A Framework for Evaluating Trust of Service Providers in Cloud Marketplaces

Sheikh Mahbub Habib
Telecooperation Group
Technische Universität
Darmstadt/CASED
Germany
sheikh.habib@cased.de

Vijay Varadharajan
INSS Research Group
Macquarie University Sydney
Australia
vijay@science.mq.edu.au

Max Mühlhäuser
Telecooperation Group
Technische Universität
Darmstadt/CASED
Germany
max@informatik.tu-darmstadt.de

ABSTRACT

The Cloud Security Alliance (CSA) provides a framework for cloud platform providers that manages standardized self-assessments regarding security controls. The framework as it stands does not allow consumers to specify and check their own requirements, nor does it contain any means for verifying the capabilities claimed by the providers. From a customer perspective, both these aspects are essential for evaluating the trustworthiness of cloud providers and for making an informed decision. We propose a novel concept for verifying the capabilities captured in the CSA's framework, plus a decision model that checks consumer requirements against the verification results. Our capability verification combines hard trust based on rigid validation with soft trust based on evidence about past behaviour. Elaborate formal methods are applied in both fields and combined into a single concept.

1. INTRODUCTION

Trust evaluation of service providers in emerging cloud marketplaces is one of the important challenges that consumers are facing at present. In such marketplaces, cloud providers offer similar kind of services with same kind of functionalities. Hence, the challenge for consumers is to determine which cloud providers are trustworthy according to their own requirements before they decide to take up the services offered by those cloud providers. The *CSA* partly address this challenge by introducing a self-assessment questionnaire framework, i.e., *CAIQ*[1] (Consensus Assessments Initiative Questionnaire) as a part of their *Trusted Cloud* initiative. The *CAIQ* is designed for the cloud providers who want to publicize security-specific capabilities regarding the services they offer for prospective consumers. At present, several providers have published completed *CAIQ*s through the STAR[2] (Security, Trust and Assurance Registry) hosted by the *CSA*.

Table 1: Taxonomy of Trust Properties

Trust Properties (listed by CAIQ Id)	Validation Authorities
$CO-01$	3^{rd}-party Certified
$CO-03$	Self Certified
$DG-01$	3^{rd}-party Certified
$IS-02$	Self-claimed
$IS-03$	3^{rd}-party Certified
$IS-21$	Self- or 3^{rd}-party certified

With the published CAIQs, consumers are able to browse security-specific capabilities (we denote these capabilities as "trust properties") of the cloud providers. The fundamental question that arises is, how do consumers *trust* that these properties are indeed satisfied as claimed by the providers and that they fulfil the consumers' requirements. In this paper, we propose a framework by leveraging the notion of *hybrid trust* [2] to verify the *trust properties*. Additionally, our proposed framework includes a decision model that enables consumers to determine trustworthiness of cloud providers by checking consumers' requirements against the verification results.

2. TRUST EVALUATION FRAMEWORK

Our proposed evaluation framework (cf. Fig. 1) leverage *hybrid* trust to verify the properties that are claimed by the cloud providers. In this context, *hybrid* trust combines the concepts of *hard* and *soft* trust. *Hard* trust is defined as trust that is derived from concrete security mechanisms such as validation of properties through certificates [4]. Usually, these mechanisms are characterized by certainty. *Soft* trust is defined as trust that is derived from past experiences and behaviour associated with an entity, e.g., Certification Authority (*CA*) or Cloud Provider (CP). The related mechanisms [1] of soft trust, as used in various service environments, consider aspects such as intrinsic human perceptions and interaction experiences to determine a trustworthy entity.

In the context of *CAIQ*, there are properties (cf. Table 1), P_1 that can be validated using property attestation technique by third-party (3^{rd}*-party Certified*) or cloud providers (*Self Certified*). For validating P_1 properties, we use the *hard* trust approach. There are another type of properties (cf. Table 1), P_2 which cloud providers claimed (*Self-claimed*) to have in their policy service. In order to assess P_2 properties, soft trust mechanisms are taken into account.

