Towards a Trust Management System for Cloud Computing

Sheikh Mahbub Habib*, Sebastian Ries†, Max Mühlhäuser‡
Technische Universität Darmstadt, CASED
Mornewegstr. 32, DE-64293, Germany
Email: *sheikh.habib@cased.de,†ries@cased.de,‡max@informatik.tu-darmstadt.de

***Abstract*—Cloud computing provides cost-efficient opportunities for enterprises by offering a variety of dynamic, scalable, and shared services. Usually, cloud providers provide assurances by specifying technical and functional descriptions in Service Level Agreements (SLAs) for the services they offer. The descriptions in SLAs are not consistent among the cloud providers even though they offer services with similar functionality. Therefore, customers are not sure whether they can identify a trustworthy cloud provider only based on its SLA. To support the customers in reliably identifying trustworthy cloud providers, we propose a multi-faceted Trust Management (TM) system architecture for a cloud computing marketplace. This system provides means to identify the trustworthy cloud providers in terms of different attributes (e.g., security, performance, compliance) assessed by multiple sources and roots of trust information.**

***Index Terms*—Cloud computing, Trust models, Reputation, Trust Management, Architecture**

I. Introduction

Cloud computing offers dynamic, scalable, shared resources (e.g., computing power, storage, software) over the internet from remote data centres to the 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 of these services often feel that they lose the control over their data, and they are not sure whether they can trust the cloud providers. 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). At present, although cloud providers demonstrate their preventive measures by including related descriptions in the SLAs, assurances and compensations for SLA violations are not convincing enough for the consumers. Especially, SLAs with vague clauses and unclear technical specifications lead the consumers into 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 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. Such a competitive market needs means to reliably assess the quality level of the service providers.

Trust and reputation (TR) systems [2] are successfully used in numerous application scenarios to support users in identifying the reliable and trustworthy providers, e.g., on eBay, Amazon, and app markets for mobile applications. Similar approaches are needed to support customers in selecting appropriate trustworthy cloud providers. 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 [3] that are required to support the customers in selecting providers in a cloud marketplace. Therefore, TR systems have to evolve into Trust Management (TM) systems – as defined in [4] – to support the customers in making transparent assessments before selecting reliable trustworthy cloud providers.

The main purpose of this paper is to provide an overview of our TM system architecture for cloud computing marketplace. This architecture will reflect the multi-faceted nature of trust assessment by considering multiple attributes, sources and roots of trust. It aims at supporting customers to identify trustworthy services providers as well as trustworthy service providers to stand out.

The rest of the paper is organized as follows: Section II gives the related work. Section III provides a list of required attributes and properties for TM systems in cloud computing. Section IV gives a brief overview on modelling trustworthiness in cloud computing. Section V describes the trust metric that is used in our proposed TM system. Section VI illustrates the novel architecture of the TM system for cloud computing. In section VII, we conclude and discuss our future work.

II. 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.

A. Applied technologies

In this section, technologies that are currently applied to establish trust on the cloud providers are presented.

SLAs: In practice, one way to establish trust for cloud providers is the fulfilment of SLAs. SLA validation [5] and monitoring [6] 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 SLAs are written by the cloud providers in such a way so that the customers merely get the advantage of applying for compensation (e.g., service credits) due to SLA violation. This problem arise for not having standardized SLAs for the stakeholders in cloud computing marketplace. Although, the problem is addressed by industry driven initiative [7] for establishing standardized SLAs, this initiative is far from completion and implementation in practice.

Auditing: Cloud providers use different audit standards (e.g., SAS 70 II, FISMA, ISO 27001) to assure users about their offered services and platforms. For example, Google lists SAS 70 II and FISMA certification to ensure 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 are not sufficient to alleviate the users' security concerns [8] and most cloud providers are not willing to share the audit reports, which also leads to a lack of transparency.

Ratings & Measurements: Recently, a cloud marketplace[1] has been launched to support consumers in identifying reliable 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 the trustworthiness of cloud providers. Furthermore, there is a new commercial cloud marketplace named SpotCloud[2] that provides a platform where cloud consumers choose between potential providers based on cost, quality, and location. Here, 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 (CAI) questionnaire [9]. This questionnaire provides means for assessing the capabilities and competence of cloud providers in terms of different attributes (e.g., compliance, information security, governance). However, the metrics working group does not provide any proposals for a metric yet (in contrast to the other working groups of CSA).

