Trust mechanisms for clouding computing

Jingwei . Huang   David. M Nicol

Information Trust Institute
University of Illinois at Urbana-Champaign

presented by Ji Wang
Outline

1 Problem description and background knowledge
   - The Basic Problem That We Studied

2 State-of-art trust mechanisms in cloud
   - General description
   - Detailed description

3 The author’s story
   - Separate view
   - Integrated view
Outline

1. Problem description and background knowledge
   - The Basic Problem That We Studied

2. State-of-art trust mechanisms in cloud
   - General description
   - Detailed description

3. The author’s story
   - Separate view
   - Integrated view
Introduction

Problem
  ▶ What does “trust” mean in cloud computing.
  ▶ How the customer, provider, and society in general establish that trust in cloud computing.

Challenges of trust in cloud computing
  ▶ Require some formal trust mechanisms: cloud broker, auditors...

This paper:
  ▶ focus on the conceptual basis instead of mathematical modeling.
How to define trust in general

- Definition of trust a mental state with three elements:
  - Expectancy: the trustor expects a specific behavior from the trustee.
  - Belief: the trustor believes the expected behavior occurs based on the evidence of trustee.
  - Willingness to take risk: the trustor is willing to take risk for that belief.
How to define trust in general

- **Types of trust**

<table>
<thead>
<tr>
<th>Types of trust</th>
<th>trust in performance (first-hand trust)</th>
<th>trust in belief (second-hand trust)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>about what the trustee <strong>performs</strong></td>
<td>about what the trustee <strong>believes</strong></td>
</tr>
<tr>
<td>Feature</td>
<td>not transitive</td>
<td>transitive</td>
</tr>
<tr>
<td>Notation</td>
<td>$\text{trus}_p(d,e,x,k)$</td>
<td>$\text{trus}_b(d,e,x,k)$</td>
</tr>
</tbody>
</table>
  
  $d$ : trustor, $e$ : trustee,
  $x$ : performance,
  $k$ : context

- **Summary:** cloud computing should have the same semantics structure as above. We need to define the specific expectancy and characteristics in the context of cloud computing.
Outline

1 Problem description and background knowledge
   - The Basic Problem That We Studied

2 State-of-art trust mechanisms in cloud
   - General description
   - Detailed description

3 The author’s story
   - Separate view
   - Integrated view
What are they

- Existing trust mechanisms in the cloud:
  - Reputation based trust.
  - SLA verification based trust.
  - Cloud transparency mechanisms.
  - Trust as a service.
  - Formal accreditation, audit, and standards.

- Each of them is not enough by itself: only address one aspect of the problem.
Outline

1. Problem description and background knowledge
   - The Basic Problem That We Studied

2. State-of-art trust mechanisms in cloud
   - General description
   - Detailed description

3. The author’s story
   - Separate view
   - Integrated view
# Reputation based trust

<table>
<thead>
<tr>
<th>Name</th>
<th>Idea</th>
<th>Constraints</th>
</tr>
</thead>
</table>
| Reputation based trust | reputation: *a score reflection the overall opinion; a small number of scores on several major aspects of performance.* | - Complexity: too many cloud users and providers  
- reputation is helpful only when initially choosing a service, but not afterwards |
<table>
<thead>
<tr>
<th>Idea</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>verify and reevaluate the trust after establishing the initial trust.</td>
<td>Can not deal with “invisible” elements: security and privacy</td>
</tr>
<tr>
<td>service level agreement (SLA): legal contract between cloud users and service providers.</td>
<td>Cloud users can not evaluate on their own, require professional third party (cloud broker, cloud trust authority).</td>
</tr>
<tr>
<td>Idea</td>
<td>Constraints</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Cloud provider gives</td>
<td>Dishonest service provider:</td>
</tr>
<tr>
<td>self-assessments</td>
<td>filter out or change data</td>
</tr>
</tbody>
</table>
## Trust as a service

<table>
<thead>
<tr>
<th>Idea</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduce third-party professionals (commercial trust brokers), treat trust as a service <em>(Cloud Trust Authority)</em>.</td>
<td>Hard to establish basis for trust relation between cloud users and commercial trust brokers.</td>
</tr>
</tbody>
</table>
Formal accreditation, audit and standards

<table>
<thead>
<tr>
<th>Idea</th>
<th>Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>A trusted independent authority</td>
<td>Perfect idea, just does not exist. No formal process for assessment of cloud service by third parties.</td>
</tr>
</tbody>
</table>
Outline

1. Problem description and background knowledge
   - The Basic Problem That We Studied

2. State-of-art trust mechanisms in cloud
   - General description
   - Detailed description

3. The author’s story
   - Separate view
   - Integrated view
General description

- Three parts
  - Policy-based trust: use PKI to establish “formal” trust mechanism.
  - Evidence-based trust: attributes used as evidence.
  - Attribute assessments and certification: approach to deliver attributes

- Integrated view
  - Dependence between the trust in cloud entities and the sources of evidence for trust judgement
Policy-based trust (apply PKI idea)

Figure 1 PKI trust example. This example reveals trust relations in public key certification and validation.
Evidence-based trust

- Idea: use attributes as evidence to make trust decision (how to use semantics of trust to model trust in cloud).

