_B$
u_2
$\{\langle o_3, v_3\rangle, \langle o_4, v_4\rangle\}$
VO
$Role_C$
Data Owner (DO)
Service Provider (SP)
Users

Database		
q attr.	*content**	access policy
o_1	v_1	$Role_A \wedge Role_C$
o_2	v_2	$Role_A \wedge Role_B$
o_3	v_3	$Role_B \vee Role_C$
o_4	v_4	$Role_C$
o_5	v_5	$Role_A$

*Content is encrypted by CP-ABE

Fig. 1: Verifiable Attribute-based Search

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.

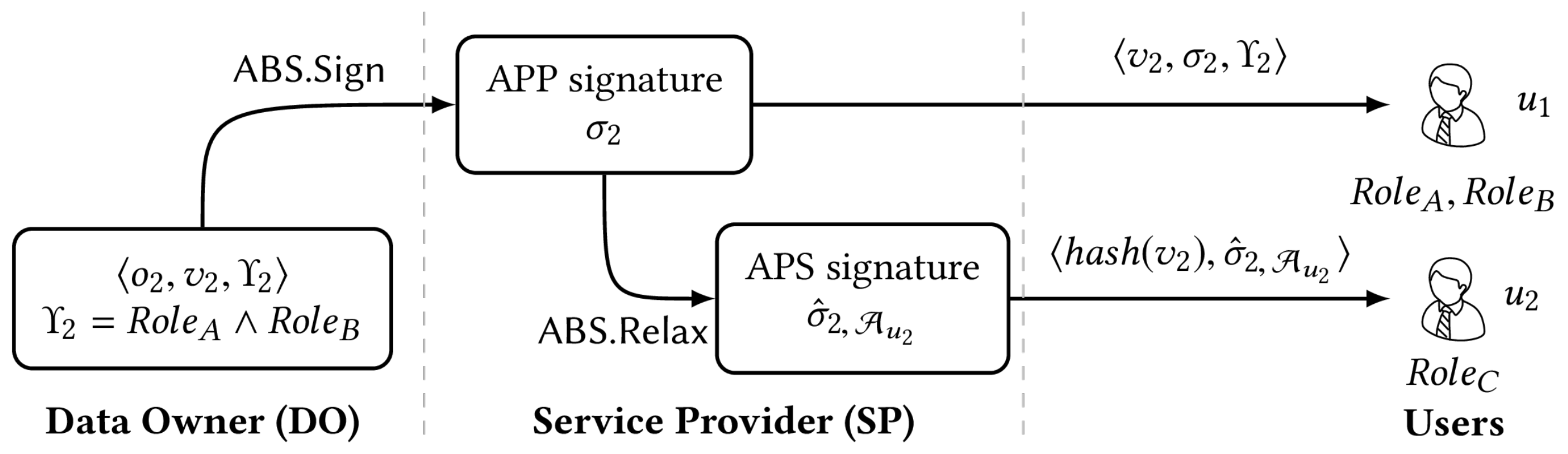

ABS.Sign
APP signature
σ_2
$\langle o_2, v_2, \Upsilon_2\rangle$
$\Upsilon_2 = Role_A \wedge Role_B$
ABS.Relax
APS signature
$\hat{\sigma}_2, \mathcal{A}_{u_2}$
$\langle v_2, \sigma_2, \Upsilon_2\rangle$
u_1
$Role_A, Role_B$
$\langle hash(v_2), \hat{\sigma}_2, \mathcal{A}_{u_2}\rangle$
u_2
$Role_C$
Data Owner (DO)
Service Provider (SP)
Users

