Evidence for Accountable Cloud Computing Services

Thomas Rübsamen, Christoph Reich
Hochschule Furtwangen University HFU

Aryan Taherimonfared, Tomasz Wiktor Wlodarczyk, Chunming Rong
Center for IP-based Service Innovation, TN-IDE, University of Stavanger
Agenda

1. Introduction
2. Accountability and evidence
3. What should be evidence?
4. Where is evidence collected?
5. Challenges
6. Summary
Introduction

• Transparency and control issues arise, when data is stored remotely in the cloud
  • Lost control over physical servers/networks
  • Service provision/de-provision
  • Tenant isolation
  • Data processing/movement
• Adding key terms to cloud SLAs is not enough
  • Processes and mechanisms must be developed to monitor and audit these terms
  • Providers must provide evidence
  • Cloud customer must be allowed to verify, that his data is being stored and maintained correctly in the cloud, and that his policies are adhered to
  • Evidence collection shall capture, integrate and process logs, (data) policies and context
• Showing what happens in the cloud and providing evidence for it can address transparency and accountability issues
Accountability and Evidence I

- Evidence may be derived from different sources, events and architectural layers
- Mapping of evidence to accountability contracts/SLAs and other policy requirements
- No efficient mechanisms to gather convincing evidence from verified log data
- No incentive for providers to publish log information
- How to make evidence gathering mechanisms compatible and interoperable?
Accountability and Evidence II

- Collect evidence to support (external) audits and verification
  - Evidence is provided to (automated) audits for fault detection
- Accountability attributes are assured by evidence
  - Attributability: a property of an observation can be assigned to an actor
  - Observability: how well internal actions of a system can be described by observing the external output
  - Assurance: Provision of evidence to proof an incident has happened / not happened
  - Verifiability: An aspect of a contractual relationship can be observed through evidence
Accountability and Evidence IV

Evidence for Accountable Cloud Computing Services

Accountability Contracts, SLAs → Policy Requirements

 Audit Verification → Evidence supports

Evidence → Attributability, Observability, Assurance, Verifiability

Evidence → Source 1: Log data
Evidence → Source 2: Log data
Evidence → Source 3: Log data

Mapping → Source 1, Source 2, Source 3

6/21/2013
What should be evidence?

- Information about data traveling in the cloud (where, jurisdiction)
- Information about data access (by whom and when, role, identity, purpose, time)
- Information about processes (data lifecycle events)
- Logging data from involved components/services
Where is Evidence Collected - Gathering Points

- Guest App
- Guest OS
- Hypervisor
- Host OS
- Hardware
- Network
- CMS

- SaaS
- PaaS
- IaaS
- Guest Usage
Challenges of Evidence

- Large amounts of data (Big Data?)
- Various data formats
- How can evidence be trusted (certification, singing, tamper-evident recording)
- Retention-time of evidence (laws may apply)
- Interoperability of evidence collection in multi-provider scenarios (cloud provider accountability chains)
- Multi-tenancy in monitoring tools and devices
Summary

- Build an evidence base for collected information to assure accountability and support audits
- Evidence will be collected at many architectural layers in the cloud stack
- Many challenges to address
Thank You for Your Attention!