B. Research trends

This section presents research-driven state-of-the-art approaches regarding trust establishment in various service environments.

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) [2], [10]. The concepts have also been adapted in grid computing [11], [12], inter-cloud computing environments [13], and selecting web services [14]. The approaches for TR-based decision making in different environments usually do not take account of multiple attributes (e.g., performance, security, customer support) and contextual attributes (e.g., different service delivery models and service deployment models) except the approach for grid computing environment and selecting web services by Irfan et al. [11] and Wang et al. [14], respectively. Irfan et al. proposed a trust model based on certificates (PKI (public key infrastructure)-based) and reputation-based trust system as a part of an SLA validation framework. Wang et al. proposed a trust model which takes multiple factors (reputation, trustworthiness, and risk) into account when evaluating web services. Both approaches consider SLA validation as the main factor for establishing trust on the grid service and web service providers. An SLA validation framework can help identifying violation-prone service providers. However, in order to serve the customers best, a TR model should take into account all the available sources of information including user feedback and third-party performance measurements.

Furthermore, trust models for cloud computing need to take specific cloud-related attributes into account that are relevant when selecting cloud providers. Those attributes go beyond the usual QoS parameters [15], which are considered when selecting web service providers. Examples for those cloud-related parameters are: elasticity, service delivery and deployment models, geographical location, and audit standards.

Moreover, 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 [12], [16], [17], [18]. The challenge of these approaches is to find good models for deriving trust from direct experience of a user, recommendations from third parties, and sometimes additional information, e.g., social relationships. Especially, those models aim on providing robustness to attacks, e.g., misleading recommendations, re-entry, sybil attacks. For those tasks, they usually provide operators for combining evidence from different sources about the same target (called consensus) and for weighting recommendations based on the trustworthiness of the source (called discounting).

[1] http://beta-www.cloudcommons.com/web/cc/about-smi

[2] http://www.spotcloud.com/

The operators for consensus and discounting are important when deriving trust based on recommendations. In cloud computing environments, cloud-based services are hosted in complex distributed systems. For deriving the trustworthiness of a complex distributed system based on the knowledge about the trustworthiness of its components and subsystems regarding different attributes (e.g., security, performance, customer support), we additionally need operators for the evaluation of propositional logic terms, which are not addressed by most approaches [12], [19], [20], except for *Subjective Logic* [21], [22] and *CertainLogic* [23].

Trusted Computing: Apart from the field of trust and reputation models, there are a number of approaches from the field of trusted computing for ensuring a 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 [24]. Schiffman et al. proposed a hardware-based attestation mechanism to provide assurance of data processing protection in the cloud for customers [25]. There are further approaches like property-based TPM virtualization[26], which can be used in the cloud scenario to assure the users about the fulfilment of security properties in cloud platforms using attestation concepts. However, in general attestation concepts based on trusted computing, e.g., [27], focus on the evaluation of single platforms not on compositions. Moreover, several ambiguities arise from the property-based attestation approach which can be addressed in dynamic trust models (e.g., [28]).

Our objective is to develop a TM system that aggregates and manages trust-related information from different sources (user ratings, provider statements, measurements, property certificates) which are relevant (and often available) when assessing the trustworthiness of a cloud provider. In our previous publications [29], [23], [30], we provided a formal approach for modelling, representing and assessing the trustworthiness of complex distributed systems and presented how the approach contributed to trust-based decision making when selecting trustworthy cloud providers. In this paper, we provide a novel architecture and a description of internal components of a TM system based on the formal approach to enable transparent, reliable and trustworthy selection of cloud providers.

III. Trust Management Systems for Cloud Computing

TM systems allow relying parties/entities to reliably represent their capabilities and competence of the underlying systems in terms of relevant attributes. In cloud computing, multiple attributes and trust information from multiple sources and roots are needed to be taken into account when selecting trustworthy cloud providers. TM system for cloud computing should be able to combine multi-attribute based trust derived from multiple sources and roots: soft (e.g., user feedbacks or reviews) and hard trust (e.g., certificates or audits).

A. Attributes for Trust Assessment in Cloud Computing

During the trust assessment phase, multiple attributes need to be taken into account 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 (*QoS+*) is given in a recent publication [3] and in the *Cloud Controls Matrix (CCM)* [31] by CSA. We aim to assess the trustworthiness of a cloud provider with respect to these attributes.

