This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

SelCSP: A Framework to Facilitate Selection of Cloud Service Providers

Nirnay Ghosh, Soumya K. Ghosh, Sajal K. Das

***Abstract*—With rapid technological advancements, cloud marketplace witnessed frequent emergence of new service providers with similar offerings. However, *service level agreements (SLAs)*, which document guaranteed quality of service levels, have not been found to be consistent among providers, even though they offer services with similar functionality. In service outsourcing environments, like cloud, the quality of service levels are of prime importance to customers, as they use third-party cloud services to store and process their clients' data. If loss of data occurs due to an outage, the customer's business gets affected. Therefore, the major challenge for a customer is to select an appropriate service provider to ensure guaranteed service quality. To support customers in reliably identifying *ideal* service provider, this work proposes a framework, *SelCSP*, which combines *trustworthiness* and *competence* to estimate risk of interaction. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on *transparency* in provider's SLA guarantees. A case study has been presented to demonstrate the application of our approach. Experimental results validate the practicability of the proposed estimating mechanisms.**

***Keywords*-Cloud, Service provider, Trust, Reputation, Relational risk, Performance risk, Competence, Service Level Agreement, Control, Transparency**

I. Introduction

CLOUD computing facilitates better resource utilization by multiplexing the same physical resource among several tenants. Customer does not have to manage and maintain servers, and in turn, uses the resources of cloud provider as services, and is charged according to pay-as-you-use model. Similar to other on-line distributed systems, like e-commerce, p2p networks, product reviews, and discussion forums, a cloud provides its services over the Internet.

Among several issues that prevented companies from moving their business onto public clouds, *security* is a major one. Some of the security concerns, specific to cloud environment are: *multi-tenancy*, *lack of customer's control over their data and application* [1], *lack of assurances and violations for SLA guarantees* [2], *non-transparency with respect to security profiles of remote datacenter locations* [3], and so on. Recent advancements in computation, storage, service-oriented architecture, and network access have facilitated rapid growth in cloud marketplace. For any service, a cloud customer may have multiple service providers to choose from. Major challenge lies in selecting an "ideal" service provider among them. By the term ideal, we imply that a service provider is trustworthy as well as competent. Selection of an ideal service provider is non-trivial because a customer uses third-party cloud services to serve its clients in cost-effective and efficient manner. In such a scenario, from the cloud customer's perspective, persisting to a guaranteed level of service, as negotiated through establishing service level agreement (SLA), is of prime importance. Data loss owing to provider's incompetence or malicious intent can never be replaced by service credits. In the present work, we focus on selection of a trustworthy and competent service provider for business outsourcing.

In 2010-11, a series of cloud outages[1,2] have been reported which include commercial service providers viz. *Amazon EC2, Google Mail, Yahoo Mail, Heroku, Sony,* and so on. In most cases, it has been observed that the failover time is quite long and customers' businesses were hugely affected owing to lack of recovery strategy on vendor side. Moreover, in some instances, customers were not even intimated about the outage by providers. Cloud providers may use the *high-quality first-replication (HQFR)* strategy proposed in [4] to model their recovery mechanism. In this work, authors propose algorithms to minimize replication cost and the number of QoS-violated data replicas. Hence, it is desirable from customer's point-of-view to avoid such loss, rather than getting guarantees of service credits following a cloud outage. Avoidance of data loss requires reliable identification of competent service provider. As customer does not have control over its data deployed in cloud, there is a need *to estimate risk prior to outsourcing any business onto a cloud*. This motivated us to propose a risk estimation scheme which makes a quantitative assessment of risk involved while interacting with a given service provider. To the best of our knowledge, estimation of risk of interaction in cloud environment has not been addressed. Hence, in this respect, the current work is significant as it proposes a framework, *SelCSP* [3], which attempts to compute risk involved in interacting with a given cloud service provider. The framework estimates perceived level of interaction risk by combining trustworthiness and competence of cloud provider. Trustworthiness is computed from ratings obtained through either direct interaction or feedback. Competence is estimated

Nirnay Ghosh is a PhD student in the School of Information Technology, Indian Institute of Technology, Kharagpur - 721302, India E-mail: nirnay.ghosh@gmail.com.

Soumya K. Ghosh is a Professor in the School of Information Technology, Indian Institute of Technology, Kharagpur - 721302, India E-mail: skg@iitkgp.ac.in.