Fig. 2: ADS Generation and Query Processing

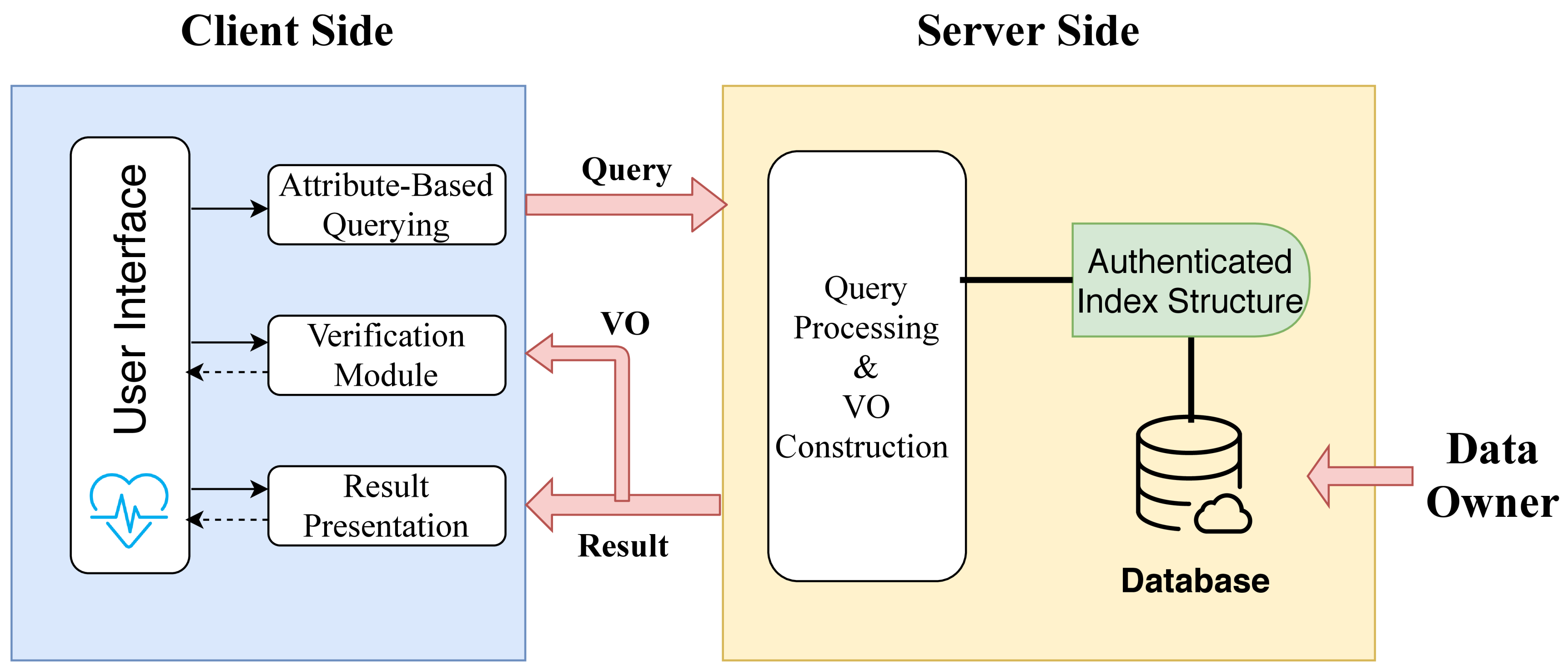
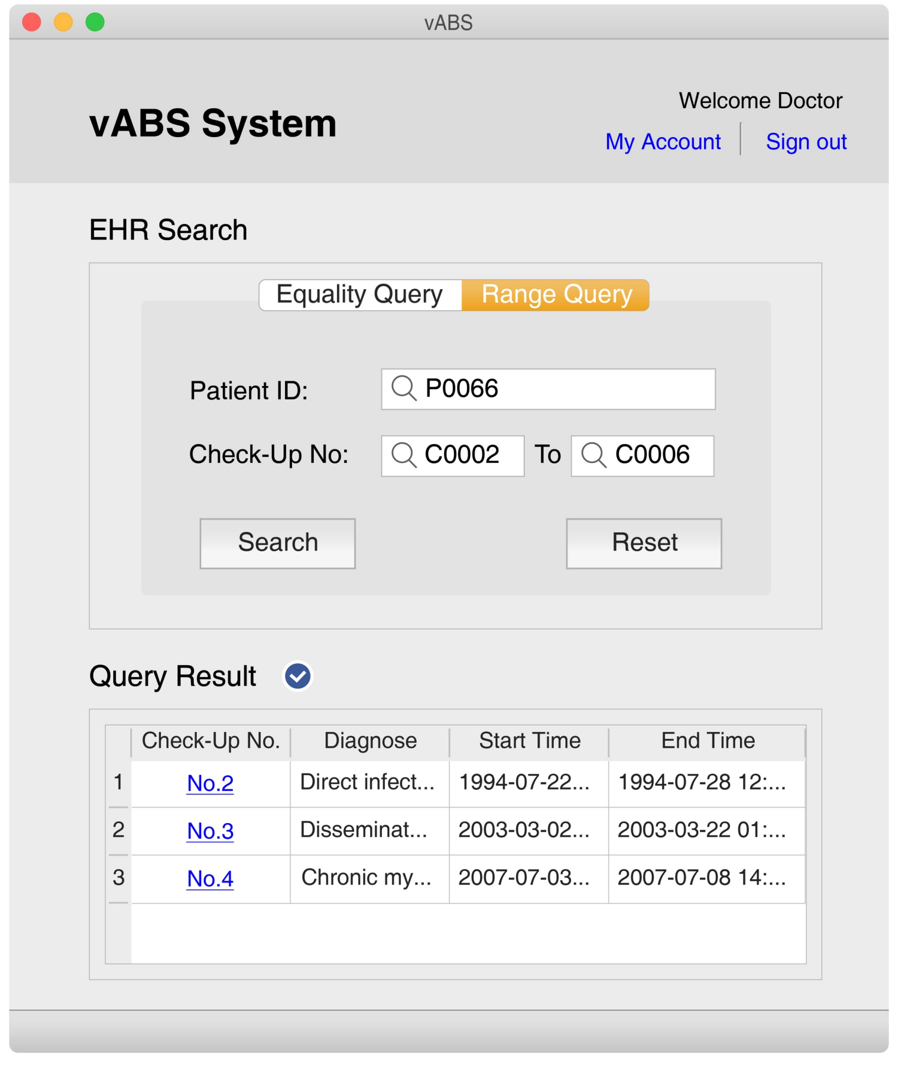