[1]https://cloudsecurityalliance.org/research/cai/

[2]https://cloudsecurityalliance.org/star/

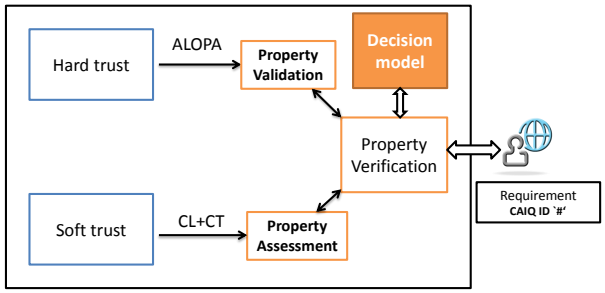

Figure 1: Conceptual Trust Evaluation Framework

Usually, soft trust mechanisms consider one's own direct experience with the other party in the past, recommendations from others or a combination of both. However, trust saturation is a common problem with soft trust based approaches alone. On the other hand, hard trust may not be aware of dynamic changes. In this sense, hard trust approaches are quite rigid, as they are usually based on single-time check which once bypassed put the service platforms in a vulnerable state. Combining *soft* and *hard* trust mechanisms in a hybrid model overcomes the limitations of these mechanisms used separately. Hence, a hybrid trust model is a good option to evaluate the overall trust on cloud service platforms as well as on service providers.

The proposed framework consist of following three building blocks: i) *property validation* using *hard* trust mechanism, ii) *property assessment* using *soft* trust mechanism, and iii) a *decision model* using the threshold-based mechanism.

2.1 Property Validation

In order to validate the properties, a simple logic language ('ALOPA' [2]) was proposed to express the property relationships as well as the dependency among the properties. Using 'ALOPA', it is possible to validate whether a cloud platform satisfies a given property by extrapolating the available set of cloud-specific platform properties. For brevity, we are not going to discuss the 'ALOPA' language in detail. However, we describe its specific features that are required in the context of our proposed framework .

'ALOPA' consists of mainly seven predicate symbols namely '$HasC$', '$HasPF$', '$IFlow$', '$SatC$', '$SatPF$', '$PreReq$' and 'Do'. In this paper, we discuss the 'ALOPA' rules using five predicates which are '$HasC$', '$HasPF$', '$SatC$', '$SatPF$', and '$PreReq$'. 'Has' generally defines a hierarchical relationship between two entities and 'Sat' in general defines the relationship between an entity and the property it satisfies. Here, the entities are platforms and platform components. '$HasC$' defines the relationship between two components in a given platform and '$HasPF$' defines a same kind of relationship between a platform and a component. For instance, $HasC(c_1, c_2)$ is read as component 'c_1' has (or contains) the component 'c_2'. $HasPF(pf_1, c_1)$ is read as a platform pf_1 has the component c_1. $SatC(c_1, p_1)$ is interpreted as component c_1 satisfies property p_1 and $SatPF(pf_1, p_1)$ is interpreted as platform pf_1 satisfies property p_1. '$PreReq$' defines the 'prerequisite' relationship between two components or platforms in satisfying certain properties. For example, $PreReq((pf_1, p_1), (pf_1, p_2))$ is interpreted as platform pf_1 satisfies property p_1 only if the prerequisite property p_2 is satisfied in platform pf_1. The following example shows how 'ALOPA' predicate '$SatPF$' can be used to formalize the property relationships in the context of $CAIQ$ validation.

Cloud provider's claim regarding "antivirus application" $(IS-21)$ property is validated if antivirus (or anti-malware) software is installed or certified that the cloud platform is malware-free $(IS-21.1)$ and the signatures as well as lists of behavioural patterns are up-to-date $(IS-21.2)$. A suitable 'ALOPA' policy to validate the property is as follows:

$$SatPF(pf, IS-21) \leftarrow SatPF(pf, IS-21.1) \wedge SatPF(pf, IS-21.2) \quad (1)$$

2.2 Property Assessment

In certificate-based validation mechanisms, there are Certification Authorities (CAs) who certify the properties to be existent in cloud service platforms. The fundamental question that arises here is, how certain a user (U) can be that published properties ($CAIQ$ controls in $STAR$) of a cloud provider which are validated by the CAs indeed satisfy their requirements. We argue that given the nature of certificate-based validation, uncertainties are introduced by induced events in the attestation or certification process. There are several reasons for such uncertainties to arise which are detailed in [2]. These include uncertainties due to time-of-check-time-of-use vulnerabilities as well as uncertainties arising out of the trustworthiness of the CAs and their validation mechanisms.