Sajal K. Das is a Department Chair & St. Clair Endowed Chair in the Department of Computer Science, Missouri University of Science and Technology, MO 65409, USA Email: sdas@mst.edu

[1] http://www.crn.com/slide-shows/index.htm

[2] http://cloutage.org/

[3] SelCSP stands for "Select Cloud Service Provider"

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

from the transparency of SLA guarantees.

We summarize the contributions of this work as follows:

- Develop a framework, called SelCSP, to compute overall perceived interaction risk.
- Establish a relationship among perceived interaction risk, trustworthiness and competence of service provider.
- Propose a mechanism by which trustworthiness of a service provider may be estimated.
- Propose a mechanism by which transparency of any provider's SLA may be computed.
- Comparison of trust and competence results generated by SelCSP and those obtained from models reported in literature.
- Analysis of results to provide insight into the behavior of the proposed risk model.

The rest of the paper is organized as follows. Section II presents a brief literature survey on other trust models used in different online systems. Section III gives brief description to proposed SelCSP framework and its different modules. An approach to estimate interaction risk with reference to multi-agent alliance has been presented in Section IV. In Section V and VI, trust and reputation estimations are proposed for computation of trustworthiness of service provider. In Section VII, competence of a service provider based on transparency of SLA is evaluated. Validation and analysis of results generated by our framework have been done in Section VIII. Finally, a conclusion is drawn in Section IX.

II. Related Works

Trust and reputation are important concepts in Internet-based applications. They facilitate decision making relevant to choosing reliable agent for electronic transactions. In the literature, trust has two notions: *reliability trust* [5] and *decision trust* [6]. Reliability trust is the subjective probability by which an individual expects that another individual performs a given action on which former's welfare depends. Decision trust is the extent to which one party is willing to depend on another even though negative consequences are possible. In cloud scenario, both notions are prevalent as customer depends on third-party provider, believing that it is reliable enough to produce positive utility. Some works [7] [8] have proposed computation models for trust by incorporating the concept of risk. Like trust, reputation has also been studied extensively. From the perspective of social network researchers [9], reputation is perceived as an entity which is globally visible to all members of a social network community. In survey papers on trust [10] [11], the authors have classified trust into five categories viz. *provision, access, delegation, identity,* and *context*. These categories model trust relationships between a relying party and: (i) a service provider, (ii) accessing resources, (iii) third-party arbitrator, (iv) signed attributes, and (v) supporting transactions, respectively. In cloud context, trust between customer and provider is of provision type. Reputation system has been classified into two types [11]: *centralized* and *distributed* depending on the site of computation. In centralized type, a central authority (reputation center) collects all the ratings, computes a reputation score for every participant, and makes all scores publicly available, while in distributed type there can be distributed stores where ratings can be submitted, or each participant simply records the opinion about each experience with other parties, and provides this information on request from relying parties. Distributed reputation systems are primarily deployed in peer-to-peer (P2P) networks.

A number of methodologies have been proposed for evaluating reputation. Some of the noteworthy are summation or average of ratings, as used in eBay's reputation forum [12], Bayesian system [13], belief models [14] [15], and fuzzy models [7] [16].

The concepts of trust and reputation have been successfully implemented in multiple Internet mediated services viz., *eBay's feedback forum* [4], *Epinions* [5], *Amazon* [6], *Slashdot* [7], and so on. A cloud environment is similar in nature to these online services, where trust and reputation also need to be enforced. One major difference between cloud and the other online systems (P2P, e-commerce, etc.) is the *degree of control* which a customer has on his data/application while using these Internet-mediated systems. A customer outsources its data and applications to a third-party cloud vendor for ease of manageability and maintainability. For Software-as-a-Service (SaaS) cloud model, this control completely rests with the provider. On contrary, P2P is largely responsible for file-sharing applications, online recommendation systems gives product reviews to support decision making, and in case of e-commerce, autonomous domains interoperate through service chaining, governed by predefined global policy.