In [3], the attributes (e.g., security measures, compliance, customer support) are mentioned without giving detailed definitions. In *CCM*, CSA has documented the attributes with detailed definitions. Additionally, they showed the applicability of the attributes in different service delivery models (e.g., SaaS, IaaS, PaaS) and demonstrated the compliance mapping of the attributes with different audit standards in cloud computing.

B. Properties for TM Systems in Cloud Computing

TM systems require specific properties to incorporate those attributes for trust establishment in a cloud marketplace.

Multi-faceted Trust Computation: The computation of trust should consider the attributes mentioned in [31] and [3], 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 the following:

- Multiple attributes: TM systems should possess mechanisms to aggregate multiple attributes (cf. Section III-A) 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 asks for considering multiple sources of information in contrast to just relying on a single source of information (due to limitations in the TM systems and TR models). For example, information related to a performance attribute may come from two sources– providers and third-party. Moreover, multiple sources can provide quantitative and qualitative information, being factored into the trust establishment process, derived from multiple roots. For example, information related to 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 can 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 a specific sources and roots of trust information and to a specific attributes based on their interests and requirements. TM system 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 [29], [23].

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 together 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 earlier [32]. A number of different attacks (e.g., playbooks, proliferation attacks, reputation lag attacks, false praise or accusation (collusion), whitewashing (reentry), sybil attacks) against trust and reputation systems have been discussed [32]. These types of attacks will also be of concern when designing trust management systems for a cloud computing marketplace. Thus, attack resiliency is a central design goal.

IV. 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 III-A). 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 and OR), those propositions can become the basis for combined statements in the form of propositional logic terms (PLTs).

V. Trust Metric: Representation and Computation

When assessing whether or not a cloud provider fulfils a particular property, one usually encounters problems like 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 [33].

Following this basic idea, we use *CertainTrust* [20] and *CertainLogic* [30] as the basis for a trust metric in our planned instantiation of the architecture presented in the next section. In the following, we provide a brief introduction to the representation and computation that we need to support.

A. Representation

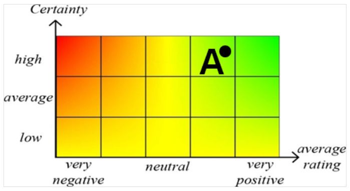

Figure 1. CertainTrust: Graphical Interface

In CertainTrust (for the full details see [20]), 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, $o = (t, c, f) \in \{[0, 1] \times [0, 1] \times [0, 1]\}$ 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 [20], [30], the assessment of the parameters can be based on evidence from past experience, based on expert assessments, derived from opinions in subjective logic [21], or derived from a Bayesian probability distribution. 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:

$$E(t, c, f) = t * c + (1 - c) * f$$

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

B. Computation

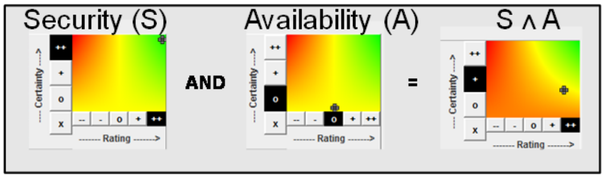

Figure 2. Example: Computation of Trust – AND

The evaluation of the trustworthiness of an entity usually requires operators for considering recommendations from third parties and for the combination of trust values that are associated with different opinions. Here, *CertainTrust* and *CertainLogic* already provide a set of operators. The operators for deriving trust from recommendations are called *consensus* and *discounting* (see [18], [34]). The consensus operator provides a 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 the source. This aggregation can also be optimized to counteract Sybil attacks [34].

Furthermore, the operators for AND, OR, and NOT proposed in [23], [30] allow the evaluation of PLTs under uncertainty – in particular, those operators provide means for the evaluation of combinations of independent statements. Fig. 2 shows an example using the AND operator to combine an opinion on the *security* of a system with the opinion on the *availability* of this system. Especially, these operators have been shown to be compatible with subjective logic and with the standard probabilistic approach [30].

Currently, we believe that we require an additional operator ($FUSION$) for the fusion of dependent statements. The definition of this operator is part of our future work.