The soft Trust Model (TM) uses CertainTrust and CertainLogic to assess trust under uncertainty [3]. In both models, trust is represented using an opinion metric which is denoted as o. Each opinion is represented as 3-tuple of values, $o = (t, c, f) \in \{[0,1] \times [0,1] \times [0,1]\}$ where t denotes average rating (relative frequency of positive or negative evidences), c denotes certainty associated with the average rating, and f denotes dispositional trust which can be derived independently. The notion of dispositional trust is not considered in the context of this paper.

The TM can be defined as TM = (E, TR, OP) where E includes U (User), CP (Cloud Provider) and CA (Certification Authority) as entities, TR defines the trust relationships that is shared between two entities for a given property, and OP is the set of CertainTrust (CT) and CertainLogic (CL) operations for management of the trust relationships. An example of a trust relationship is $TR = (U, CP, IS-21, satisfaction, Jul\ 11\ 2012\ 12:00, [1.0, 0.83], 5, 0, 1)$. This entry represents a trust relationship that is shared between a platform of a consumer (U) and a platform of a cloud provider (CP). U's platform has *satisfaction trust* on CP's platform that it satisfies the property $IS-21$. Trust is expressed by opinion metric $[1.0, 0.83]$ representing average rating and certainty respectively. This opinion is evaluated based on U's past experiences with CP where the given property was satisfied 5 times in the past (i.e., positive experience) and the outcome was indeterminable two times (i.e., uncertain experience). Experience was recorded on Jul 11 2012 12:00.

Trust Operations (OP) Trust operations are the basis for evaluating trust of cloud providers in marketplaces. These operations include evidence collection from past experiences, trust evaluation mechanisms and a model for trust comparison.

Evidence collection. Evidence is extracted either directly using one's own experiences termed as *direct experiences* or using referrals from others known as *recommendations*. An evidence is classified as positive (p), negative (n) and uncertain (u). Every evidence is extracted and recorded

Table 2: Experiments: Property Assessment

Trust Property	Trust Experience Base	Derived Trust	Trust Threshold (τ)
$IS-21$	$(U, CP, IS-21, satisfaction, Jul\ 11\ 2012\ 12:00, [1.0, 0.83], 5, 0, 1)$ $(U, CA, IS-21, certification, Jul\ 11\ 2012\ 12:00, [0.72, 0.84], 8, 3, 2)$ $(R_1, CP, IS-21, satisfaction, Jul\ 14\ 2012\ 12:00, [0.31, 0.94], 5, 11, 1)$ $(R_1, CA, IS-21, certification, Jul\ 14\ 2012\ 12:00, [0.90, 0.78], 10, 1, 3)$ $(R_2, CP, IS-21, satisfaction, Jul\ 16\ 2012\ 12:00, [1.0, 0.50], 1, 0, 1)$ $(R_2, CA, IS-21, certification, Jul\ 16\ 2012\ 12:00, [0.67, 0.75], 2, 1, 1)$	$(0.3690, 0.9178)$	$(0.80, 0.90)$

based on the induced events related to the validation mechanisms (e.g., attestation or certification process).

Trust evaluation. In this section, we briefly list the essential definitions used for trust evaluation in the proposed framework.

DEFINITION 2.1. *(Direct Trust) Direct Trust is the belief that one entity holds on another entity in certain context, based on it's* own evidences *of past experiences with that entity. The direct trust of a platform A about platform B is calculated by combining (using* AND *operator) satisfaction and certification opinion on the platform properties.*

$$^{A-dir}o_{B,(c_i,p_j)} = {}^{A}o_{B,sat(c_i,p_j)} \wedge {}^{A}o_{CA,cer(c_i,p_j)} \quad (2)$$