Usually, the cloud customer uses third-party cloud services to manage its clients' data in a cost-effective and convenient manner. Therefore, if there is a loss of such data from cloud provider's end, the customer loses both business and reputation to its clients. Hence, it is imperative to establish trust relationship between customer and service provider to facilitate reliable usage of cloud-based services. A cloud customer demands not only *availability* of services from a provider, but also expects that the services should persist to the guaranteed quality levels. In any SLA, service guarantees are given in form of *service level objectives (SLOs)*. These SLOs are objectively measurable conditions for services and are expressed in terms of SLA parameters. Some examples of SLOs are as follows:

- Availability of a service X is 99.9%
- Response time of a database query Q is between 3 to 5 seconds
- Throughput of a server S at peak load time is 0.875

Here, *availability*, *response time*, and *throughput* are the high-level SLA parameters. In a shared environment, like cloud, where competitive businesses with strong conflicts of interest co-reside, additional motives to access confidential information becomes prominent [1]. Under such situation, even if a cloud provider is trusted, one or more customers

[4] http://ebay.com
[5] http://www.epinions.com/.
[6] http://www.amazon.com/
[7] http://slashdot.org

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

may behave maliciously (misbehaves), leading to *reputation fate sharing* [1]. Therefore, it is essential that a cloud provider must be competent to ensure security and proper isolation of resources so that cloud customers can reliably outsource their businesses onto cloud.

Not many works have been reported on trust establishment in cloud computing. Some works [2] [17] point out the requirement of considering multiple-attributes for trust computation in cloud environment. These attributes are certificates, user statements, provider statements, expert assessments, *NIST* recommendations. In [18] [3], motivation for requirement of trust in cloud environment has been discussed, while [1] [19] identified trust management as a new research challenge in cloud domain.

A summary of different trust models in context of cloud computing has been presented in Table I. It is evident from Table I that most of the works have not presented mathematical formulation of their trust or risk models. In [26], some results have been given, however, the motivation is different. Works on selection of web services [28] [29] based on QoS and trust are available in the literature. Moreover, Buyya *et al.* [30] proposed a framework that prioritizes cloud services based on measured service quality levels. These works focus on selecting resources (e.g., service, products, etc.) by modeling their reputation. On contrary, our work aims at modeling the reputation of people or agents, and make selection decision on the basis of risk of interaction. Therefore, based on the following limitations of reported works on cloud-based trust model and service level agreement, we form the motivation of this work:

- No work addresses the issue of selecting trustworthy service provider in cloud marketplace.
- Estimation of risk of outsourcing a business onto third-party cloud has not been handled in reported works.
- Models proposed in reported works lack experimentation and analysis.
- In the state-of-the-art cloud, the security guarantees and responsibilities are specified in SLAs. However, vague clauses and unclear technical specifications of SLAs make selection of service provider difficult for customers [2].
- Transparency of provider's SLA [31] is one of the provisions to deduce competence. We have used this approach in the present work to estimate cloud provider's competence.

III. SelCSP Framework

In this section, a framework, termed as SelCSP, has been proposed to facilitate customers in selecting an ideal cloud service provider for business outsourcing. Figure 1 depicts different modules of the framework and how these modules are functionally related. As evident in Figure 1(a), the dotted boundary region denotes the SelCSP framework which acts as a third-party intermediator between customers and cloud service providers (CSPs).

SelCSP framework provides APIs through which both customers and providers can register themselves. After registering, customer can provide trust ratings based on interactions with provider. Cloud provider needs to submit its SLA to compute competence. At present, verifying the correctness of submitted ratings or sanitizing the erroneous data in the framework is beyond the scope. We assume that only registered customers can provide referrals/feedbacks and they do not have any malicious intents of submitting unfair ratings. Various modules constituting the framework are as follows:

1) *Risk Estimate*: It estimates perceived interaction risk relevant to a customer-CSP interaction by combining trustworthiness and competence.
2) *Trust Estimate*: It computes trust between a customer-CSP pair provided *direct interaction* has occurred between them.
3) *Reputation Estimate*: It evaluates reputation of a CSP based on *referrals/feedbacks* from various sources and computes the belief a customer has on former's reputation.
4) *Trustworthiness Computation*: Function to evaluate a customer's trust on a given CSP.
5) *SLA Manager*: This module manages SLAs from different CSPs. It takes into account different recommendations/standards and controls which are supposed to be satisfied by the SLAs.
6) *Competence Estimate*: It estimates competence of a CSP based on the information available from its SLA.
7) *Competence Computation*: It computes transparency with respect to a given SLA and hence evaluates the competence of the CSP.
8) *Risk Computation*: It computes perceived interaction risk relevant to a customer-CSP interaction.
9) *Interaction ratings*: It is a data repository where customer provides feedback/ratings for CSP.

