Compliance-preserving Cloud Storage Federation
based on Data-driven Usage Control

Tobias Wüchner, Technische Universität München
Steffen Müller, Karlsruhe Institute of Technology
Robin Fischer, Karlsruhe Institute of Technology

Motivation

Single Provider Cloud Storage

Data availability entirely depends on provider availability. Provider failure leads to full data unavailability.

Federated Cloud Storage

Transparent data distribution and replication among several cloud storage providers necessary to ensure data availability [1].

Problem

Compliance Issues in Federated Cloud Storage

Data Distribution and Replication

Limited Control on Data Flows

Compliance Issues

“How can we enhance user control for compliant data distribution and replication?”

Solution & Contribution

Idea: Leverage Data-driven Usage Control (DUC) for transparent and compliant data distribution and replication.

Goal

Anticipate data and mission-specific compliance requirements for federation data distribution decisions

Main Challenges

- Balance trade-off: Availability vs. Compliance
- Fine-grained per-data policy enforcement

Solution

1. User uploads data D with attached compliance policies P
2. a) Send P to DUC infrastructure; b) Send D to MetaStorage
3. MetaStorage intercepts attempted distribution events to storage locations L and asks DUC infrastructure for permission
4. DUC infrastructure (a)llows, (i)nhibits, or (m)odifies events
5. MetaStorage distributes D to storage locations L as granted
6. MetaStorage updates internal distribution table

Data-driven Usage Control:

“Enforcement of what should and what must not happen to all instances of a data item after its initial dissemination.” [2]

Evaluation

Security

<table>
<thead>
<tr>
<th>Threat</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy malicious policies</td>
<td>Authentication and Authorization</td>
</tr>
<tr>
<td>Man-in-the-Middle attack</td>
<td>End-to-End Encryption</td>
</tr>
<tr>
<td>DoS via Policy Flooding</td>
<td>Restricted Policy Update Frequencies</td>
</tr>
</tbody>
</table>

Assumption: Trusted and tamper-proof DUC framework.

Performance

<table>
<thead>
<tr>
<th>System</th>
<th>Avg. Lat.</th>
<th>Min. Lat.</th>
<th>Max. Lat.</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaStorage</td>
<td>207 ms</td>
<td>103 ms</td>
<td>515 ms</td>
<td>4.72 Ops/s</td>
</tr>
<tr>
<td>MetaStorage + DUC</td>
<td>261 ms</td>
<td>201 ms</td>
<td>1306 ms</td>
<td>3.77 Ops/s</td>
</tr>
<tr>
<td>Overhead</td>
<td>+26%</td>
<td>+95%</td>
<td>+153%</td>
<td>-20%</td>
</tr>
</tbody>
</table>

Average overhead of 20% acceptable in compliance-critical scenarios.

References

3. Tobias Wüchner, Technische Universität München, tobias.wuechner@tum.de
4. Steffen Müller, Karlsruhe Institute of Technology, st.mueller@kit.edu
5. Robin Fischer, Karlsruhe Institute of Technology, robin.fischer@kit.edu

Contact