Fig. 3: System Architecture


vABS

vABS System

Welcome Doctor
My Account | Sign out

EHR Search

Equality Query | Range Query

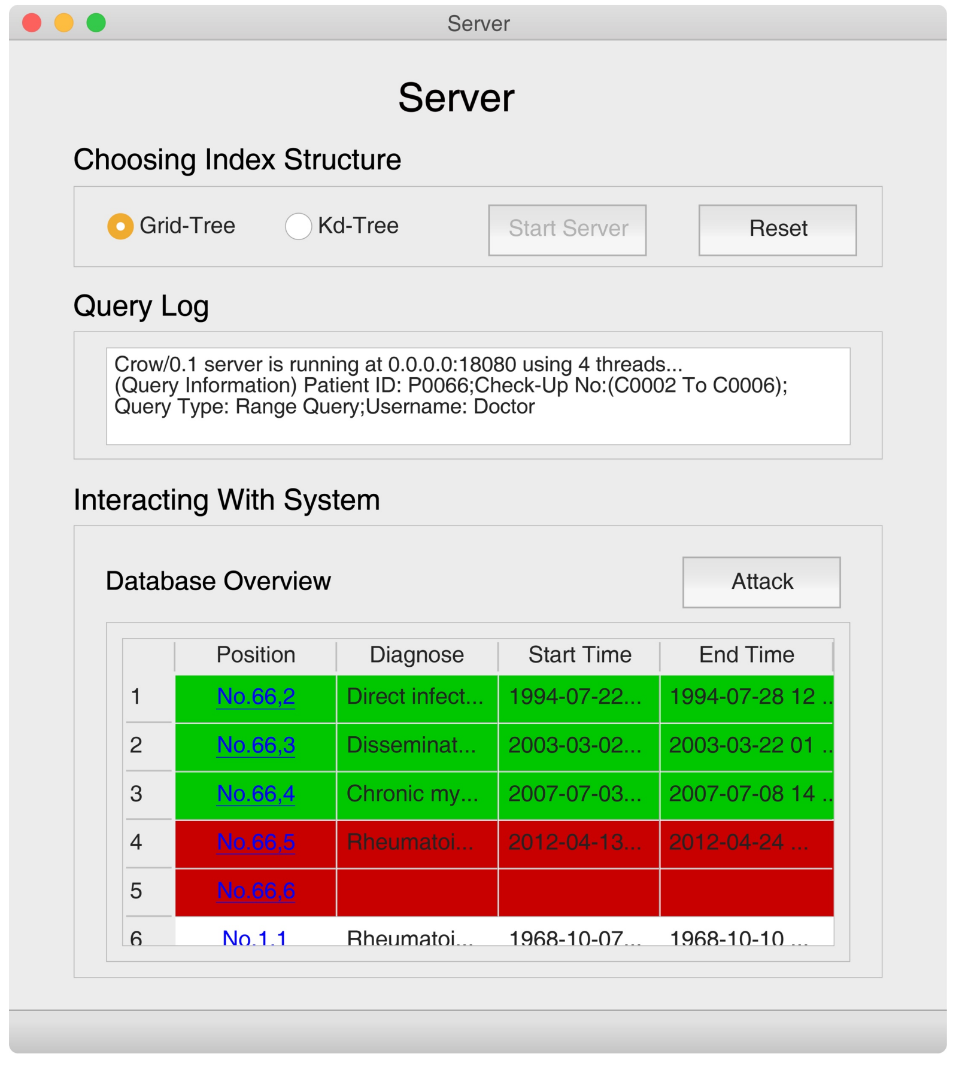
Patient ID: P0066
Check-Up No: C0002 To C0006