VI. Trust Management System Architecture for Cloud Computing

Having introduced the necessary tools for assessing, representing and computing trust, in this section, we propose a novel architecture (cf. Fig. 3) of a TM system for cloud computing marketplaces and a brief description of its internal components.

A. 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 CAI questionnaire as a part of 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.

B. Consensus Assessments Initiative Questionnaire (CAIQ) Engine

The CAIQ engine allows cloud providers to fill in the CAI 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 are designed to be answered in 'yes' or 'no'. All the answers are stored in the TI for further processing.

C. Trust Manager (TMg)

The TMg allows cloud users to specify their requirements and opinions when accessing the trust score of cloud providers. It provides a web-based 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 the self-assessment using the CAIQ and assessment of cloud-based 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, 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 individual trust values in the form of opinions ($o(t, c, f)$) and a graphical interface (i.e., HTI) of every single attribute used for calculating the overall trust value. In the TM system architecture (cf. Fig. 3), the TMg is tightly coupled with the TSE and TCE to support the above mentioned features for the cloud users.

D. Trust Semantics Engine (TSE)

The TSE models which configuration of PLTs are considered to be the expected (trustworthy) behaviour of a cloud provider in terms of a specific attribute. A default configuration of PLTs should be based on the CAIQ answers stored in the repository (TI). The TSE should be able to convert every trust relevant information into PLTs. For deriving PLTs from system/service specifications, the TSE integrates the formal framework proposed in [29]. PLTs can also be derived from the CAI questionnaire. Especially, we model the bottom-level questions of the