- How to define trust (in performance and or in believe)
  - \( \text{believe}(u, \text{attr}_1(s, v_1)) \land \ldots \land \text{believe}(u, \text{attr}_n(s, v_n)) \rightarrow \text{trust}_\ast(u, s, x, c) \).
    - ★ \( u \): trustor; \( s \): trustee; \( x \): information created by \( s \); \( c \): a specific context.
    - ★ \( \ast \): either belief or performance.
    - ★ \( \text{attr}_k(s, v_k) \): \( s \) has attribute \( k \) with value \( v_k \).

- Then how to define believe
  - \( \text{trust}_\ast(p)(u, a, \text{attr}(s, v), c) \land \text{madeBy}(\text{attr}(s, v), a, c) \land \text{inContext}(c) \rightarrow \text{believe}(u, \text{attr}(s, v)) \)
    - ★ \( u \): trustor; \( s \): trustee; \( c \): a specific context; \( a \): attribute authority.
    - ★ \( \text{madeBy}(\text{attr}(s, v), a, c) \): \( a \) makes assertion that \( s \) have attribute with value \( v \) under \( c \).
    - ★ \( \text{trust}_\ast(p)(u, a, \text{attr}(s, v), c) \): as defined above.
How to define the attribute for evidence-based trust

- Attributes for evidence-based trust (two dimensions)
  - Domain-specific expectation: performance, security, privacy
  - Sources of trust: competency, good intention, consistency
- Different cloud users may consider different trust attributes.
- Relationship with policy-based trust: the belief that an entity conforms to a trusted policy implies the belief that the entity has a set of attributes associated with that policy
Attribute assessment and certification

- Idea: the sources of attributes assessment must be trustworthy.
- Sources of attributes:
  1. Cloud user observation: first-hand (most relevant), narrow vision (just one piece of information).
  2. Peer users’ opinion: indirect, How to aggregate: social network based; reputation based.
  3. Service provider’s statement: need to be verified before used, require third party independent professional organizations.
  4. Cloud auditor/accreditor’s assessment: objective and formal, but not real-time information.
  5. Cloud broker’s observation: real-time, relatively complete picture, non-objective.
Attribute assessment and certification

- Idea: the attributes need to be **distributed** in a trustworthy way.
- Attribute certificate: can be based on IETF X.509 AC standard, but need to adjust the followings:
  1. Include attributes like **security** and **privacy**.
  2. Find the right one to become Attribute Authority.
  3. Establish more complicated trust structure: cross-domain attribute certification and validation.
Outline

1 Problem description and background knowledge
   - The Basic Problem That We Studied

2 State-of-art trust mechanisms in cloud
   - General description
   - Detailed description

3 The author’s story
   - Separate view
   - Integrated view
An integrated view

- Dependence between the trust placed in various cloud entities and the sources of evidence for trust judgment.
  - Cloud entities: cloud auditor, cloud broker, cloud service provider, cloud service
  - Societal trust: foundational in all trust models, leads cloud users to put their trust in the accreditation of cloud entities including auditors, brokers, and service provider
  - Trust mechanisms
    1. already exist: reputation/recommendation, QoS/SLA monitoring, Self-assessment,
    2. not exist: attributes, policy compliance(Audit), accreditation.
## Expectancy to trust entities

<table>
<thead>
<tr>
<th>Role</th>
<th>Expectancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>auditor</td>
<td>the objective and professional assessment on a cloud entity’s service</td>
</tr>
<tr>
<td>broker</td>
<td>trustworthy value-added services</td>
</tr>
<tr>
<td>service provider</td>
<td>trustworthy cloud services</td>
</tr>
<tr>
<td>service</td>
<td>a set of attributes; reliability, safety, privacy</td>
</tr>
</tbody>
</table>
From cloud broker’s perspective

Figure 4 Evidence and chains for trust judgment on a cloud broker. Trust placed in a cloud broker is based on one or more of: (1) accreditation; (2) policy compliance; (3) certified attributes; (4) self-assessment and information revealing, which is based on the trust placed in this broker with respect to telling truth; (5) reputation calculated or recommendation made by another trusted broker.
Dependence from cloud service’s perspective

Figure 6 Evidence and chains for trust judgment on a cloud service. Trust placed in a cloud service is based on one or more of: (1) cloud service provider, whom is trusted; (2) policy compliance; (3) certified attributes; (4) QoS monitoring and SLA verification, which are conducted by a trusted party such as a trusted broker; (5) reputation calculated or recommendation made by a trusted broker.
The whole picture

**Figure 7 Chains of trust relations in clouds.** This figure provides an integrated picture to illustrate the chains of trust relations from a cloud user to a cloud service and related cloud entities, where accreditation is omitted for simplicity.
Summary

- The state of art:
  - What are the existing provided schemes
  - Why they are not enough by themselves

- The provided scheme:
  - Three separate parts
  - Integrated view

- Future work:
  - Mathematical formal framework
Questions

Thanks a lot :)