Federated Sharing of Disparate Database Resources

Joshua Roberts
System Goal

*Sharing data between different organizations*

Motivation: To improve collaboration among alliances.

Examples:

- Share medical information related to patient care in collaboration with multiple providers;
- Share data among law enforcement agencies to aid investigations;
- Share clinical trial data among multiple research organizations to discover new therapeutics;
- Share data from IoT systems among different organizations to amass data to find optimizations and to build innovations.
System Goal

**Problem:**
- Multiple types of DBMS with different schema makes sharing data between different organizations a challenge.
- Solution had to be non-intrusive while maintaining the security, privacy, and integrity of the data.

**Approach:**
- Leverage two proven NIST technologies: Next Generation Database Access Control (NDAC), and data block matrix to have controlled shared access.
- Exchange attributes not data
Approach - NDAC

• Middleware that leverages NGAC and policy review for imposing access control over database queries
• Eliminates the need to implement and manage access control in the application or DBMS
• Translates a user’s query to a **permitted** query for Select, and Grant/Deny for Update, Delete, and Insert
  • User’s query may fetch entire data sets and NDAC restricts access to the set of data permissible for the user.
• Enforcement of policy combinations over DBMS data down to the field level
NDAC Architecture

Data/
Deny
SQL, Uid

Access
Manager

Data

Permitted SQL

Database

Deny/Permitted SQL(s)

SQL, Uid

Translator

NGAC Input

Authorization
Response

Policy Analytics

NGAC
Authorization
Engine

Access
Control
Data

NDAC components shown in red
Modeling SQL in NGAC
Approach - Data Block Matrix

- A NIST developed distributed ledger
  - integrity protection of a blockchain but with the ability to edit or delete data.
- Provides an API for storing, managing and sharing attributes
  - Stores a catalog of common attributes using standard nomenclature (e.g., SNOMED-CT) in the federation (e.g., Dr, Nurse, Patient, Clerk, HR, Supervisor)
  - Enables user access to the resources of other Relying Party’s (RPs), not for accessing resources in their own organization.
- Establishing trust in the federation (e.g., who under what authority can create/delete in the DBM.)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>X_{0,0}</td>
<td>X_{0,1}</td>
<td>X_{0,2}</td>
<td>X_{0,3}</td>
<td>X_{0,4}</td>
</tr>
<tr>
<td>1</td>
<td>X_{1,0}</td>
<td>X_{1,1}</td>
<td>X_{1,2}</td>
<td>X_{1,3}</td>
<td>X_{1,4}</td>
</tr>
<tr>
<td>2</td>
<td>X_{2,0}</td>
<td>X_{2,1}</td>
<td>X_{2,2}</td>
<td>X_{2,3}</td>
<td>X_{2,4}</td>
</tr>
<tr>
<td>3</td>
<td>X_{3,0}</td>
<td>X_{3,1}</td>
<td>X_{3,2}</td>
<td>X_{3,3}</td>
<td>X_{3,4}</td>
</tr>
<tr>
<td>4</td>
<td>X_{4,0}</td>
<td>X_{4,1}</td>
<td>X_{4,2}</td>
<td>X_{4,3}</td>
<td>X_{4,4}</td>
</tr>
<tr>
<td></td>
<td>H_{0,}</td>
<td>H_{1,}</td>
<td>H_{2,}</td>
<td>H_{3,}</td>
<td>H_{4,}</td>
</tr>
</tbody>
</table>
Operational Sharing of Data Resources

Diagram showing interactions between Endocrinologist, Patient Portal, Gastroenterologist, IDP, Data Block Matrix, and SQL databases.
Federated Consent Scenario

• Gastroenterologist doctor requests access to patient1’s endocrinologist record
• Patient1 accepts request
• Doctor is onboarded into endocrinologist with attributes from the data block matrix
• Doctor accesses patient1’s record at the endocrinologist
Gastroenterologist requests access to patient1’s endocrinologist record
Patient1 accepts request and Gastro Doctor is onboarded
Gastro Doctor accesses patient1’s record at the endocrinologist
Demo User Story

• Patient1 is 15 years old
• Diagnosed with T1D at the age of 10
• Patient1_mom has control of patient1’s record
• Sees a primary care physician and an endocrinologist to maintain T1D
• Recently visited the primary care physician with symptoms of celiac disease, so the doctor referred patient1 to a gastroenterologist
• Patient1 and patient1_mom are about to visit the gastroenterologist
Links

• Data Block Matrix Whitepaper

• Data Block Matrix GitHub
  • https://github.com/usnistgov/blockmatrix

• NIST Policy Machine GitHub
  • https://github.com/PM-Master/policy-machine-core

• NDAC Whitepaper
  • https://csrc.nist.gov/publications/detail/conference-paper/2017/03/24/imposing-fine-grain-ngac-over-database-queries