SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 0000; **00**:1–18
DOI: 10.1002/sec

RESEARCH ARTICLE

Towards a Trust Management System for Cloud Computing Marketplaces: using CAIQ as a trust information source

Sheikh Mahbub Habib*, Sebastian Ries, Max Mühlhäuser, Prabhu Varikkattu

Technische Universität Darmstadt/CASED, Telecooperation Group, Darmstadt, Germany

ABSTRACT

Cloud computing enables IT related services in a more dynamic and scalable way than before – more cost-effective than before due to the economy of scale and of sharing resources. Usually, cloud providers describe their promised behaviour – regarding functional and non-functional aspects of the service provision – by way of Service Level Agreements (SLAs). For different providers offering similar functionality, SLAs are often insufficiently claimable and inconsistent with the aspects considered important by customers. Therefore, customers face problems identifying a trustworthy cloud provider based solely on its SLA. In order to support customers in reliably identifying trustworthy cloud providers, we propose a multi-faceted Trust Management (TM) system architecture for cloud computing marketplaces and related approaches. This system provides the means for identifying trustworthy cloud providers in terms of different attributes, e.g., compliance, data governance, information security. In this article, we present the first realization of our proposed TM system using the Consensus Assessment Initiative Questionnaire (CAIQ), initiated by the Cloud Security Alliance (CSA), as one of the sources of trust information. In particular, our proposed approach contributes to the challenge of extracting trust information from CAIQs completed by cloud providers. Finally, our implemented system and related approaches are experimented using real datasets.

KEYWORDS

Cloud computing, Trust models, Reputation, Trust Management, Architecture, CAIQ, Self-Assessment

***Correspondence**

Corresponding author's address. Email: sheikh.habib@cased.de

Received . . .

1. INTRODUCTION

Cloud computing offers dynamic, scalable, shared resources (e.g., computing power, storage, software) over the internet from remote data centres to users (e.g., business organizations, government authorities, individuals). The highly distributed and non-transparent nature of cloud computing represents a considerable obstacle for the acceptance and market success of cloud services. Potential customers (or consumers) of these services often feel that they lose the control over their data and are not sure whether they can trust the cloud providers in offering dependable services. A recent survey [1], conducted among more than 3000 cloud consumers from 6 countries, shows that 84% of the consumers are concerned about their data storage location and 88% of the consumers worry about who has access to their data.

Consumer concerns can be mitigated by using preventive measures for privacy (e.g., demonstrating compliance standards) and security (e.g., secure hypervisors, TPM based servers). Although cloud providers demonstrate their preventive measures by including related descriptions in the *SLA*s, compensations and related clauses for *SLA* violations are not convincing enough for the consumers, e.g., service credits [2] merely compensate the business losses due to *SLA* violations. In particular, *SLA*s with vague clauses and unclear technical specifications lead the consumers to a decision dilemma when considering them as the only basis to identify trustworthy providers.

As the business market is growing rapidly with new providers entering the market, cloud

Prepared using secauth.cls [Version: 2010/06/28 v2.00]

providers will increasingly compete for customers by providing services with similar functionality. However, there can be huge differences regarding the provided quality level of those services as well as the competencies and capabilities of the service providers. It becomes more difficult to assess when intermediary parties such as cloud brokers and resellers offer add-on services on behalf of cloud providers, but promise the same level of competencies and capabilities. Such a diverse and competitive cloud marketplace [3] needs means to reliably assess the dependability (or trustworthiness) of the service providers offering services of good quality.

Trust and reputation (*TR*) systems [4] are successfully utilized in numerous electronic marketplaces to support users in identifying dependable and trustworthy providers, e.g., on eBay, Amazon, and app markets for mobile applications. Similar approaches are needed to support customers in selecting trustworthy service providers in cloud marketplaces. Existing *TR* systems rely on customer feedback without considering other sources and roots of information (e.g., property certificates, compliance with audit standards, provider statements). Moreover, there are additional parameters [5] that are required to support the customers in selecting providers in cloud marketplaces. Therefore, *TR* systems have to evolve into Trust Management (*TM*) systems – as defined in [6] – to support the customers in making transparent assessments before selecting dependable and trustworthy cloud providers.

Contributions

This paper provides the first realization of our proposed *TM* system [7] for cloud computing marketplaces. This system aims to reflect the multi-faceted nature of trust assessment by considering multiple attributes, sources, and roots of trust. It also aims to support customers in identifying trustworthy services providers, as well as service providers in standing out. In this paper, we implement the first instantiation of the *TM* system using the *CAIQ* (cf. Section 2) as one of the trust information sources. We contribute to the approach by extracting trust information from *CAIQ*s completed by cloud providers. We also contribute to the implementation of the required components of the proposed *TM* system that is used to assess the trustworthiness of cloud providers based on the extracted trust information from the *CAIQ*. Our implementation includes an intuitive graphical interface for the cloud providers, allowing for convenient and faster input than the current approach (using excel sheet) for filling out the *CAIQ*. The graphical interface also allows consumers to navigate through the different domains and check the detailed assessment results under each domain of the *CAIQ*. Finally, our implemented instantiation of the *TM* system is validated by experimental evaluation based on the completed *CAIQ*s stored in the public registry (i.e., *CSA STAR* [8]).

Contents

The rest of the paper is organized as follows: Section 2 presents the related work. Section 3 provides a list of required attributes and properties of TM systems for cloud computing marketplaces. Section 4 propose the required solutions for trust management. Section 5 discusses the technical details of the proposed *TM* system based on the *CSA CAIQ* framework and the system is validated by experimental evaluation in Section 6. Finally, in Section 7, we present our concluding remarks.

2. RELATED WORK

We classify the current trends and existing approaches in the field of trust establishment into two categories: 1) applied technologies and 2) research trends. The third section discusses research trends of TM system, which is considered as a driving element in the field of trust establishment.

2.1. Applied technologies in trust establishment

In this section, technologies that are currently applied to establish trust on the cloud providers are presented. These technologies show that various approaches are available in cloud marketplaces which can be considered for establishing trust on cloud providers.

SLAs: In practice, one way to establish trust for cloud providers is the fulfilment of *SLA*s. *SLA* validation [9] and monitoring [10] schemes are used to quantify what exactly a cloud provider is offering and which assurances are actually met. In cloud computing environments, customers are responsible for monitoring *SLA* violations and informing the providers for compensation. The compensation clauses in *SLA*s are written by the cloud providers in such a way so that the customers merely gets the advantage of applying for compensation (e.g., service credits) due to *SLA* violation. This problem arises from not having standardized *SLA*s for stakeholders in the cloud computing marketplaces. Although, the problem is addressed by an industry driven initiative [11] for establishing standardized *SLA*s, this initiative is far from completion and implementation in practice.

Security Comm. Networks 0000; **00**:1–18 © 0000 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

Auditing: Cloud providers use different audit standards (e.g., SAS 70 II, FISMA, ISO 27001) to reassure users about their offered services and platforms. For example, Google lists SAS 70 II and FISMA certification to reassure users about the security and privacy measures taken for Google Apps. The audit SAS 70 II covers only the operational performance (e.g., policies and procedures inside datacenters) and relies on a highly specific set of goals and standards. They, however, are not sufficient in alleviating the users' security concerns [12] and most cloud providers are not willing to share audit reports, which also leads to a lack of transparency.

Ratings & Measurements: Recently, a cloud marketplace* was launched to support consumers in identifying dependable cloud providers. Cloud providers are rated based on a questionnaire that needs to be filled in by current cloud consumers. In the future, CloudCommons aims to combine consumer feedback with technical measurements for assessing and comparing service-specific competencies and capabilities of cloud providers. Furthermore, there is a new commercial cloud marketplace, SpotCloud†, that provides a platform where cloud consumers can choose among potential providers in terms of cost, quality, and location. In this platform, the cloud providers' ratings are given in an Amazon-like 'star' interface with no documentation on how the ratings are computed.

Self-assessment Questionnaires: The Cloud Security Alliance (*CSA*) proposed a detailed questionnaire for providing security control transparency – called the Consensus Assessment Initiative Questionnaire (*CAIQ*) [13]. This questionnaire provides means for assessing the capabilities and competencies of cloud providers in terms of different attributes (e.g., compliance, information security, governance). However, the metrics working group has not yet provided any proposals for a metric yet (in contrast to the other working groups of the *CSA*).

