



Leveraging Semantic Context to Establish Access Controls for Secure Cloud-Based EHRs

Redwan Walid*, Karuna P. Joshi*, Seung Geol Choi†

*University of Maryland, Baltimore County

†United States Naval Academy

Email: rwalid1@umbc.edu, kjoshi1@umbc.edu, choi@usna.edu



Motivation

With the growth of healthcare systems and data, medical organizations are concerned about storing data to provide fast services while adhering to healthcare regulations.

The heterogeneous medical data makes it challenging for the existing healthcare systems as they often use relational databases.

The data retrieval performance of the current systems decreases with the increasing patient data, and they fail to adapt to changes with time due to having a fixed schema.

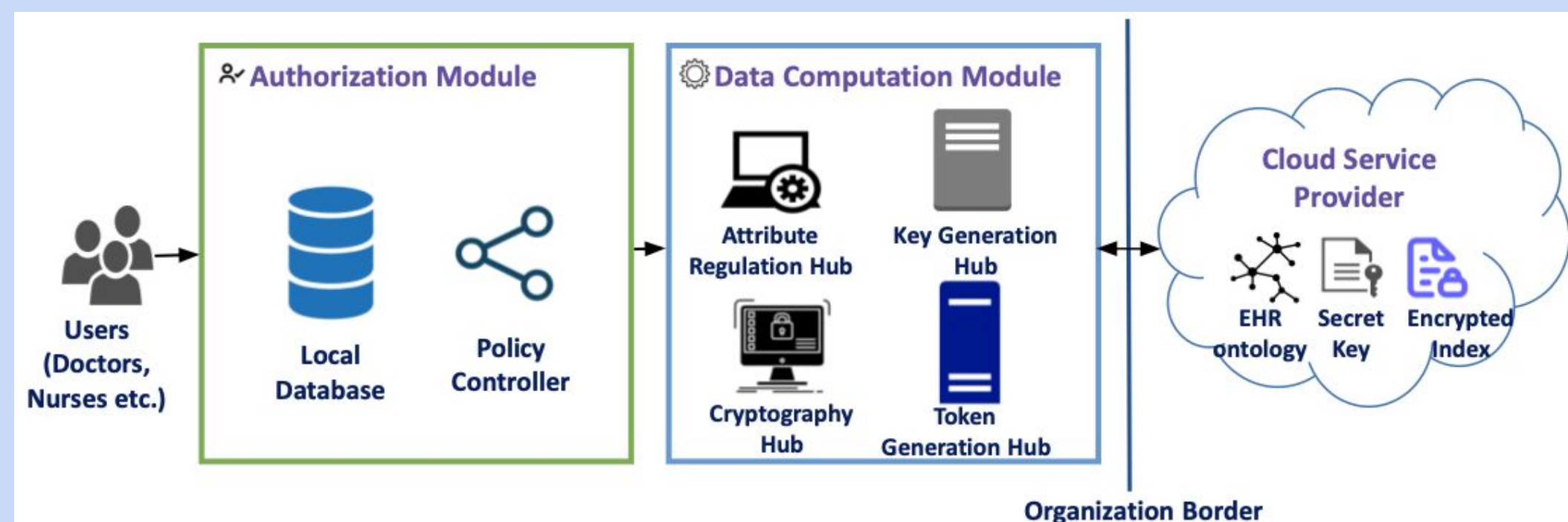
Approach

The knowledge graph handles system functions such as attribute based access control, attribute based encryption, user attribute revocation, searchable encryption, and data storing.

The knowledge graph stores encrypted data in the nodes that can maintain stable performance and handle heterogeneous data.

System Architecture

The system is split into two sections: Authorization Module and Data Computation Module within the organization and Cloud Service Provider outside the organization boundary. Authorization module allows user request checks, access control and semantic reasoning. Data Computation Module allows data cryptography, search token generation, encrypted index building, and attribute revocation.