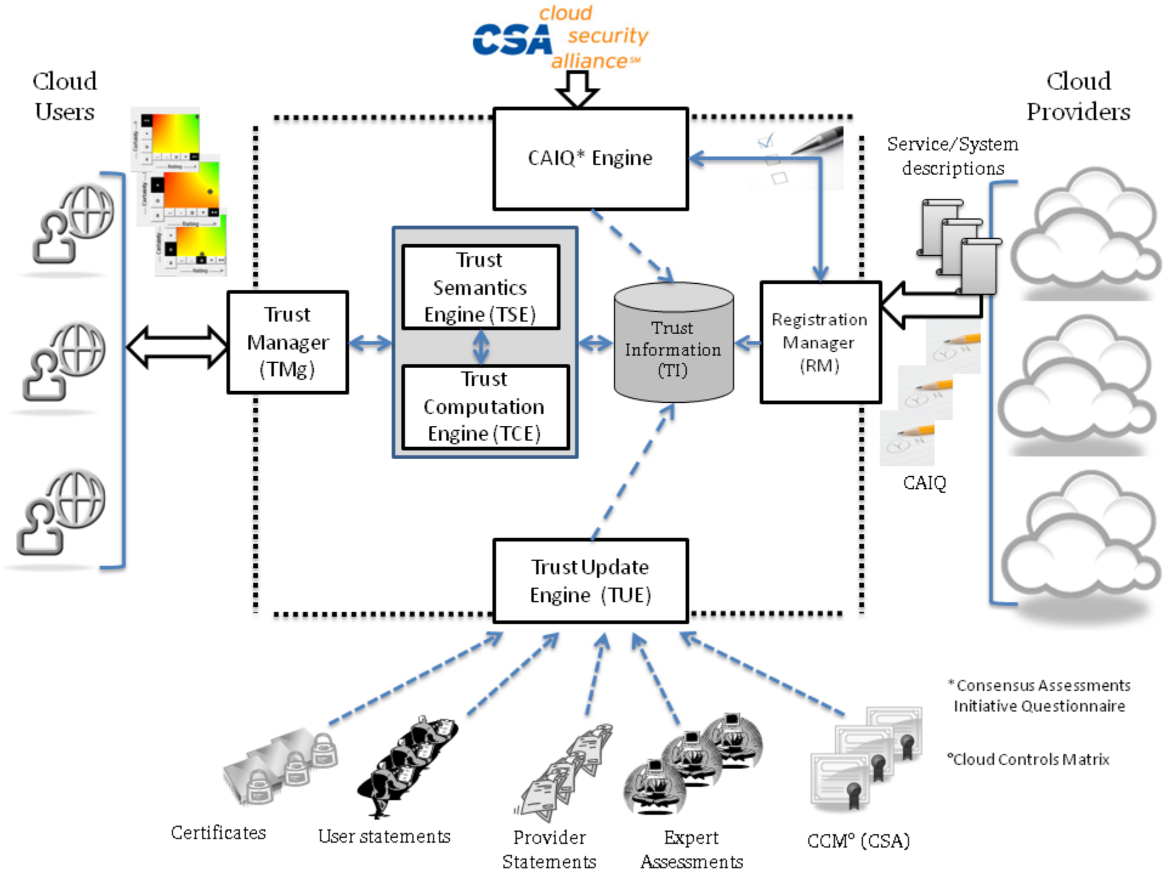

Figure 3. Architecture Overview

questionnaire, e.g., CO-01 to CO-07, in the category compliance (CO) as propositions, and ask the cloud providers for their opinions. Afterwards, we use the *CertainLogic's AND* operator to combine these opinions on the propositions within each category. Finally, we combine the opinions that have been derived per category over all the categories. Moreover, this engine supports users to express their preferred attributes and also the sources and roots of information which they choose to be taken into account. The TSE should be able to customize the configuration of PLTs in order to reflect the users' preference. Customized PLTs are sent to the TCE for the final evaluation.

E. Trust Computation Engine (TCE)

The TCE consist of operations related to the operators (*AND*, *OR*, *NOT*, *FUSION*, *CONSENSUS*, *DISCOUNTING*), used in PLTs to compute the corresponding trust values. The TCE is tightly coupled with the TSE to evaluate the PLTs and compute corresponding trust values. The trust values are archived in the TI repository after computation.

F. Trust Update Engine (TUE)

The TUE allows to collect opinions from various sources and roots about the trustworthiness of cloud providers. The opinions collected here should be filtered in such a way so that the users may use the valid opinions according to their requirements. For example, spam and information filtering should be used to eliminate junk or useless information to be stored in the TI repository. The filtered opinions are then taken into account when updating the trust value of cloud providers.

VII. Conclusion and Future Work

The business market of cloud computing is growing rapidly. New cloud providers are entering the market with huge investments and the established providers are investing millions into new data centres around the world. At present, it is extremely difficult for cloud customers to tell the difference between a good and poor quality cloud provider. In fact, cloud marketplaces are lacking a system or platform which can distinguish the cloud providers in terms of different attributes (cf. III-A). Therefore, we propose an architecture of a multi-faceted TM system for cloud marketplaces providing means to efficiently differentiate between a good and a poor quality (beyond the performance issues) providers. The system is designed to provide a customized trust score of a provider based on the attributes selected by the customers. Moreover, the system aims to provide trust scores of the cloud providers based on trustworthy behaviour of the underlying systems and the service providers' answers to the CSA CAI questionnaire [9]. In particular, we believe that taking into account this standardized questionnaire lowers the entrance barrier for cloud providers. For the customers, this system has a special feature allowing them to select from various sources and roots of trust information (e.g., user statements, property certificates via remote attestation, compliance to audit standards via CCM) as a basis for the computation of the trust scores. Finally, the trust score will not be represented in plain numbers only, but the presentation will be supported by an intuitive graphical interface. The proposed TM system will increase transparency between the customers and the cloud providers, which is extremely important for the healthy economic growth of cloud marketplace.

At present, we have implemented java-based tools that will serve as a basis for TSE and TCE (with *AND*, *OR*, *NOT*, *CONSENSUS*, and *DISCOUNTING* operators). Currently, we are implementing the tool for the CAIQ Engine. Trust Manager, Registration Manager, and Trust Update Engine (with content or information filtering mechanisms) are part of our future work.

References

[1] Fujitsu Research Institute, "Personal data in the cloud: A global survey of consumer attitudes," 2010.

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

[3] S. M. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," *Symposia and Workshops on ATC/UIC*, vol. 0, pp. 410–415, 2010.

[4] A. Jøsang, C. Keser, and T. Dimitrakos, "Can we manage trust?" in *iTrust*. Springer, 2005, pp. 93–107.

[5] I. U. Haq, I. Brandic, and E. Schikuta, "Sla validation in layered cloud infrastructures," in *GECON*, ser. Lecture Notes in Computer Science. Springer-Verlag, 2010, pp. 153–164.

[6] 3Tera Applogic, "3tera's Cloud Computing SLA goes live," March 31 2009.

[7] Cloud Computing Use Case Discussion Group, "Cloud computing use cases white paper- introducing slas," in *Technical Report*. Cloud Computing Use Case Discussion Group, 2010, http://cloudusecases.org/.