2.2. Research trends in trust establishment

This section presents research-driven state-of-the-art approaches regarding trust establishment in various service environments. We classify the approaches into two schools of thought [14]: 1) *TR* models, which are referred to as "soft trust" mechanisms, and 2) Trusted computing based approaches, which can be refereed to as "hard trust" mechanisms. On the one hand, "hard trust" (e.g., trusted computing) approaches consider the service platforms 'trusted' if the existence of necessary security primitives is 'provable'. On the other hand, 'soft trust' involves aspects such as intrinsic human emotions, perceptions, interaction experiences and assumes that no 'hard trust' mechanisms are perfect, no matter how rigid the design procedures are [15]. A recent survey [15] shows that both schools of thought are important to consider when establishing trust on cloud providers in marketplaces.

Trust and Reputation models

TR models have been proven useful for decision making in numerous service environments (e.g., e-commerce, p2p networks, product reviews) [4, 16]. The concepts have also been adapted in grid computing [17, 18], cloud computing environments [19, 20], and selecting web services [21]. The approaches for *TR*-based decision making in different environments usually do not take multiple attributes (e.g., security, compliance, data governance) into account. The approaches proposed by Irfan et al. [17], Wang et al. [21], and Pawar et al. [20] for grid computing, web service, and cloud computing environments respectively are the exceptions in the context of trust evaluation based on multiple attributes.

Irfan et al. proposed a trust model considering certificates (i.e., PKI-based) and reputation-based trust system as a part of an *SLA* validation framework. Wang et al. proposed a trust model that takes multiple factors such as reputation, trustworthiness, and risk into account for evaluating web services. These approaches consider *SLA* validation as the main factor for establishing trust on the grid service and web service providers. *SLA* validation frameworks can help to identify violations of service-specific performance parameters agreed between a consumer and a cloud provider.

The *SLA* compliance issue has recently been considered in a trust model [20] proposed in the context of a cloud-specific project [22]. The objective of the proposed model is to evaluate trustworthiness of cloud infrastructure providers based on the compliance of performance parameters agreed between providers and consumers via *SLA*s. In contrast to [17, 21], the trust model in [20] considers two additional parameters: i) satisfaction ratings, e.g., when a consumer provide a rating for the provider and ii) consumer behaviour, e.g., if a consumer opted to use a service from a cloud provider independent of rating that it has provided to the provider. Considering consumers' satisfaction ratings together with expert assessments, self-assessments and certificate-based assessment are already shown

*http://beta-www.cloudcommons.com/web/cc/about-smi

†http://www.spotcloud.com/

essential and practical to evaluate trustworthiness of cloud providers in cloud marketplaces [7]. In contrast to approaches [17, 21, 20], the approach presented in this paper considers *CSA CAIQ* assessment information (combining information from multiple attributes) to manage trust. Moreover, our approach focus on heterogeneity of service-specific attributes whereas the approaches in [21, 20] focus on multiple factors or parameters to evaluate trustworthiness of service providers.

Though the approaches are slightly different, we argue that our approach and the approach in [20] are cross-complementary. The additional parameter, *consumer behaviour*, can be complimentary to our approach in the context of user-centric *CAIQ* assessment, whereas our approach can be complementary to [20] for evaluating trustworthiness of cloud providers before the *SLA* negotiation phase, i.e., pre-(service deployment phase).

Trust and Uncertainty: Modelling uncertainty is especially important in the field of trust and reputation. There are a number of approaches modelling the (un-)certainty of a trust value, well-known approaches are given in [18, 23, 24, 25]. The challenge of these approaches is to find good models for deriving trust from direct user experiences, recommendations from third parties, and sometimes additional information, e.g., social relationships. In particular, those models aim to provide robustness against attacks, e.g., misleading recommendations, re-entry, and sybil attacks.

Trust Operators: For trust calculation, the above mentioned trust models usually provide operators for combining evidence from different sources about the same target (namely 'consensus') and for weighting recommendations based on the trustworthiness of the source (namely 'discounting'). These operators are important when deriving trust based on direct experience and recommendations. In cloud computing environments, services are hosted in complex distributed systems. In order to assess trustworthiness of a complex distributed system based on knowledge about the trustworthiness of it's constituent components and subsystems regarding different attributes (e.g., security, performance, customer support), we need additional operators for the evaluation of propositional logic terms. These operators are proposed in [26, 27, 28].

Trusted Computing

Apart from the field of trust and reputation models, there are a number of approaches from the field of trusted computing designed to ensure trustworthy cloud infrastructure. Krautheim et al. proposed a Private Virtual Infrastructure (*PVI*), which is a security architecture for cloud computing and uses a trust model to share the responsibility of security between the service provider and client [29]. Schiffman et al. proposed a hardware-based attestation mechanism to provide assurance regarding data processing protection in the cloud for customers [30]. There are further approaches such as property-based TPM virtualization [31], which can be used in the cloud scenario to assure users about the fulfilment of security properties in cloud platforms using attestation concepts. However, in general, attestation concepts based on trusted computing, e.g., [32], focus on the evaluation of single platforms, but, not on compositions. Moreover, several ambiguities arise due to the nature of property-based attestation mechanism which are addressed in dynamic trust models (e.g., [33]).

2.3. Research trends of TM systems

The TM systems developed in the last century, e.g., KeyNote [34], REFEREE [35], IBM Role-based Access Control Model [36], assumed trust relationships as *monotonic* and do not manage trust considering the notion of learning from the available information. These systems are useful for access control decisions, where a service provider determines what a consumer is allowed to do, but, not in a scenario where trust is a negotiation process, e.g., cloud computing. To overcome these problems in existing *TM*s, Grandison et al. [37] proposed a policy-based *TM* framework that includes notation for specifying trust and reputation concepts as well as software tools for analysing and monitoring trust specifications. The framework does not address the concept of uncertainty as a part of trust specification language for specifying trust relationships between a trustor (consumer) and a trustee (provider). Modelling and representing uncertainty is important when trust is assessed between a trustor and a trustee based on information that is incomplete or insufficient or derived from unreliable sources. In our proposed *TM* system, the underlying trust metric considers uncertainty of information in assessing trustworthiness and represent trust under uncertainty with an intuitive graphical interface. The proposed *TM* system is also able to combine (or aggregate) multi-attribute-based trust derived from multiple sources and roots under uncertainty.

Our proposed *TM* system aims to aggregate and manage trust-related information from different sources, e.g., user ratings, provider statements, measurements, property certificates. These pieces of information are relevant (and often available) in assessing the trustworthiness (or dependability) of a cloud provider. The approaches discussed in Section 2.1 and 2.2 are considered complementary for managing trust in cloud marketplaces. However,

Security Comm. Networks 0000; **00**:1–18 © 0000 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

the existing approaches are still lacking an unified approach (i.e., a multi-faceted *TM* system) to identify the most dependable cloud provider in the marketplaces. This paper proposed the first instantiation of such a *TM* system by implementing the Cloud Control Assessment (*CCA*) tool based on the *CSA CAIQ*. This tool aims to deliver trustworthy assessment of the completed *CAIQ* and provides a trust score to distinguish the level of capabilities the cloud providers possess.

3. TRUST MANAGEMENT SYSTEMS FOR CLOUD COMPUTING MARKETPLACES

According to recent literature [6], *TM* systems should allow relying parties/entities to reliably represent their capabilities and competencies of the underlying systems in terms of relevant attributes. Such systems should also allow reliant parties to make assessments and decisions regarding the dependability of potential transactions based on the available pieces of evidence. For the latter part, representational and computational trust models provide mean for assessing the trustworthiness of relying parties based on observations and evidence. In cloud computing, evidence regarding different attributes are often available from multiple sources and roots. These multi-faceted requirements need to be taken into account when selecting trustworthy cloud providers. Moreover, cloud providers should also be able to present their system/service capabilities regarding different attributes (e.g., security, compliance, performance) through a *TM* system.

3.1. Attributes for Trust Assessment

During the trust assessment phase, multiple attributes need to be taken into account in order to ensure reliable decision making in any application scenario. This is particularly true for cloud computing environments, where multiple attributes (e.g., security, compliance, availability) are important for reliably determining the quality level of cloud providers. A set of such attributes is given in a recent publication [5] and in the *CAIQ*. We aim to assess the trustworthiness of a cloud provider with respect to these attributes.

In [5], these attributes (e.g., security measures, compliance, customer support) are mentioned without giving detailed definitions. In the *CAIQ*, *CSA* has documented the attributes with detailed definitions. Additionally, the *CAIQ* framework provide means for cloud providers to publish the capabilities regarding these attributes according to the service models (e.g., SaaS, IaaS, PaaS) they follow.

3.2. Properties of TM Systems

TM systems require specific properties to incorporate those attributes for establishing trust on service providers in cloud marketplaces.