The broad objective of SelCSP framework is to evaluate risk involved in interacting with different cloud service providers. Risk evaluation is done by computing trust which a customer has on a particular provider and transparency obtained from latter's service level agreement guarantees. For clear understanding, a high-level functional overview of the framework has been presented in Figure 1(b).

The *risk estimate* block receives customer request regarding estimation of interaction risk for a provider. This block delegates the request to *relation risk* and *performance risk* blocks to compute trustworthiness and competence of the provider, respectively. The *relational risk* block checks if the requester has previous interaction ratings with the provider. If such ratings are available, trust is calculated, otherwise feedback-based reputation is computed, both eventually leads to estimation of trustworthiness. In contrast, performance risk is computed by evaluating the transparency of provider's SLA guarantees. Finally, trustworthiness and competence gives a measure of interaction risk through *compute: interaction risk* block.

IV. Risk Estimation

In this work, our objective is to support cloud customers to reliably identify an "ideal" cloud provider for outsourcing. The term "ideal" implies that the service providing agent is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

TABLE I
SUMMARY OF THE CLOUD TRUST MODELS

Reference	Remarks	ModelsProposed	Experiment&Validation
Sato *et al.* 2010 [20]	Two types of trust introduced: *internal trust* & *contracted trust*.	No mathematical model presented	No experiment or validation done.
Schryen *et al.* 2011 [21]	Trust is measured in distributed systems with respect to two security requirements: (i) availability and (ii) anonymity. For achieving availability, k out of N entities need to show trustworthiness, while to achieve anonymity, 1 out of N entities has to be trustworthy.	Trust model has been proposed using propositional logic and probability theory.	No experimental results have been presented to claim validity.
Abbadi *et al.* 2012 [22]	Establishes chain of trust between customer and *virtual control center (VCC)* to facilitate secure manageability	No trust model.	Experimental results have not been presented.
Arias-Cabarcos *et al.* 2012 [23]	Security implications involved in federation of cloud and evaluates risk	No mathematical risk model presented.	No experimental results given.
Li *et al.* 2010 [24]	Proposes a design of multi-tenancy trusted computing environment model (MTCEM) to provide a trusted computing environment and separation of duty function.	No model given	No experimental result shown to illustrate the effect of MTCEM on system performance and validation about practical feasibility.
Alhamad *et al.* 2011 [25]	Model based on: scalability, availability, security, and usability. A fuzzy-set theoretic approach has been followed, where trust is assigned based on the values of four dimension, using Sugeno Fuzzy Inference System.	Mathematical modeling has not been presented	Experimental results have been given. However, they lack analysis and the authors do not make any claim regarding the validity of their approach.
Noor *et al.* 2011 [26]	Trust-as-a-Service (TaaS) framework to distinguish between credible trust feedbacks and malicious feedbacks by considering cloud service consumers' capability and majority consensus of their feedbacks.	Model has been proposed	Approaches have been validated by the prototype system and experimental results.
Abbadi *et al.* 2011 [18]	Five properties on which operation trust of a cloud provider will depend: adaptability, resilience, scalability, availability, and reliability.	No model proposed	No experimental results provided.
Li *et al.* 2009 [27]	Model can compute trust of a provider. If the computed trust exceeds a threshold, entities will initiate transaction. Trust value can be updated following re-evaluation after every transaction	The paper does not present the mathematical model of trust as well as how it gets updated.	Some results have been given to establish higher accuracy of the model, but lacks analysis.
Proposed work	The current work proposes a framework which facilitates risk-based cloud service provider selection by combining its trustworthiness and competence. The motivation is to support the customers in reliably identifying an "ideal" service provider.	Mathematical models for trust, reputation, competence, and risk estimation schemes have been provided.	Experimental results have been provided. Validity of the models have been claimed through publicly available dataset and reported works.

trusted as well as competent enough to provide secure and guaranteed service. This results in low perceived interaction risk.

In [32], the authors have identified total perceived interaction risk as a sum of *relational risk* and *performance risk*. That is,

$$\mathcal{R} = \mathcal{R}_r + \mathcal{R}_p \tag{1}$$

where, $\mathcal{R}_r$ denotes relational risk and $\mathcal{R}_p$ is performance risk.

In [32] [33], definitions of relational and performance risks are given as follows:

- *Relational risk*: It is defined as the probability and consequence of not having satisfactory cooperation. This risk arises because of potential opportunistic behavior on part of both stakeholders (consumer and provider).
- *Performance risk*: It is defined as the probability and consequences that alliance objectives are not achieved despite satisfactory cooperation among the partner firms.