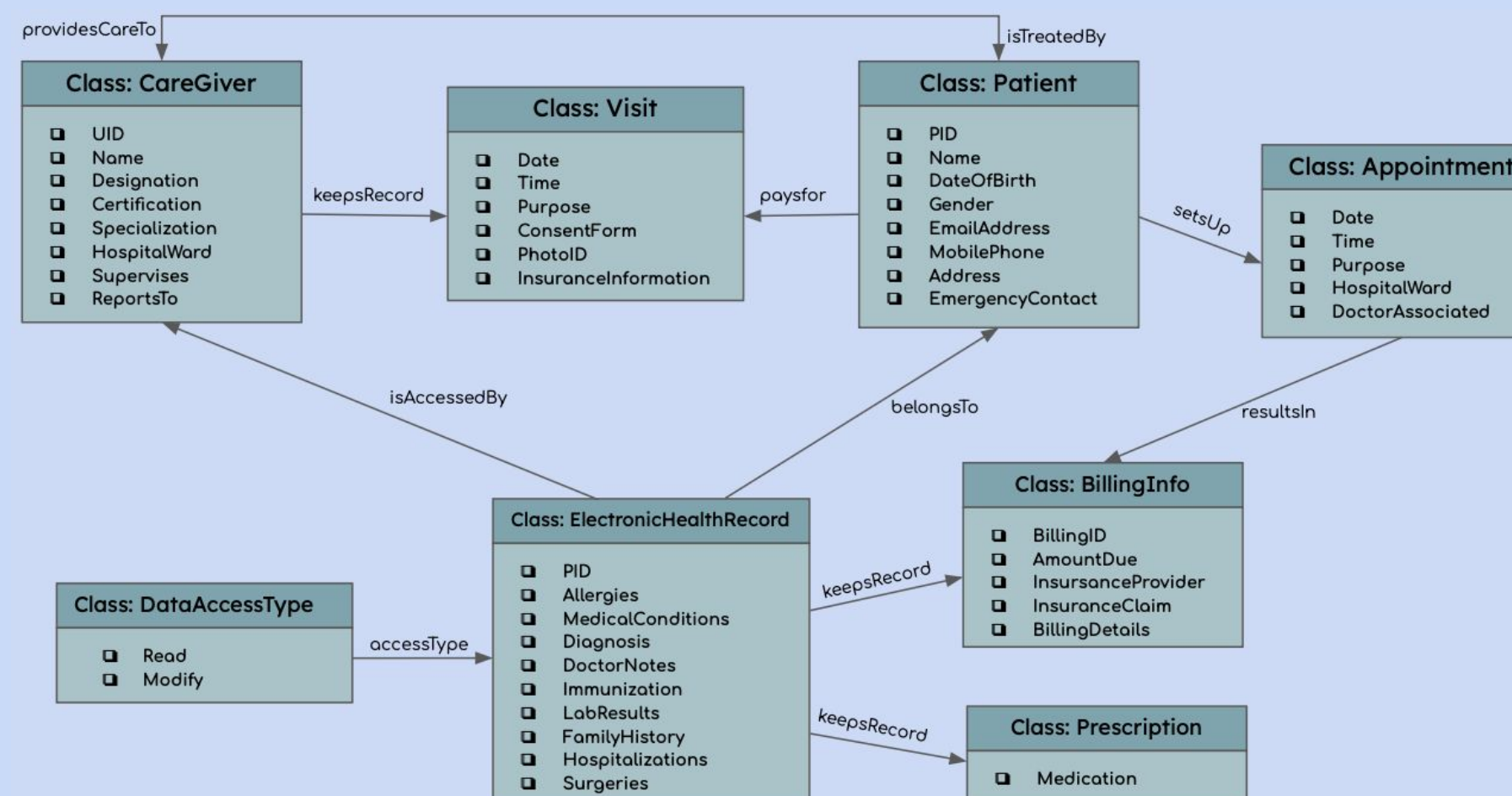
Performance Evaluation

The tables show the query performances in the system with flat files and the new system and highlight the percentage decrease in time for different use cases.

Query Performances With Flat Files			
Data size	Retrieve (and Decrypt) (s)	Search (s)	Revoke (s)
40,000	0.0172066	0.1847897	0.0193267
80,000	0.0174678	0.3376495	0.0184021
120,000	0.0173397	0.493178	0.0176004
160,000	0.0182211	0.6392195	0.0175358
200,000	0.0186612	0.7903189	0.0167967

Query Performances In the New System			
Data size	Retrieve (and Decrypt) (s)	Search (s)	Revoke (s)
40,000	0.0103081	0.1847897	0.0106127
80,000	0.0106438	0.3376495	0.0102164
120,000	0.0103354	0.493178	0.0105571
160,000	0.0102828	0.6392195	0.0105158
200,000	0.0108574	0.7903189	0.0100075

Knowledge Graph



Use Case	Percentage Decrease in Query Time for Different Data Sizes in New System				
	40,000	80,000	120,000	160,000	200,000
Decrypt (and Retrieve)	40.09%	39.07%	40.40%	43.57%	41.82%
Revoke	45.09%	44.48%	40.02%	40.03%	40.42%