Problem Statement

- Data is transient while queries remain continuous.
- Data Provider does not control processing location
- Clouds and Data Consumers may not be trusted to access data
- Access Controls are difficult to enforce remotely
- Computation must still be performed on the cloud

Idea

- Realtime, cryptographically enforced access controls
- Key management based on user attributes
- Combine policies from data providers, consumers, and computation nodes
- Support almost any type of query on remote servers

Security Punctuations

- Policies are transmitted and updated using a modification to the notion of Security Punctuations.
- Security Punctuations are special tuples injected into streams.
- Punctuation frequency affects throughput, but is not as detrimental as ABE every tuple.

Enabling Computation on the Server

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Types of Queries</th>
<th>Supported Operators</th>
<th>Information Leaked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Deterministic</td>
<td>Equality</td>
<td>Select, Project, Count, Order, Group, Equi-Join</td>
<td></td>
</tr>
<tr>
<td>Order Preserving</td>
<td>Range</td>
<td>Select, Join, Count</td>
<td></td>
</tr>
<tr>
<td>Homomorphic</td>
<td>Summation</td>
<td>Sum</td>
<td>Partial Order</td>
</tr>
</tbody>
</table>

Access Control Policies

- Data Provider uses Attribute Based Access Controls (ABAC) enforced by Attribute Based Encryption (ABE)

Combining Policies

- 3 Different Policies:
  - Data Provider: Nurse or Doctor
  - Client: George, Marge, and Alice
  - CRN: Only Client 1 and Client 4

Result:

- Only Marge and Alice are permitted access.

Other Experimental Results

<table>
<thead>
<tr>
<th>T/s</th>
<th>Enc</th>
<th>Dec</th>
<th>ABE</th>
<th>Comp</th>
<th>Trans</th>
<th>Wait</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,000</td>
<td>4.0</td>
<td>3.8</td>
<td>6.0</td>
<td>41.2</td>
<td>9.5</td>
<td>35.6</td>
</tr>
<tr>
<td>4,000</td>
<td>4.0</td>
<td>5.3</td>
<td>6.1</td>
<td>61.7</td>
<td>10.3</td>
<td>12.6</td>
</tr>
<tr>
<td>6,000</td>
<td>3.8</td>
<td>7.1</td>
<td>6.2</td>
<td>69.0</td>
<td>12.2</td>
<td>1.6</td>
</tr>
<tr>
<td>8,000</td>
<td>3.9</td>
<td>8.6</td>
<td>5.8</td>
<td>76.8</td>
<td>15.9</td>
<td>0.0</td>
</tr>
</tbody>
</table>

References and Acknowledgements:


This work was supported by the NSF under awards CNS-1253204 and IIS-0746696.