In context of cloud computing, alliance objective implies adhering to negotiated SLA guarantees (for both provider and customer) and quick recovery from failures, such that the failover period is minimal and all data is restored.

According to [34], formal definition of risk is as follows:

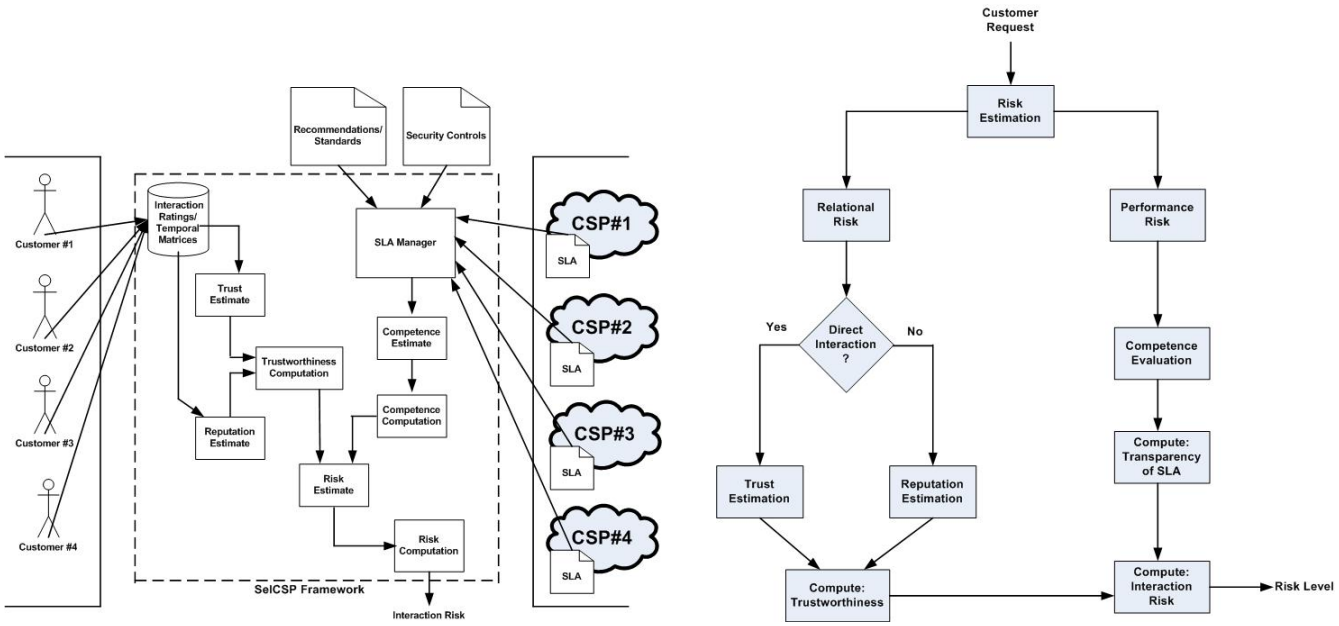
Definition 1: (Risk). Risk is defined as a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization.

We interpret probability and consequence in contexts of relational and performance risks as:

- *Probability*: likelihood of an asset being compromised, which depends either on opportunistic behavior (relational risk) of the alliance or commercial/technological/strategic hazards (performance risk) in course of multi-agent cooperation.
- *Consequence*: it is the impact generated following an adverse event (unauthorized usage/disclosure of resources) on the organization and is a function of the value of resource being compromised.

Therefore, from the definition of relational risk, it is evident that degree of such risk increases if there is lack of trust among the cooperating agents. Conversely, opportunistic behavior of partner firms will be reduced if there exists a trust relationship

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing



(a) SelCSP Modules

(b) Functional Relationship among SelCSP Modules

Fig. 1. SelCSP Framework and Module Interactions

between them. This assumption becomes more prominent by the following proposition [32].

Proposition 1: A customer's trust on a service providing agent reduces former's perceived relational risk in an interaction.

Trust generates faith, good intentions, and integrity which reduces the perceived likelihood of opportunistic behavior.

Similarly, competence of a cooperating agent is its ability to do appropriate things which leads to low perceived performance risk. Therefore, to achieve alliance objectives, cooperating firms must be competent. This argument is supported by the following proposition [32].

