The HybrEx Model for Confidentiality and Privacy in Cloud Computing

Steven Y. Ko¹, Kyungho Jeon¹ and Ramsés Morales²
¹Department of Computer Science and Engineering, University at Buffalo and ²Xerox Research Center Webster

Research Motivation

• Some just don't trust the clouds.
• Confidentiality and privacy concerns
• Threats do exist.
• However, cloud computing offers benefits.
• Elasticity
• Pay-as-you-go
• Availability & maintenance

How Much Can We Utilize Clouds without Sacrificing Confidentiality and Privacy?

No Utilization
No Trust

Exploring the Middle

Full Utilization
Full Trust

How Much Do We Trust the Clouds?

<table>
<thead>
<tr>
<th></th>
<th>Computation Code</th>
<th>Data</th>
<th>Execution Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Cloud</td>
<td>Trusted</td>
<td>Trusted</td>
<td>Trusted</td>
</tr>
<tr>
<td>Public Cloud</td>
<td>Untrusted</td>
<td>Untrusted</td>
<td>Untrusted</td>
</tr>
</tbody>
</table>

Integrity

• Data integrity
  • Keep the hashes of the public data in the private cloud
  • Computation integrity
  • Re-execute every task: only for accounting
  • Selectively check the results from the public cloud

Our Approach of Hybrid Execution

• Our approach: integration with safety

HybrEx (Hybrid Execution)

• Partitions data, computation and system
• Utilizes public clouds only for public data and computation

HybrEx MapReduce and HybrEx Bigtable

New Execution Categories

(a) Vertical Partitioning
(b) Horizontal Partitioning
(c) Map Hybrid
(d) Hybrid