Multi-faceted Trust Computation

The computation of trust should consider the attributes mentioned in [38] and [5], which refer to the competencies and capabilities of a service provider in certain aspects. For example, service providers can be assessed based on security measures, compliance with audit standards, performance of a specific service, and customer support facilities. Considering these attributes in trust computation introduce further challenges, which are as follows:

- Multiple attributes: *TM* systems should possess mechanisms to aggregate multiple attributes (cf. Section 3.1) irrespective of the types of evaluation methods followed to evaluate the attributes (e.g., subjective evaluation of attributes– recommendations or objective evaluation of attributes– real-time measurements).
- Multiple sources and roots: The degree of fulfilment of the attributes can be derived best when considering information from all relevant sources. This often requires considering multiple sources of information in contrast to relying on a single source of information. For example, information about performance attribute may be provided by two sources– providers and third-party. Moreover, multiple sources can provide quantitative and qualitative information that need to be factored into trust establishment process and the required information can be derived from multiple roots. For example, information about security measures can be based on two sources with different evaluation methods– TPM-based remote attestation and customer feedback. Information collected from multiple roots and sources might be conflicting as well. *TM* systems should be able to aggregate this information derived from different roots and sources.

Trust Customization

It is important to consider the subjective interests and requirements of the customers when assessing the trustworthiness of a service provider. Based on the individual interests and requirements, each customer will get a local (subjective) or customized

trust value of a service provider. Subjective trust values provide means for considering the preference of each customer in detail. Customers may give priority to specific sources and roots of trust information and to specific attributes based on their interests and requirements. *TM* systems should have specific mechanisms to deliver customized trust values to the users.

Trust Evaluation

In complex distributed environments, it is important to evaluate the trustworthiness of a cloud provider considering the knowledge on the architecture of the systems and the trustworthiness of its components and subsystems [39, 28].

Trust Representation

The derived trust values of the cloud providers must be transparent to and comprehensible enough for the customers, so that they can easily and confidently make a trust-based decision. To make the trust values transparent and comprehensible, customers need to be supplied with an intuitive representation of trust along with enough information regarding the relevant attributes.

Attack Resistance

As soon as the influence of *TM* systems on the decision of customers increases, the interests in manipulating the trust scores of the cloud providers will grow accordingly, as already seen in other service environments [40]. A number of different attacks (e.g., playbooks, proliferation attacks, reputation lag attacks, false praise or accusation (collusion), whitewashing (re-entry), sybil attacks) against trust and reputation systems have been discussed [40]. These types of attacks will also be of concern when designing trust management systems for cloud computing marketplaces. Thus, attack resiliency should be considered during the development phase of these systems.

4. PROPOSED SOLUTIONS FOR TRUST MANAGEMENT

This section discusses the solutions that are essential in developing a *TM* system for cloud marketplaces. An overview of the *TM* system architecture and description of its internal components are also provided where the proposed solutions are applied.

4.1. Modelling Trustworthiness in Cloud Computing

The trustworthiness of a cloud provider depends on the expected behaviour of the services and underlying systems with respect to specific attributes (cf. section 3.1). Therefore, modelling the trustworthiness of a cloud provider requires statements on the expected behaviour of the offered services or systems. In the following, we give a few examples that show how those statements can be given in the form of propositions:

- Security: "Provider B keeps my data confidential."
- Latency: "System A responds within $100ms$."
- Availability: "Cloud A provides 99.99% uptime in a year."
- Customer support: "Cloud B's customer support is competent."

In these examples, we see that the propositions refer to different attributes. Using the operators (AND, OR), those propositions become the basis for combined statements in the form of Propositional Logic Terms (PLTs).

When assessing whether or not a cloud provider fulfils a particular attribute or a set of attributes, one usually encounters problems such as incomplete information, insufficient knowledge about the architecture of the system or service, or unreliable sources. Therefore, when modelling trust, one has to consider that trust relevant information as well as a trust value derived from this information are subject to uncertainty. Thus, we propose to model trust as a subjective probability, which follows the definition of trust provided in [41].

4.2. Trust Metric: Representation and Computation

Following the idea of modelling trust as a subjective probability, we use *CertainTrust* [42] and *CertainLogic* [43] as the basis for a trust metric in our planned instantiation of the architecture (cf. Section 4.3). In the following, we provide a brief introduction to the trust representation and computation that we need to support.

Representation

In CertainTrust (for the full details, cf. [42]), one models the trustworthiness of an entity based on opinions that express one's belief that a certain proposition (or a combination of propositions) is true. For example, one could consider an entity to be trustworthy if it is expected to deliver a certain service with a pre-agreed quality (or with a pre-agreed quality and in time). Each opinion is modelled as a triple of values, $o = (t, c, f) \in \{[0, 1] \times [0, 1] \times$

Security Comm. Networks 0000; **00**:1–18 © 0000 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

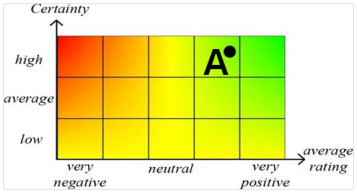

Figure 1. CertainTrust: Graphical Interface

$[0, 1]\}$ where t denotes the average rating, c the certainty associated with the average rating, and f denotes the initial expectation assigned to the truth of the statement.

As shown in our previous publications [42, 43], the assessment of the parameters can be based on evidence from past experience, derived from opinions in subjective logic [26], or derived from a Bayesian probability distribution. The parameters can also be derived from expert assessments or CSA CAIQ assessment (cf. Section 5.1). Beyond providing means for explicitly modelling uncertainty, the representation provides a graphical interface (HTI– Human Trust Interface), which supports intuitive access for users (see Fig. 1).

Each opinion $o = (t, c, f)$ is also associated with a expectation value, i.e., a point estimate, taking into account the initial expectation f, the average rating t, and the certainty c as follows:

$$E(t, c, f) = t * c + (1 - c) * f \tag{1}$$

Thus, the expectation value shifts from the initial expectation value f to the average rating t with increasing certainty c.

Computation

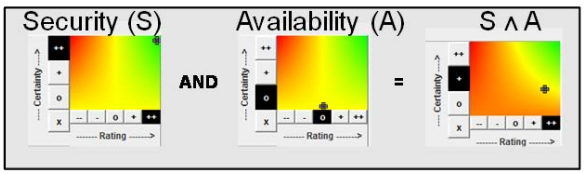

Figure 2. Example: Computation of Trust – AND

The evaluation of the trustworthiness of an entity usually requires operators for combining opinions from multiple sources. Hereby, *CertainTrust* and *CertainLogic* provide a set of operators. The operators for deriving trust from recommendations are called *consensus* and *discounting* (cf. [25, 44]). The consensus operator provides means for aggregating opinions on the same statement from different (independent) sources; and the discounting operator provides means for weighting those opinions based on the trustworthiness of those sources. This aggregation can also be optimized to counteract Sybil attacks [44].

Furthermore, the operators for AND, OR, and NOT proposed in [28, 43] allow the evaluation of PLTs under uncertainty. In particular, those operators provide means for evaluating composite independent propositions by combining opinions associated with the propositions. In this paper, we use the AND (cf. Table 2) operator for aggregating opinions derived from the CAIQ (cf. Section 5.1). Figure 2 shows an example to combine an opinion about the *security* attribute of a system with the opinion about the *availability* attribute of the same system. We assume that there are mechanisms [39, 43] to evaluate such attributes of a system or a service and represent the evaluation by means of opinions [43]. Particularly, those operators have been shown equivalent to subjective logic and compatible with the standard probabilistic approach [43].

When the independence cannot be assumed among the propositions, the above mentioned operators are no longer sufficient. For instance, this is the case when one has to combine two opinions, based on same observation methods by different sources, associated with a proposition or propositions (i.e., PLTs). Thus, an additional operator (i.e., FUSION) is needed. For brevity, the definition and applicability of this operator for assessing trust in a cloud marketplace scenario is omitted but can be found in the technical report [45].

4.3. TM System Architecture

Having introduced the necessary tools for assessing, representing, and computing trust, in this section, we propose a novel architecture (cf. Figure 3) of a *TM* system for cloud computing marketplaces. A brief description of the system's internal components are as follows.

Registration Manager (RM): Cloud providers register through the *RM* to be able to act as sellers in a cloud marketplace. They have to provide system/service specifications related to the service delivery models (e.g., SaaS, PaaS, IaaS) they offer and fill in the *CAIQ* as a part of the cloud marketplace policy. The RM forwards the answers of the questionnaire and system/service description to the *CAIQ* engine and *TI* (Trust Information) respectively for further processing.