Proposition 2: Perceived performance risk in an interaction will be reduced if competence of service providing agent is high.

Competence of a cooperating agent gives a sense of confidence that the partner firm is capable of accomplishing a given task successfully.

Proposition 1 can be represented as:

$$\mathcal{R}_r(c_j, p_k) \propto \frac{1}{\mathcal{T}(c_j, p_k)} \tag{2}$$

where, c_j is j^{th} customer who wishes to interact with k^{th} cloud service provider p_k, $\mathcal{T}(c_j, p_k)$ is the trust which c_j has on p_k.

Similarly, Proposition 2 is as follows:

$$\mathcal{R}_p(c_j, p_k) \propto \frac{1}{\mathcal{C}(p_k)} \tag{3}$$

where $\mathcal{C}(p_k)$ is the competence of provider p_k.

From equations (2) and (3), we model risk as:

$$\mathcal{R}(c_j, p_k) = \kappa_1 . \frac{1}{\mathcal{T}(c_j, p_k)} + \kappa_2 . \frac{1}{\mathcal{C}(p_k)} \tag{4}$$

κ_1, κ_2 are the proportionality constants.

In [33], the authors stated that rational motive behind opportunistic behavior depends on the *context of interaction*. Relational risk in any alliance increases if one of the partners finds it difficult to protect its proprietary resources from others. Intuitively, any proprietary resource is very important from an organizations perspective, as it contains organizational "know-how", and its unauthorized disclosure or misuse causes noteworthy damage. Therefore, the requirement of trustworthy relation becomes high, if the context of interaction has significant *importance* to the customer.

In contrast, performance risk related to multi-party cooperation becomes high, if the consumer agent expects higher return on investment (or utility) from non-recoverable investments made towards an alliance with strategic objectives. In [35], authors observed that decision-makers use potential gains and losses to estimate risk, which implies that a higher non-recoverable investment leads to the perception of higher performance risk.

We observe that *context importance* and *utility benefits* have been used in a previous risk model [36]:

- *Importance*: Function $\mathcal{I}_{c_j}(\alpha)$ computes the degree of importance of context α from customer c_j's perspective. It is an agent-centered or subjective judgment of any context and has the values within the range (0, +1]. This implies that every context has some, however negligible, importance. The concept of *negative importance* has been discarded to support the assumption that agents interact

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

among themselves expecting to get the job done.

- *Utility*: Function $\mathcal{U}_{c_j}(\alpha)$ measures the amount of utility customer c_j is expected to gain from the context α. The utility of any context will be estimated from a *benefit-cost* ratio and has the values strictly within the interval [0, +1].

Based on the above arguments, we incorporate context importance and utility benefits in Equation (4):

$$\mathcal{R}(c_j, p_k) = \mathcal{I}_{c_j}(\alpha).\frac{1}{\mathcal{T}(c_j, p_k)} + \mathcal{U}_{c_j}(\alpha).\frac{1}{\mathcal{C}(p_k)} \quad (5)$$

Hence, we summarize the contribution of this section as: identifying the entities for perceived interaction risk as: (i) relational risk, (ii) performance risk, developing their mathematical forms, and establishing relationship between context importance and relational risk, and utility benefits and performance risk. In following sections, trust and competence estimating schemes have been described to formally define the proposed risk model.

V. Trust Estimation

Reliability of an entity cannot be estimated by traditional hard security mechanisms: *authentication* and *access control*, two central aspects of information and system security [37]. The reason is, in a distributed environment like cloud, where customers are not aware of service or resource provider's reliability, the latter may act deceitfully by providing false or misleading information related to service quality levels [11]. Interestingly, the problem of providing security has reversed, and we have to protect cloud customers rather than resource providers. In this scenario, soft security mechanisms like trust and reputation can provide protection against such threats [37].

Trust is a socio-cognitive phenomenon which has a wide range of definitions proposed by different researchers. It is a subjective view of a customer on a provider which is usually gained from personal experiences obtained through direct interactions, taken place in the past. We assume reliability of a service provider to be *context or situation-sensitive*. This is because, a provider may behave differently under varying contexts, and such behavior is largely independent of one another.

