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

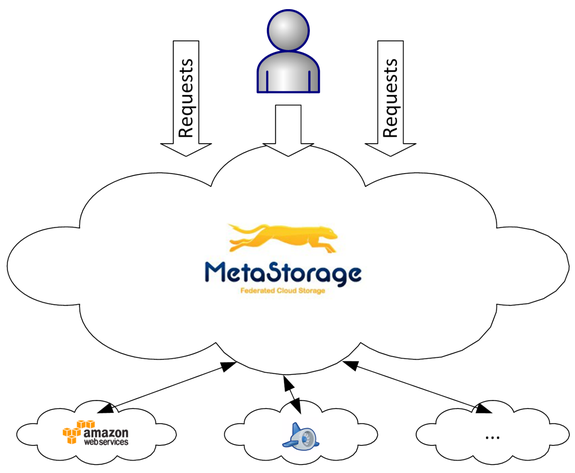
Tobias Wüchner, Technische Universität München
Steffen Müller, Karlsruhe Institute of Technology
Robin Fischer, Karlsruhe Institute of Technology

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

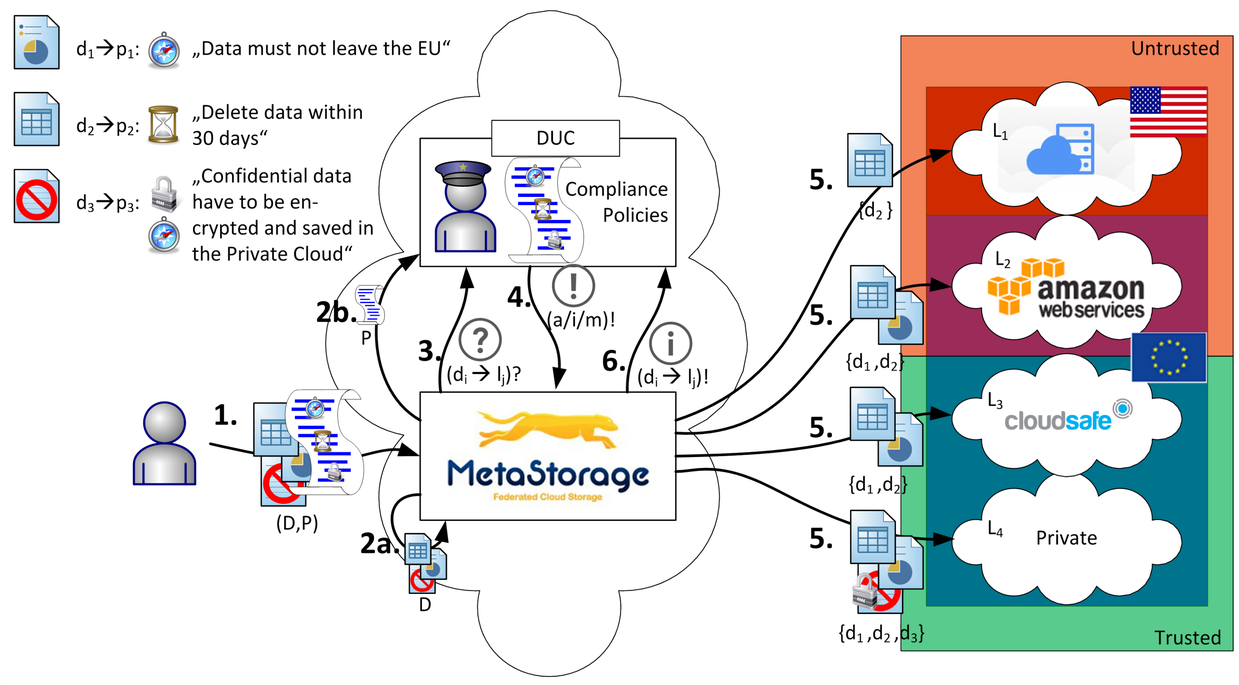
Main Challenges

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

Contributions

- Compliance-aware cloud storage federation
- Light-weight compliance proxy
- Non-intrusive compliance policy enforcement
- Supports multi-dimensional compliance policies
- Inter-provider provenance tracking of data
- Comparably low impact on efficiency
- No need of provider-side modifications

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

Compliance Requirements

- **Spatial Requirements**
  e.g.: Transfer personal data only if destination country ensures an adequate level of protection. (EU Directive 95/46/EC)

- **Temporal Requirements**
  e.g.: Audit-related information must be maintained for a time period not less than 7 years. (Sarbanes-Oxley Act)

- **Qualitative Requirements**
  e.g.: Access to and transportation of financial data must be secured. (PCI-DSS)

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

Threat	Countermeasures
Deploy malicious policies	Authentication and Authorization
Man-in-the-Middle attack	End-to-End Encryption
DoS via Policy Flooding	Restricted Policy Update Frequencies

Assumption: Trusted and tamper-proof DUC framework.

Performance

System	Avg. Lat.	Min. Lat.	Max. Lat.	Throughput
MetaStorage	207 ms	103 ms	515 ms	4.72 Ops/s
MetaStorage + DUC	261 ms	201 ms	1306 ms	3.77 Ops/s
Overhead	**+26%**	**+95%**	**+153%**	**- 20%**

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

References

1. Bermbach, Klems, Menzel, and Tai, "Meta-storage: A federated cloud storage system to manage consistency-latency tradeoffs," in Proc. of CLOUD'11, 2011.
2. Pretschner, Lovat, and Büchler, "Representation-independent data usage control", in Proc. of STM'11, 2011.

Contact

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