Consensus Assessments Initiative Questionnaire (CAIQ) Engine: The *CAIQ* engine allows cloud providers to fill in the questionnaire by providing an intuitive graphical interface through the *RM*. The questionnaire helps cloud providers to represent their competencies to the potential users with respect to different attributes. The questions

Table I. Definition of the AND operator

AND	$c_{A\wedge B} = c_A + c_B - c_A c_B - \frac{(1-c_A)\,c_B\,(1-f_A)\,t_B + c_A\,(1-c_B)\,(1-f_B)\,t_A}{1-f_A f_B}$ $t_{A\wedge B} = \begin{cases} \frac{1}{c_{A\wedge B}} \left(c_A c_B t_A t_B + \frac{c_A(1-c_B)(1-f_A)f_B t_A + (1-c_A)c_B f_A (1-f_B) t_B}{1-f_A f_B} \right) & \text{if } c_{A\wedge B} \neq 0, \\ 0 & \text{else .} \end{cases}$ $f_{A\wedge B} = f_A f_B$

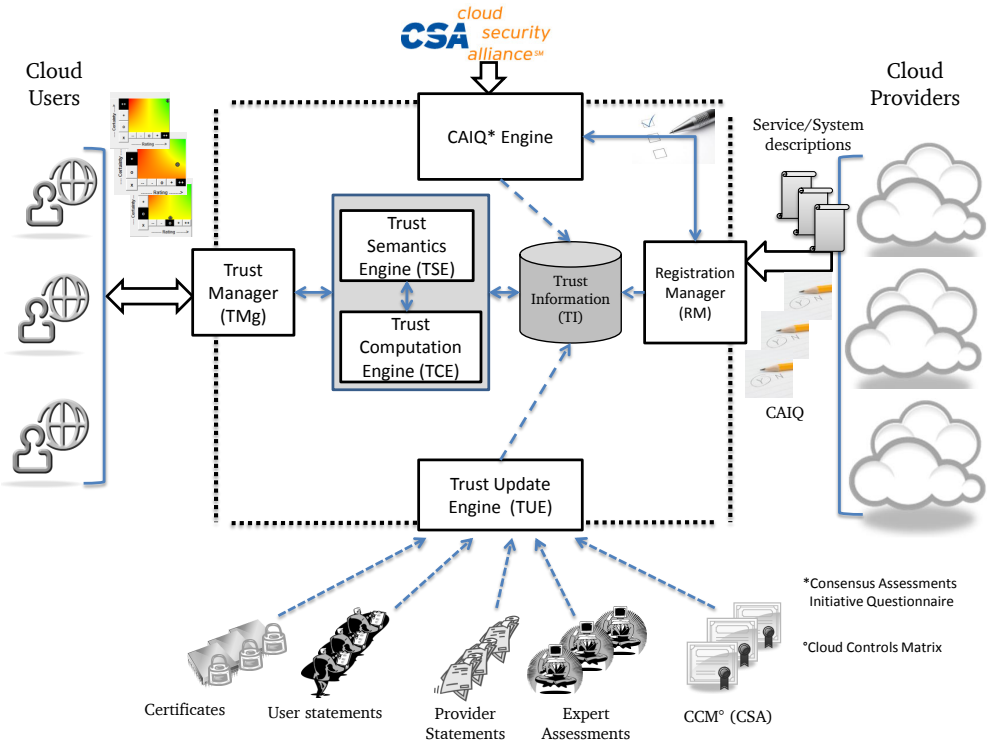

Figure 3. Architecture Overview

are designed to be answered in 'yes' or 'no'. All the answers are stored in the *TI* for further processing. In order to utilize the completed *CAIQ*s in trust assessment process, we first need to assess the assertions and then, convert the assessment results into the CertainTrust opinion representation. The *CAIQ*s assessment is discussed in Section 5.1. Experimental evaluation is performed using the completed *CAIQ*s, published in the *CSA STAR*, in Section 6.

Trust Manager (TMg): The *TMg* allows cloud consumers to specify their requirements before assessing the trustworthiness of cloud providers. It provides a front end to the users for specifying their requirements. Based on the requirements, the *TMg* provides the trust score of cloud providers by using the Trust Semantic Engine (*TSE*) and Trust Computation Engine (*TCE*). By default, users receive the trust value of a cloud provider based on their completed *CAIQ* and the assessment of their underlying services/systems. Otherwise, users can specify their own preferences (e.g., security and performance are preferred over customer support), according to their business policy and requirements in order to get a customized trust value of the cloud providers. Users may also choose the sources and roots of information that need to be taken into account when computing the trust value of cloud providers. The *TMg* should also be able to provide trust value for every single attribute considered for the calculation of overall trust value by means of opinion $((t, c, f))$ representation and graphical interface (i.e., *HTI*). In the *TM* system architecture (cf. Fig. 3), the *TMg* is tightly coupled with the *TSE* and *TCE* to offer the above mentioned features to cloud consumers.

Trust Semantics Engine (TSE): The *TSE* is able to model which configuration of *PLT*s are considered by the consumers to be the expected (trustworthy) behaviour of a cloud provider. A default configuration of *PLT*s should be based on the CAIQ answers stored in the repository (*TI*). The *TSE* should be able to convert all trust-relevant information into *PLT*s. For deriving *PLT*s from system/service specifications, the *TSE* integrates the formal framework proposed in [39]. *PLT*s can also be derived from the *CAIQ*. The approach for deriving the *PLT*s is discussed in Section 5.1.

Moreover, this engine supports users in expressing their preferred attributes as well as the sources and roots of the information that they choose to be taken into account. The *TSE* should be able to customize the configuration of *PLT*s in order to reflect the users' preference. Customized *PLT*s are sent to the *TCE* for the final evaluation.

Trust Computation Engine (TCE): The *TCE* consist of operations related to the operators (AND, OR, NOT, $FUSION$, $CONSENSUS$, $DISCOUNTING$), used in *PLT*s to compute the corresponding trust values. The *TCE* is tightly coupled with the *TSE* in evaluating the *PLT*s and computing corresponding trust values. The trust values are archived in the *TI* repository after computation.

Trust Update Engine (TUE): The *TUE* allows for the collection of opinions from various sources regarding the trustworthiness of cloud providers. The opinions collected here should be filtered appropriately so that users may use opinions that are valid according to their requirements. For example, spam filtering should be used to eliminate junk or useless information stored in the *TI* repository. Moreover, the sources should be authorised before they are able to provide opinions. The authorisation process should verify the identity of a source as well as trustworthiness of it's underlying platforms. The filtering of opinions and authorisation of sources are extremely important to ensure the reliability of trust assessment process inside the *TM* system.

Currently, we have implemented the first instantiation of the system based on the *CAIQ* assessment for supporting cloud consumers in identifying the trustworthy providers. In the next subsequent sections, we describe our approach to assess the *CAIQ*, discuss the implementation of our system using the *CAIQ* assessment and evaluate the system under different cases.

5. CAIQ BASED TRUST MANAGEMENT

The *CAIQ* includes 11 domains (e.g., Compliance (CO), Data Governance (DG)) which are aligned with the *CSA* guidelines [46] for moving IT resources to the cloud. Each of the domains consists of several controls that resemble specific requirements to comply with the corresponding domain. There are, in total, 98 controls under 11 domains in the *CAIQ* framework. Each of those controls has one or more questions that are designed to query about cloud providers' capabilities and competencies regarding different attributes (e.g., audit planning, security policies, risk assessments). Through quantitative assessment of cloud providers' assertions under each control and domain support consumers to identify the dependable (or trustworthy) providers in the cloud marketplaces.

5.1. CAIQ Assessment

Our approach for the *CAIQ* assessment is based on the following assumptions. We assume that cloud providers provide one set of valid answers to the *CAIQ* for each of the services they offer and the answers are stored in the *TI* (similar to the *CSA STAR*). The *CSA* is responsible for checking the authenticity and the basic accuracy of the answered questionnaires [47].