In a highly dynamic environment, like cloud, where the network, services, requests, and the actor base (providers, customers, etc.) change frequently, static trust value is meaningless. Also trust value calculated for one context may not be suitable to be used for another context. Moreover, it is impossible to derive whether *an authenticated provider who was proved to be trusted previously, is still reliable enough for interaction under the same or different context*. Hence, trust estimation must take into account context-awareness and dynamic nature to realize real-world interaction scenarios. Before describing the trust estimation scheme, some of the factors on which trust depends [38] [36] have been presented below:

- *Temporal window*: Trust associated with an entity is dynamic and changes over time. For trust calculation, interactions which have taken place within a predefined *time window* will only be taken into consideration. Time is an intrinsic variable and can be denoted with an ordered discrete set τ of time values, such that, $t_i \in \tau$, $i \in N$, $t_{i-1} < t_i$.
- *Context*: Context defines the scope of interaction between provider/consumer agents. It refers to services which are offered by cloud provider. These services are used by customers to accomplish their tasks. Based on the type of cloud service delivery model, context of interaction will vary. We present some contexts specific to different service delivery models below [39]:
  1) *Infrastructure-as-a-Service (IaaS)*: backup and recovery, instances for computation, content delivery networks (CDN), service management, storage
  2) *Platform-as-a-Service (PaaS)*: development environment, database, testing, integration, deployment
  3) *Software-as-a-Service (SaaS)*: email and office suite, collaboration, customer relation management (CRM), document management, social networks, enterprise resource planning (ERP)

  Each of these contexts may be having multiple granular sub-contexts on which cloud-based interactions may take place. However, in the present work, we focus only on broad contexts.
- *Trust domain* : Trust domain contains five qualitative elements or states of trustworthiness: *distrusted (D)*, *partially distrusted (PD)*, *undecided (U)*, *partially trusted (PT)*, and *trusted (T)*. The respective quantitative ratings lie in the closed interval $[0, 2]$: $\mathbb{D} = \{0, 0.5, 1.0, 1.5, 2.0\}$
- *History of interaction*: A history of interaction H on any context α_i observed during the temporal window τ with N time values, will have cardinality $|H| = N$ and is given by a set of ratings $\delta_1, \delta_2, \ldots \delta_N$, such that $\forall \delta_i \in H : \delta_i \mapsto \mathbb{D}$.

A formal definition of our trust estimation scheme is as follows:

Definition 2: (General trust vector). Given a customer c_j that will compute trust on provider p_k before interaction, a general trust vector model GTV is a seven-tuple GTV = (P, A, I, $\mathbb{D}$, τ, $\mathcal{F}$, $\mathcal{G}$), where P is a set of providers from which c_j will select to interact, A is a set of contexts over which previous interactions have occurred, I is an interaction matrix which belong to customer c_j, $\mathbb{D}$ is the trust domain, τ is the predefined temporal window, $\mathcal{F}$ is a probability distribution function following which the expected trust degrees will be assigned, and $\mathcal{G}$ is a function to evaluate the general trust vector.

Following any interaction between customer c_j and provider p_k on a context α_i, the former gives ratings from trust domain $\mathbb{D}$. All such ratings related to context α_i assigned during temporal window τ are stored as history of interaction H. Trust on p_k is computed by assigning probability values to different trust ratings. Assignment of probability values is done following distribution function $\mathcal{F}$. Distribution of such probabilities can be defined in a number of ways. In the present work, we take it as probability of occurrences of different ratings. For example, if there are N number of time values in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

history, and three different trust ratings from $\mathbb{D}$ have been assigned p, q, and r times (such that, $p+q+r=N$), then probabilities of occurrences are given as $\frac{p}{N}$, $\frac{q}{N}$, and $\frac{r}{N}$ respectively.

For each customer, SelCSP framework maintains an interaction matrix I. It contains trust scores computed from ratings assigned by the customer to different providers for interactions occurring over various contexts. Formally, interaction matrix is defined as:

Definition 3: (Interaction matrix). Interactions in a cloud environment with $|P|$ service providers over $|A|$ contexts is represented in a matrix I, where any element $\mu_{c_j}(p_k, \alpha_i)$ indicates the expected degree of trust that the customer c_j has on provider p_k with respect to context α_i. If there is no interaction with a provider on a particular context, it is indicated by $-\infty$.