DEFINITION 2.2. *(Indirect Trust) Indirect Trust is the belief that one entity holds on another entity in certain context, based on the* recommendations *derived from its peer entities' past experiences with that entity. The indirect trust of a platform A about platform B is calculated by combining satisfaction and certification opinion of the recommenders on the platform properties.* $^{A-ind}o_{B,(c_i,p_j)}$ *represent the overall recommended opinion of a platform A on B regarding different properties. The overall opinion is computed from the individual opinions of A's recommenders using consensus ($\oplus$) operator. Each of the recommender opinions about the service platform B are discounted (using a discounting ($\otimes$) operator) based on A's opinion (positive or negative experience) on the recommender.*

$$^{A-ind}o_{B,(c_i,p_j)} = ({}^{A}o_{R_1} \otimes {}^{R_1}o_{B,(c_i,p_j)}) \oplus \ldots \ldots \oplus ({}^{A}o_{R_m} \otimes {}^{R_m}o_{B,(c_i,p_j)}) \quad (3)$$

DEFINITION 2.3. *(Derived Trust) Derived Trust is the belief that one entity holds on another entity for a given context, based on atomic trust relationships such as direct trust and indirect trust. Derived opinion for a property p_j of component c_i is calculated combining the direct and indirect opinions for that property (cf. Equation 4).*

$$^{A-der}o_{B,(c_i,p_j)} = {}^{A-dir}o_{B,(c_i,p_j)} \oplus {}^{A-ind}o_{B,(c_i,p_j)} \quad (4)$$

Trust comparison: Let o_1 and o_2 are two given opinions, we define an opinion comparison operator $\geq_o$, whereby $o_1 \geq_o o_2$ holds if $t_1 > t_2, c_1 > c_2$. In such cases, o_1 is greater than o_2.

2.3 Decision Model

The decision model is designed using the threshold-based mechanism. For instance, a user specify trust threshold values (τ) for each of the properties that service providers possess. In this case, if all the required properties are validated using *hard trust* and if the soft trust values regarding the required properties are equal or exceed the threshold values (τ), then a cloud provider is considered trustworthy.

3. EXPERIMENTAL EVALUATION

We have developed a prototype of our trust evaluation framework and conducted experiments in a practical cloud marketplace scenario. In such a scenario, a cloud consumer wants to select a trustworthy provider in a cloud marketplace for a storage service. The user considers a cloud storage provider 'trustworthy' if and only if the provider possesses the properties required by the consumer, the properties have been validated, and they satisfy the user defined thresholds. In the target scenario, the consumers relies on the *CSA STAR* which publishes the security-specific capabilities of the cloud providers.

For validating the property $IS-21$, the required 'ALOPA' policy (cf. Equation 1) is checked against the policy details associated with the certificate. If the property is validated, the next step is to check the *soft* trust status of the property. This is done using the *property satisfaction* module and related results are shown in the Table 2. For brevity, we limit our experiments with $IS-21$ property. In our initial experiments, we considered 4 types of trust relationships regarding the property $IS-21$ in the trust experience base (cf. Table 2). In Table 2, *U*, *CP*, *CA*, R_1 and R_2 are consumer's platform, cloud provider's platform, certification authority, and recommender 1 & 2 respectively. Based on the definitions (cf. Def. 2.1, 2.2 and 2.3), the derived trust value is calculated which does not satisfy the trust threshold (τ) defined by the consumer. Thus, the consumer might not be interested to provision a service from the cloud provider.

4. CONCLUSION

In evaluating trustworthiness of cloud providers, validation of their claimed capabilities (trust properties), plus consumers' satisfaction on the validation process play a critical role. In this vein, we have proposed a framework to verify cloud providers' security-specific properties by means of *soft* and *hard* trust mechanisms. Furthermore, a threshold-based decision model is introduced to check whether user-defined requirements in terms of trust-threshold (τ) are satisfied against the value which is derived using hard and soft trust mechanisms. We demonstrate applicability of our framework in the context of a competitive marketplace that takes the *CSA CAIQ* as a basis to evaluate trustworthiness of cloud providers.

5. REFERENCES

[1] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618–644, 2007.

[2] A. Nagarajan. *Techniques for Trust Enhanced Distributed Authorisation using Trusted Platforms.* PhD thesis, Macquarie Universtiy, 2010.

[3] S. Ries, S. M. Habib, M. Mühlhäuser, and V. Varadharajan. Certainlogic: A logic for modeling trust and uncertainty. Technical Report TUD-CS-2011-0104, Technische Universität Darmstadt, 2011.

[4] A.-R. Sadeghi and C. Stüble. Property-based attestation for computing platforms: caring about properties, not mechanisms. In *Proceedings of the NSPW '04*, pages 67–77. ACM, 2004.