We propose a two-step approach for assessing the *CAIQ*. The approach is detailed as follows:

1. Firstly, the *TSE* configures the *PLT*s based on the *CAIQ* domains. It means that the *PLT* configuration contains 11 operands (i.e., domains) combined with 10 AND ($\wedge$) operators. Conceptually, *PLT* configuration appears as follows:
   $CO \wedge DG \wedge FS \wedge HR \wedge IS \wedge LG \wedge OP \wedge RI \wedge RM \wedge RS \wedge SA$
2. Secondly, for evaluating the *PLT*s, the associated opinion (t, c, f) for each of the domains is required. The opinions are from the cloud providers based on the self-assessment of their security controls according to the guidance (i.e., *CAIQ*) of *CSA*. We model the answers (i.e., 'yes' or 'no') in the evidence space and use the mapping [48] to derive opinions for every domain under the *CAIQ*. We adopted the mapping between evidence space and CertainTrust opinion representation from [48] and adjusted it according to the context of *CAIQ* assessment. The mapping is as follows:

$$t = \begin{cases} 0 & \text{if } r+s=0 \ , \\ \frac{r}{r+s} & \text{else} \ . \end{cases}$$
$$c = \frac{N.(r+s)}{2.(N-(r+s))+N.(r+s)} \quad (2)$$
$$f = 0.99$$

Let us define the variables used in the above mapping:

- Average rating, t, is calculated based on the number of positive assertions (i.e., r=number of 'yes' assertions) and the number of negative assertions (s= number of 'no' assertions) under each domain. If there are no questions answered with 'yes' or 'no', t is 0. Otherwise, t is the relative frequency of positive assertions.
- Certainty, c, is calculated based on the total number of questions, N and the number of positive and negative assertions under each domain. The c is 1 when all questions under each domain (e.g., Compliance (CO)) are answered "positive" or "negative" assertions and 0 if none are answered.
  The definition of N is adjusted according to the context of *CAIQ* assessment. The total number of questions, N, not only consider positive and negative assertions but also the unanswered questions under each domain. We assume that the unanswered questions can be of two types: 1) Questions that cloud providers left out for 'unknown' reasons and 2) Questions that are not in the scope of services (i.e., Not Applicable) offered by the cloud providers. In order to deal with such type of questions, we define the N as following:
  - For type (1), the 'unknown' (in short 'u') marked answer(s) to the corresponding question(s) under each domain are taken into account. That means, $N = r + s + u$.
  - For type (2), the 'Not Applicable' (in short, 'NA') marked answers under each domain are not included in the calculation of N. That means, $N = (r + s + u) - NA$
- Initial expectation, f, is set as high for every single domain assuming that the cloud provider release their control information regarding different domains via STAR repository truthfully and accuracy of those information are validated using CSA's Cloud Control Matrix (CCM) [38] and CloudAudit [49] framework.

Example

In order to provide an in-depth understanding of our approach, we illustrate our approach by means of a quantitative example. Let us apply our approach (cf. Section 5.1) for assessing a completed *CAIQ* questionnaire. To keep it simple, we apply the assessment on two domains, *Compliance (CO)* and *Information Security (IS)*.

According to the latest version of *CAIQ* [13], *CO* has 16 questions divided under six different controls. Assume that, cloud provider 'X' has answered the *CO* domain which are as follows:

- Number of *positive* assertions, $r = 11$
- Number of *negative* assertions, $s = 2$
- Number of *unknown* assertions, $u = 2$
- Number of *Not Applicable* assertions, $NA = 1$
- Number of questions, $N = 15$, due to 1 NA question

Now, using the Equation 2, the resulting opinion (t, c, f) is as follows:

$$t = \frac{11}{(11+2)} = 0.8462$$
$$c = \frac{15.(11+2)}{2.(15-(11+2))+15.(11+2)} \quad (3)$$
$$= 0.9798$$
$$f = 0.99$$

The corresponding opinion, (t, c, f) for *IS* domain can be derived from the given answers by the cloud provider 'X' following the same approach as *CO* domain. According to the cloud provider's given answers, the resulting opinion for the *IS* domain is, $(t, c, f) = (1, 1, 0.99)$. It means that all the questions are answered with positive assertions.

Following the first step of our approach, we can easily construct the *PLT*s ($CO \wedge IS$) as described in Section 4.2. Now the resulting opinions derived from the given answers provide a basis for evaluating the *PLT*s. Cloud provider's opinion on Compliance (*CO*) and Information Security (*IS*) are combined using the *AND* operator (cf. Table I). The final opinion on *PLT*s (i.e., ($CO \wedge IS$)) means that the cloud provider 'X' expected to be trustworthy (or dependable) in terms of *Compliance* and *Information Security* controls.

In the next section, we discuss the implementation of the assessment tool which is used for evaluating the *CAIQ*.

5.2. Implementation

The Cloud Control Assessment (*CCA*) (i.e., instance of the TM system) tool is developed using Java to evaluate the *CAIQ*, answered by the cloud providers. It has two special features:

Security Comm. Networks 0000; **00**:1–18 © 0000 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

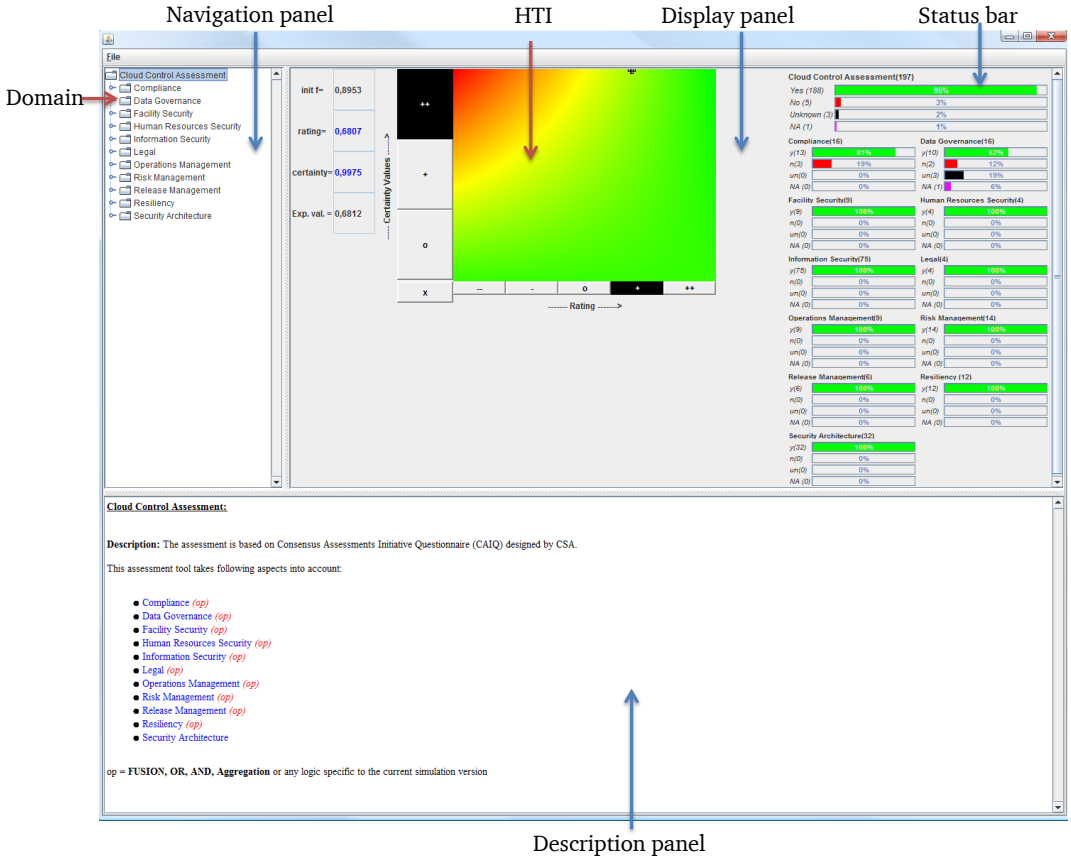

Figure 4. Visualization of CCA tool: Domain

- The tool provides a intuitive graphical interface for answering questions and supports interactive visualization of the assessment.
- The tool also allows loading of a completed questionnaire from the *CSA STAR*. For evaluating the questionnaire, *CCA* includes the features of the TSE (configuring the *PLT*s) and *TCE* (definition of the operators (e.g., *AND*)) component as described in Section 4.3 to factor the *CAIQ* assessment into a trust score (i.e., expectation value, E) as well as an opinion representation. This assessment tool is the first realization of the *TM* system (cf. Section 4.3) for cloud computing marketplaces.