[8] SearchCIO, "Amazon gets SAS 70 Type II audit stamp, but analysts not satisfied," Nov 17 2009.

[9] CSA, "Consensus Assessments Initiative," 2011, https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/.

[10] S. Ruohomaa, L. Kutvonen, and E. Koutrouli, "Reputation management survey," in *The Second International Conference on Availability, Reliability and Security (ARES)*, 2007, pp. 103 –111.

[11] I. U. Haq, R. Alnemr, A. Paschke, E. Schikuta, H. Boley, and C. Meinel, "Distributed trust management for validating sla choreographies," in *Grids and Service-Oriented Architectures for Service Level Agreements*. Springer US, 2010, pp. 45–55.

[12] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "Travos: Trust and reputation in the context of inaccurate information sources," *AAMAS*, vol. 12, no. 2, pp. 183–198, 2006.

[13] J. Abawajy, "Determining service trustworthiness in intercloud computing environments," *Int. Symposium on Parallel Architectures, Algorithms, and Networks*, vol. 0, pp. 784–788, 2009.

[14] S.-X. Wang, L. Zhang, S. Wang, and X. Qiu, "A cloud-based trust model for evaluating quality of web services," *Journal of Computer Science and Technology*, vol. 25, pp. 1130–1142, 2010.

[15] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in *Proceedings of the 27th ICDCSW*. Washington, DC, USA: IEEE Computer Society, 2007, p. 25.

[16] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks," in *P2PEcon 2004*, 2004.

[17] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Conference on Electronic Commerce*, 2002.

[18] S. Ries and A. Heinemann, "Analyzing the robustness of CertainTrust," in *2nd Joint iTrust and PST Conference on Privacy, Trust Management and Security*. Springer, 2008, pp. 51 – 67.

[19] Y. Wang and M. P. Singh, "Formal trust model for multiagent systems," in *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI)*, 2007.

[20] S. Ries, "Extending bayesian trust models regarding context-dependence and user friendly representation," in *Proceedings of the ACM SAC*. New York, NY, USA: ACM, 2009, pp. 1294–1301.

[21] A. Jøsang, "A logic for uncertain probabilities." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–212, 2001.

[22] A. Jøsang and D. McAnally, "Multiplication and comultiplication of beliefs," *International Journal of Approximate Reasoning*, vol. 38(1), pp. 19–51, 2005.

[23] S. Ries, S. M. Habib, M. Mühlhäuser, and V. Varadharajan, "Certainlogic: A logic for modeling trust and uncertainty," in *Trust and Trustworthy Computing*, ser. Lecture Notes in Computer Science, vol. 6740. Springer Berlin / Heidelberg, 2011, pp. 254–261.

[24] F. J. Krautheim, "Private virtual infrastructure for cloud computing," in *Proceedings of the HotCloud'09*. Berkeley, CA, USA: USENIX Association, 2009, pp. 5–5.

[25] J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel, "Seeding clouds with trust anchors," in *Proceedings of the ACM CCSW '10*. New York, NY, USA: ACM, 2010, pp. 43–46.

[26] A.-R. Sadeghi, C. Stüble, and M. Winandy, "Property-based tpm virtualization," in *Information Security*, ser. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2008, vol. 5222, pp. 1–16.

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

[28] A. Nagarajan and V. Varadharajan, "Dynamic trust enhanced security model for trusted platform based services," *Future Gener. Comput. Syst.*, vol. 27, pp. 564–573, May 2011.

[29] G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in *Proceedings of the ACM SAC*, 2011.

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

[31] CSA, "Cloud Controls Matrix," 2011, https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/.

[32] R. Kerr and R. Cohen, "Smart cheaters do prosper: defeating trust and reputation systems," in *AAMAS '09: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems*. Richland, SC: IFAAMAS, 2009, pp. 993–1000.

[33] D. Gambetta, "Can we trust trust?" in *Trust: Making and Breaking Cooperative Relations, electronic edition*, D. Gambetta, Ed., 2000, ch. 13, pp. 213–237.

[34] S. Ries and E. Aitenbichler, "Limiting sybil attacks on bayesian trust models in open soa environments," in *Proceedings of the The First International Symposium on Cyber-Physical Intelligence (CPI-09)*, 2009.