Search | Reset

Query Result ✓

	Check-Up No.	Diagnose	Start Time	End Time
1	No.2	Direct infect...	1994-07-22...	1994-07-28 12:...
2	No.3	Disseminat...	2003-03-02...	2003-03-22 01:...
3	No.4	Chronic my...	2007-07-03...	2007-07-08 14:...

Fig. 4: Client Interface


Server

Server

Choosing Index Structure

● Grid-Tree ○ Kd-Tree | Start Server | Reset

Query Log

```
Crow/0.1 server is running at 0.0.0.0:18080 using 4 threads...
(Query Information) Patient ID: P0066;Check-Up No:(C0002 To C0006);
Query Type: Range Query;Username: Doctor
```

Interacting With System

Database Overview | Attack

	Position	Diagnose	Start Time	End Time
1	No.66,2	Direct infect...	1994-07-22...	1994-07-28 12 ..
2	No.66,3	Disseminat...	2003-03-02...	2003-03-22 01 ..
3	No.66,4	Chronic my...	2007-07-03...	2007-07-08 14 ..
4	No.66,5	Rheumatoi...	2012-04-13...	2012-04-24 ...
5	No.66,6			
6	No.1,1	Rheumatoi...	1968-10-07...	1968-10-10 ...

Fig. 5: Server Interface

SELECTED PUBLICATIONS

1. C. Xu, J. Xu, H. Hu, and M. H. Au, “When query authentication meets fine-grained access control: A zero knowledge approach,” in Proceedings of the 2018 ACM SIGMOD International Conference on Management of Data, Houston, TX, USA, Jun. 2018, pp. 147–162.
2. Y. Ji, C. Xu, J. Xu, and H. Hu, “vABS: Towards Verifiable Attribute-Based Search over Shared Cloud Data” in Proceedings of the 35th IEEE International Conference on Data Engineering (ICDE ’19), Macau SAR, China, 2019, pp. 2028–2031.
3. C. Zhang, C. Xu, J. Xu, and B. Choi. "Distributed kNN Query Authentication." Proc. the 19th IEEE International Conference on Mobile Data Management (MDM '18), Aalborg, Denmark, June 2018, pp. 167-176.
4. C. Xu, Q. Chen, H. Hu, J. Xu, and X. Hei, “Authenticating Aggregate Queries over Set-Valued Data with Confidentiality.” IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 30, no. 4, pp. 630–644, Apr. 2018.