The graphical interface (cf. Figure 4 and Figure 5) of the tool has three panels and a menu bar:

1. Navigation Panel: This panel has tree-like structure to display and navigate the users to the *CAIQ* domains, their controls and control-specific questions.
2. Description and Input Panel: This panel provides a description of each of the domains (e.g., Compliance) when selected in the navigation panel. Moreover, the control questions are displayed with their corresponding options (i.e., 'yes', 'no', 'unknown' and 'NA') when a particular control (e.g., Independent Audits) under a domain is selected in the navigation panel. These four options are given as radio buttons to allow faster input from the users (i.e., cloud providers) compared to the current approach (manual input in a Excel sheet) designed by *CSA*.
3. Display Panel: This panel displays results and progress or status by means of a graphical interface (i.e., CertainTrust *HTI*) and status bars, respectively. The *HTI* shows the opinion (t, c, f) and the corresponding expectation value (E) in a special panel on its left. The status bars are introduced for monitoring the progress of the assessment interactively. On the one hand, it provides the cloud consumers a summary of the assessment based on the assertions provided by the cloud providers. On the other hand, cloud providers are able to monitor their progress

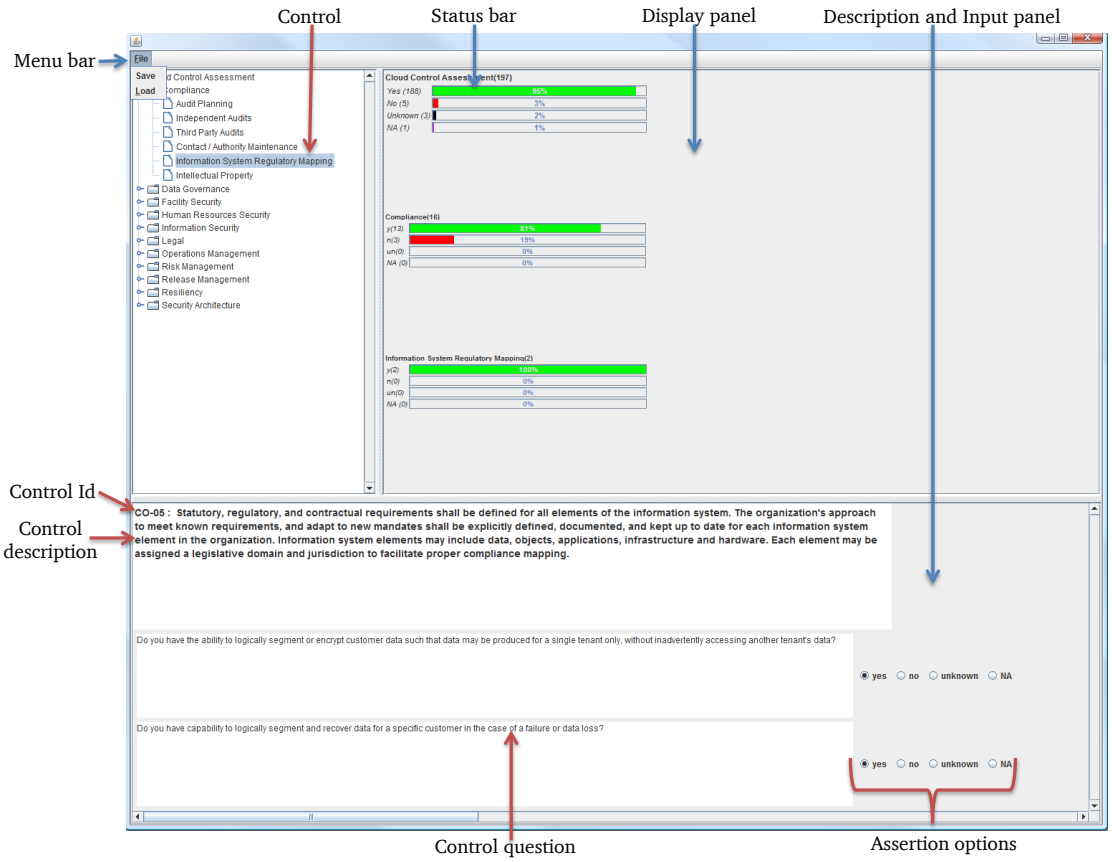

Figure 5. Visualization of CCA tool: Control Question

and corresponding opinion, represented in numerical and graphical interface based on given assertions.

4. Menu bar: The bar includes 'Save' and 'Load' functions which are extremely important for such a lengthy questionnaire (197 questions). To respond to 197 questions under 11 domains is quite a cumbersome task. Keeping that problem in mind, we developed the tool in such a way so that the cloud providers can *save* their undone tasks while filling the questionnaire and *load* them aat a more convenient time. The load function is also essential for our evaluation phase. We use this function to load the answers given by the cloud providers in the *STAR* repository.

6. EXPERIMENTAL EVALUATION

We evaluated our system (i.e., *CCA* tool) using three cases (i.e, best, practical, customised). For the best case, it is assumed that the cloud provider 'X' provides all positive assertions when filling out the *CAIQ*. In the practical (or real-world) case, we use assertions from the cloud-based service providers published in the STAR hosted by *CSA*. For the customised case, we assume that the customers might have individual preferences on selecting domains (e.g., CO, DG, SA) when assessing the capabilities of cloud providers. The *CCA* tool provides customised trust values of cloud providers based on the customers' selections of CAIQ domains. Apart from these cases, there can be a worst case where a cloud provider might leave all the questions unanswered or answer all the questions with negative assertions. This particular case is assumed to be unrealistic as the cloud provider is not going to engage herself in such a practice as might lower their reputation in the marketplace. One might think of a case in which a cloud provider could be impersonated by another malicious entity providing falsified information in order to hamper the provider's reputation. We assume *CSA* as a *trusted third party* that checks the authenticity of the submissions as well as of the cloud providers and accuracy of the contents before publishing in the public registry (i.e., *CSA STAR*).

Security Comm. Networks 0000; **00**:1–18 © 0000 John Wiley & Sons, Ltd.
DOI: 10.1002/sec
Prepared using secauth.cls

Table II. Cloud Control Assessment for Cloud 'X': Best case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment $(t, c, f); E$
CO	16	0	0	0	16	(1,1,0.99)	
DG	16	0	0	0	16	(1,1,0.99)	
FS	9	0	0	0	9	(1,1,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	75	0	0	0	75	(1,1,0.99)	
LG	4	0	0	0	4	(1,1,0.99)	(1,1,0.8953); E=1
OM	9	0	0	0	9	(1,1,0.99)	
RI	14	0	0	0	14	(1,1,0.99)	
RM	6	0	0	0	6	(1,1,0.99)	
RS	12	0	0	0	12	(1,1,0.99)	
SA	32	0	0	0	32	(1,1,0.99)	

1. Best case: Table II shows the positive assertions in the evidence space and their resulting opinions (t, c, f) using Equation 2. The last column of the table shows the final assessment based on the aggregation of all resulting opinions using the AND operator. The final assessment is given in opinion representation (t, c, f) and expectation value (E). In the final assessment one can see how the AND operator affects the initial expectation, f. It holds 0.99 (high expectation) for every single domain whereas, for all domains, it holds 0.8953, as all the information related to controls has to be true simultaneously.
2. Practical case: The *STAR* repository has several sets of completed questionnaires from different cloud providers [8]. We choose two sets of CAIQs completed by Cloud 'A' and 'B' to evaluate our approach. The identities of the cloud providers are anonymized due to *STAR*'s usage restrictions. At present, the STAR repository does not classify the completed *CAIQ*s according to the types (e.g., SaaS, PaaS, IaaS) of services offered by the cloud providers. Thus, we assume that Cloud 'Y' and Cloud 'Z' are similar to the providers (Cloud 'A' and 'B' respectively) in terms of service types. They completed the questionnaire and published the answers in the *STAR*.
   Table III and Table IV present a summary of the assertions and the corresponding resulting opinions based on the completed questionnaires stored in the *STAR*. According to the final assessment (i.e., *CAIQ* assessment) given in Table III and Table IV, cloud consumers can easily identify the trustworthy (or dependable) provider (in this case, Cloud 'A'). The expectation value of Cloud 'A' is much higher than that of Cloud 'Y'. This means that the Cloud 'A' is more dependable than the Cloud 'Y' in terms of control competencies and capabilities. Hence, the cloud consumers choose Cloud 'A' based on the expectation value (E) in this case. We also have to note that in addition to the expectation value, the certainty (c) value is a good indicator of whether the aggregated average rating (t) is supposed to be representative or whether further analysis is required. If consumers need further analysis, they can browse each domain individually (using our *CCA* tool) for comprehensive assessment of the security controls released by the cloud provider(s).
   In Table V and Table VI, we present the final assessment for Cloud 'B' and Cloud 'Z', respectively. Cloud consumers follow the same approach as described above to identify the most trustworthy (or dependable) cloud provider (Cloud 'Z') based on the assessment of their security controls.
3. Customised case: Table VII and Table VIII reflect customer's preferences when selecting a dependable and trustworthy security services provider in the cloud marketplace. We assume that, in particular, customers particularly prefer CO, DG, FS and IS domains for the required service provisioning. We test the customised case on the completed *CAIQ* by Cloud 'A' and Cloud 'Y'. We observed notable changes in the opinion values as well as expectation values for both providers compare to the values in Table III and Table IV. The customisation feature in the *CCA* tool makes the assessment more user-centric than the existing excel-based tool available on the *CSA* website. This particular case shows that different customers can get different trust

scores of the same cloud providers based on their preferred domains.

Limitations

Although, our system reliably evaluates trustworthiness of cloud providers based on the *CAIQ* assessment, there are few limitations that need to be mentioned. Firstly, the cloud providers' completed *CAIQ*s in the *STAR* repository are not classified according to the types of services. Hence, we use synthetic datasets (e.g., Cloud 'Y' and Cloud 'Z') to compare the *CAIQ*s from the *STAR* to show the validity and applicability of our approach. Secondly, we found inconsistencies in the completed *CAIQ*s, e.g., left out the assertions (yes/no/NA), completing the questionnaire only providing comments but no assertions. Currently, our approach is able to assess partial inconsistency (e.g., classify left out answers as 'unknown'), but, not able to assess comment-based *CAIQ*s.

7. CONCLUSIONS

The business market of cloud computing is growing rapidly. New cloud providers are entering the market with huge investments and established providers are investing millions into new data centres around the world. On the one hand, cloud providers need means to stand out in the marketplaces. On the other hand, it is extremely difficult for cloud consumers to identify trustworthy (or dependable) cloud providers in these marketplaces. In order to support cloud providers as well as consumers, we proposed a multi-faceted *TM* system for cloud computing marketplaces. The *TM* system not only allows cloud providers to present their competencies and capabilities regarding multiple attributes by means of a self-assessment questionnaire (i.e., *CAIQ*) but also supports consumers to determine trustworthy cloud providers based on *CAIQ* assessment. According to the *TM* system architecture presented in Section 4.3, assessment information can be derived from multiple sources regarding multiple attributes.

In this article, we present the first realization (*CCA* tool) of the *TM* system using *CAIQ* as one of the sources. The system includes our novel trust metric (*CertainTrust* and *CertainLogic*) in order to extract opinions from provider-supplied pieces of evidence (assertions to the *CAIQ* domains) and combine these opinions to assess trustworthiness of cloud providers. The system is validated using the *CSA STAR* datasets. Moreover, our proposed system includes an integrated graphical input interface. The proposed interface is designed to support the cloud providers to answer the control questions more conveniently than the existing excel-sheet based interface. The system also offers an intuitive and interactive navigation and comprehensive display interface for the consumers to analyse the assessment results. To the best of our knowledge, the *CCA* is the first-ever tool that automates the *CAIQ* and provides the basis to determine trustworthy (or dependable) cloud providers. We believe that the proposed tool not only lowers the entrance barrier for cloud providers but also ensures intuitive and seamless access to providers' competencies and capabilities for the consumers.

Future Work

We are currently working on mechanisms to derive opinions from other available sources (e.g., consumers' feedback, TPM-based attestation) in order to validate the *CAIQ* assessment. Additionally, we are performing experiments in the context of *CAIQ* assessment considering consumers' preferences in selecting reliable sources of opinions. Consumers' behaviour in selecting trustworthy cloud providers independent of rating are considered as an effective parameter to calculate trustworthiness in [20]. Thus, integration of such a parameter in our approach remains as a future work. In order to protect the TM system against attacks, we will also focus on designing attack models and their mitigation approaches as a part of our future work. Nevertheless, practical incentive mechanisms need to be integrated in the proposed system to encourage bigger portion of cloud providers to complete the questionnaire. Hence, we will investigate the existing incentive mechanisms in the area of trust management in order to develop a suitable one for our system.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their comments and suggestions to enhance the quality of this manuscript. In particular, the authors would like to acknowledge Marlin Pohlman, Said Tabet, Ryan K. L. Ko for comments and suggestions during the development of the CCA tool. The demo of the CCA tool was presented in the CSA SecureCloud 2012 event and would not have been possible without CSA's active interest and organisational support. Last of all, the authors would like to thank Peter Zastoupil for proof-reading the article.

REFERENCES

1. Fujitsu Research Institute. Personal data

Table III. Cloud Control Assessment for Cloud 'A' (anonymized): Practical case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	16	0	0	0	16	(1,1,0.99)	
DG	15	1	0	0	16	(0.9375,1,0.99)	
FS	7	0	2	0	9	(1,0.9403,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	72	2	0	1	74	(0.973,1,0.99)	
LG	2	0	0	2	2	(1,1,0.99)	(0.5186,0.9945,0.8953);E=0.5207
OM	4	3	0	2	7	(0.5714,1,0.99)	
RI	12	0	1	1	13	(1,0.9873,0.99)	
RM	5	0	0	1	5	(1,1,0.99)	
RS	9	0	2	1	11	(1,0.9612,0.99)	
SA	22	0	0	10	22	(1,1,0.99)	

Table IV. Cloud Control Assessment for Cloud 'Y': Practical case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	15	1	0	0	16	(0.9375,1,0.99)	
DG	15	1	0	0	16	(0.9375,1,0.99)	
FS	7	0	2	0	9	(1,0.9403,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	72	2	0	1	74	(0.973,1,0.9865)	
LG	2	2	0	0	4	(0.5,1,0.99)	(0.2239,0.9976,0.8953);E=0.2255
OM	4	3	0	2	7	(0.5714,1,0.99)	
RI	12	1	1	0	14	(0.9231,0.9891,0.99)	
RM	5	0	0	1	5	(1,1,0.99)	
RS	9	0	2	1	11	(1,0.9612,0.99)	
SA	22	0	0	10	22	(1,1,0.99)	

Table V. Cloud Control Assessment for Cloud 'B' (anonymized): Practical case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	13	1	0	2	14	(0.9286,1,0.99)	
DG	14	2	0	0	16	(0.875,1,0.99)	
FS	8	1	0	0	9	(0.8889,1,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	64	8	0	3	72	(0.8889,1,0.99)	
LG	2	0	0	2	2	(1,1,0.99)	(0.1798,1,0.8953);E=0.1798
OM	4	1	0	4	5	(0.8,1,0.99)	
RI	12	1	0	1	13	(0.9231,1,0.99)	
RM	3	2	0	1	5	(0.6,1,0.99)	
RS	9	2	0	1	11	(0.8182,1,0.99)	
SA	17	5	0	10	22	(0.7727,1,0.99)	

in the cloud: A global survey of consumer attitudes 2010. `http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf` Accessed Jan 05 2013.

2. Wu L, Buyya R. Service level agreement (sla) in utility computing systems. *Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions*, Cardellini V, Casalicchio E, Branco KRLJC, Estrella JC,

Table VI. Cloud Control Assessment for Cloud 'Z': Practical case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	14	0	0	2	14	(1,1,0.99)	(0.5911,0.9997,0.8953);E=0.5912
DG	15	1	0	0	16	(0.9375,1,0.99)	
FS	9	0	0	0	9	(1,1,0.99)	
HS	4	0	0	0	4	(1,1,0.99)	
IS	71	1	0	3	72	(0.9861,1,0.9861)	
LG	2	0	0	2	2	(1,1,0.99)	
OM	5	0	0	4	5	(1,1,0.99)	
RI	12	1	0	1	13	(0.9231,1,0.99)	
RM	4	1	0	1	5	(0.8,1,0.99)	
RS	10	1	0	1	11	(0.9091,1,0.99)	
SA	20	1	1	10	22	(0.9524,0.9957,0.99)	

Table VII. Cloud Control Assessment for Cloud 'A' (anonymised): Customised case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	16	0	0	0	16	(1,1,0.99)	(0.911,0.9862,0.9606);E=0.9116
DG	15	1	0	0	16	(0.9375,1,0.99)	
FS	7	0	2	0	9	(1,0.9403,0.99)	
IS	72	2	0	1	74	(0.973,1,0.99)	

Table VIII. Cloud Control Assessment for Cloud 'Y': Customised case

Domains	r	s	u	NA	N	Resulting Opinion (t, c, f)	Final Assessment (t, c, f);E
CO	15	1	0	0	16	(0.9375,1,0.99)	(0.8532,0.987,0.9606);E=0.8546
DG	15	1	0	0	16	(0.9375,1,0.99)	
FS	7	0	2	0	9	(1,0.9403,0.99)	
IS	72	2	0	1	74	(0.973,1,0.99)	

Monaco FJ (eds.). chap. 1, IGI Global, 2011; 1–25.

3. Li H, Jeng JJ. Ccmarketplace: a marketplace model for a hybrid cloud. *Proceedings of the 2010 Conference of the Center for Advanced Studies on Collaborative Research*, CASCON '10, IBM Corp.: Riverton, NJ, USA, 2010; 174–183, doi:10.1145/1923947.1923966. URL `http://dx.doi.org/10.1145/1923947.1923966`.
4. Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. *Decision Support Systems* 2007; **43(2)**:618–644.
5. Habib SM, Ries S, Muhlhauser M. Cloud computing landscape and research challenges regarding trust and reputation. *Symposia and Workshops on ATC/UIC* 2010; **0**:410–415, doi:http://doi.ieeecomputersociety.org/10.1109/UIC-ATC.2010.48.
6. Jøsang A, Keser C, Dimitrakos T. Can we manage trust? *iTrust*, Springer, 2005; 93–107.
7. Habib SM, Ries S, Muhlhauser M. Towards a trust management system for cloud computing. *IEEE TrustCom/IEEE ICESS/FCST, International Joint Conference of* 2011; **0**:933–939.
8. CSA. Security, Assurance & Trust Registry (STAR). `https://cloudsecurityalliance.org/research/initiatives/star-registry/` Accessed Jan 05 2013.
9. Haq IU, Brandic I, Schikuta E. Sla validation in layered cloud infrastructures. *GECON*, Lecture Notes in Computer Science, Springer-Verlag, 2010; 153–164.

10. 3Tera Applogic. 3tera's Cloud Computing SLA goes live March 31 2009.
11. Cloud Computing Use Case Discussion Group. Cloud computing use cases white paper-introducing slas. *Technical Report*. Cloud Computing Use Case Discussion Group, 2010. `http://cloudusecases.org/` Accessed Jan 05 2013.
12. SearchCIO. Amazon gets SAS 70 Type II audit stamp, but analysts not satisfied Nov 17 2009.
13. CSA. Consensus Assessments Initiative. `https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/` Accessed Jan 05 2013.
14. Varadharajan V. A note on trust-enhanced security. *IEEE Security and Privacy* 2009; **7**:57–59.
15. Uusitalo I, Karppinen K, Juhola A, Savola R. Trust and cloud services - an interview study. *Proc. of the 2nd IEEE Int. Conf. on Cloud Computing Technology and Science (CloudCom)*, 2010; 712–720, doi:10.1109/CloudCom.2010.41.
16. Ruohomaa S, Kutvonen L, Koutrouli E. Reputation management survey. *The Second International Conference on Availability, Reliability and Security (ARES)*, 2007; 103 –111, doi:10.1109/ARES.2007.123.
17. Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C. Distributed trust management for validating sla choreographies. *Grids and Service-Oriented Architectures for Service Level Agreements*. Springer US, 2010; 45–55.
18. Teacy WTL, Patel J, Jennings NR, Luck M. Travos: Trust and reputation in the context of inaccurate information sources. *AAMAS* 2006; **12**(2):183–198.
19. Abawajy J. Determining service trustworthiness in intercloud computing environments. *Int. Symposium on Parallel Architectures, Algorithms, and Networks* 2009; **0**:784–788, doi: http://doi.ieeecomputersociety.org/10.1109/I-SPAN.2009.155.
20. Pawar P, Rajarajan M, Nair S, Zisman A. Trust model for optimized cloud services. *Trust Management VI*, *IFIP Advances in Information and Communication Technology*, vol. 374, Dimitrakos T, Moona R, Patel D, McKnight D (eds.). Springer Berlin Heidelberg, 2012; 97–112.
21. Wang SX, Zhang L, Wang S, Qiu X. A cloud-based trust model for evaluating quality of web services. *Journal of Computer Science and Technology* 2010; **25**:1130–1142.
22. Ferrer AJ, Hernández F, Tordsson J, Elmroth E, Ali-Eldin A, Zsigri C, Sirvent R, Guitart J, Badia RM, Djemame K, *et al.*. Optimis: A holistic approach to cloud service provisioning. *Future Generation Computer Systems* 2012; **28**(1):66 – 77.
23. Buchegger S, Le Boudec JY. A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks. *P2PEcon 2004*, 2004.
24. Jøsang A, Ismail R. The beta reputation system. *Proceedings of the 15th Bled Conference on Electronic Commerce*, 2002.
25. Ries S, Heinemann A. Analyzing the robustness of certaintrust. *Trust Management II*, *IFIP Advances in Information and Communication Technology*, vol. 263, Karabulut Y, Mitchell J, Herrmann P, Jensen C (eds.). Springer Boston, 2008; 51–67.
26. Jøsang A. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 2001; **9**(3):279–212.
27. Jøsang A, McAnally D. Multiplication and co-multiplication of beliefs. *International Journal of Approximate Reasoning* 2005; **38(1)**:19–51.
28. Ries S, Habib SM, Mühlhäuser M, Varadharajan V. Certainlogic: A logic for modeling trust and uncertainty. *Trust and Trustworthy Computing*, *Lecture Notes in Computer Science*, vol. 6740, Springer Berlin / Heidelberg, 2011; 254–261.
29. Krautheim FJ. Private virtual infrastructure for cloud computing. *Proceedings of the HotCloud'09*, USENIX Association: Berkeley, CA, USA, 2009; 5–5.
30. Schiffman J, Moyer T, Vijayakumar H, Jaeger T, McDaniel P. Seeding clouds with trust anchors. *Proceedings of the ACM CCSW '10*, ACM: New York, NY, USA, 2010; 43–46, doi: http://doi.acm.org/10.1145/1866835.1866843.
31. Sadeghi AR, Stüble C, Winandy M. Property-based tpm virtualization. *Information Security*, *Lecture Notes in Computer Science*, vol. 5222. Springer Berlin / Heidelberg, 2008; 1–16.
32. Sadeghi AR, Stüble C. Property-based attestation for computing platforms: caring about properties, not mechanisms. *Proceedings of the NSPW '04*, ACM, 2004; 67–77.
33. Nagarajan A, Varadharajan V. Dynamic trust enhanced security model for trusted platform based services. *Future Gener. Comput. Syst.* May 2011; **27**:564–573.
34. Blaze M, Feigenbaum J, Keromytis AD. Keynote: Trust management for public-key infrastructures. *Infrastructures (Position Paper). Lecture Notes in Computer Science 1550*, 1998; 59–63.
35. Chu YH, Feigenbaum J, LaMacchia B, Resnick P, Strauss M. Referee: trust management for web applications. *Comput. Netw. ISDN Syst.*

September 1997; **29**:953–964.
36. Herzberg A, Mass Y, Michaeli J, Naor D, Ravid Y. Access control meets public key infrastructure, or: Assigning roles to strangers. *In Proceedings of the 2000 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, 2000; 2–14.
37. Grandison T, Sloman M. Trust management tools for internet applications. *iTrust*, *Lecture Notes in Computer Science*, vol. 2692, Nixon P, Terzis S (eds.), Springer, 2003; 91–107.
38. CSA. Cloud Controls Matrix 2011.
39. Schryen G, Volkamer M, Ries S, Habib SM. A formal approach towards measuring trust in distributed systems. *Proceedings of the 2011 ACM Symposium on Applied Computing*, SAC '11, ACM: New York, NY, USA, 2011; 1739–1745.
40. Kerr R, Cohen R. Smart cheaters do prosper: defeating trust and reputation systems. *AAMAS '09: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems*, IFAAMAS: Richland, SC, 2009; 993–1000.
41. Gambetta D. Can we trust trust? *Trust: Making and Breaking Cooperative Relations*, Gambetta D (ed.). chap. 13, Department of Sociology, University of Oxford, 2000; 213–237.
42. Ries S. Extending bayesian trust models regarding context-dependence and user friendly representation. *Proceedings of the ACM SAC*, ACM: New York, NY, USA, 2009; 1294–1301, doi:http://doi.acm.org/10.1145/1529282.1529573.
43. Ries S, Habib SM, Mühlhäuser M, Varadharajan V. Certainlogic: A logic for modeling trust and uncertainty. *Technical Report TUD-CS-2011-0104*, Technische Universität Darmstadt 2011.
44. Ries S, Aitenbichler E. Limiting sybil attacks on bayesian trust models in open soa environments. *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC '09. Symposia and Workshops on*, 2009; 178 –183, doi:10.1109/UIC-ATC.2009.82.
45. Habib SM, Ries S, Hauke S, Mühlhäuser M. Fusion of opinions under uncertainty and conflict – trust assessment for cloud marketplaces. *Technical report TUD-CS-2012-0027*, Technische Universität Darmstadt 2012.
46. CSA. Security guidance for critical areas of focus in cloud computing v3.0. *Technical Report*, Cloud Security Alliance 2009.
47. CSA. Security, Assurance & Trust Registry (STAR) FAQ. `https://cloudsecurityalliance.org/star/faq/` Accessed Jan 05 2013.
48. Ries S. Trust in ubiquitous computing. PhD Thesis, Technische Universität Darmstadt 2009.
49. CSA. Cloud Audit. `https://cloudsecurityalliance.org/research/cloudaudit/` Accessed Jan 05 2013.