Interaction matrix for customer c_j is given as:

$$I_{|P|\times|A|}(c_j) = \begin{bmatrix} \mu_{1,1} & \mu_{1,2} & \cdots & \mu_{1,|A|} \\ \mu_{2,1} & \mu_{2,2} & \cdots & \mu_{2,|A|} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{|P|,1} & \mu_{|P|,2} & \cdots & \mu_{|P|,|A|} \end{bmatrix}$$

Each element in matrix I is computed from ratings given in history of interaction H. Trust ratings in H occur in increasing order of recency i.e., if $u > v$, δ_u is a more recent rating than δ_v for any provider p_k over context α_i. The general trust vector computes a weighted sum of trust degrees acquired during different time instants of temporal window. We have considered an exponential decay function as weighing factor, which assigns higher weightages to the recent interactions, and is given as:

$$\omega = e^{-\gamma(|\tau|-t)} \tag{6}$$

where, $\gamma \in [0, \infty]$, and $t \leq |\tau|$.

Expected degree of trust on provider p_k during τ over context α_i is given as:

$$\mu_{c_j}(p_k, \alpha_i) = \sum_{l=1}^{|\tau|} \omega_l . \delta_l . \mathcal{F}(\delta_l) \tag{7}$$

Where, $\delta_l \in \mathbb{D}$ is the rating assigned on l^{th} time interval in H and probability values are given by the distribution function $\mathcal{F}(\delta_l)$.

GTV model is applicable when the following condition is satisfied:

- Customer c_j has interacted with the provider p_k over a context similar or identical to current context α_i at some time within the time window. Mathematically, it is given by:

  C1: $|H^{\tau}_{c_j}(p_k, \alpha_i)| \neq 0$

  This implies that history of interaction $H^{\tau}_{c_j}(p_k, \alpha_i)$ contains at least one element suggesting that agents have interacted over the current context. This can be represented as:

  $$\exists \alpha_i \in A : \mu_{c_j}(p_k, \alpha_i) \neq -\infty$$

Therefore, the general trust vector for provider $p_k \in P$ from customer c_j's perspective is a mean of expected trust degrees acquired for different contexts:

$$\mathcal{G}^{\tau}(c_j, p_k) = \begin{cases} \frac{1}{|A|}\sum_{\alpha_i \in A} \mu_{c_j}(p_k, \alpha_i) & \text{if } C1 \text{ is true} \\ -\infty & \text{otherwise} \end{cases} \tag{8}$$

Where, $|A|$ is the number of contexts on which interactions have been observed.

In the next section, we describe a reputation estimation mechanism which enables a customer to compute a provider's trustworthiness in absence of direct interaction. The contributions of this section are formally defining trust estimation scheme and presenting the mathematical form of expected degree of trust.

VI. Reputation Estimation

Reputation model comes into effect when customer c_j has not interacted with provider p_k on current context in the past. Under this situation, c_j has to believe in feedbacks/referrals from other customers who have directly interacted with p_k. We denote a customer providing feedback as a "witness" from c_j's viewpoint. Feedbacks from various witnesses are to be combined to obtain a global reputation score for any provider. Such referrals from different sources may not crisply declare a provider's reputation as "trusted" or "distrusted" following any boolean function. If degree of belief of a provider being trusted is $bel(t)$, then $(1 - bel(t))$ does not necessarily imply degree of belief that the agent is distrusted. Therefore, apart from an hypothesis (e.g., provider is trusted) being true or false, there may exist an element of uncertainty or ignorance, known as universal hypothesis. Classical probability theory cannot realize the element of uncertainty associated with an event [40]. We have chosen *Dempster-Shafer (DS) theory of evidence* [41] [42] to address this uncertainty issue. It allows an explicit representation of ignorance and combination of evidence [43]. Motivation behind using this model is that it is well-understood, mathematically sound, provides a formal framework for combining sources of evidences, and captures the uncertainty or universal hypothesis, which is largely prevalent while computing reputation of an entity.

Dempster-Shafer belief model [40] defines a set of possible situations which is called the *frame of discernment*. If Θ is the frame of discernment, then the power set $2^{|\Theta|}$ contains the elementary/atomic sets and all possible union of atomic sets, including Θ. In our work, we form individual frame of discernments for each element from the trust domain $\mathbb{D}$ (refer to Section V). The elementary states in these frames are the trust element itself and its *negation*. Therefore, frame of discernments considered in our framework are:

1) $\Theta_T = \{T, \neg T\}$
2) $\Theta_{PT} = \{PT, \neg PT\}$
3) $\Theta_U = \{U, \neg U\}$
4) $\Theta_{PD} = \{PD, \neg PD\}$
5) $\Theta_D = \{D, \neg D\}$

The power set for all of the above frame of discernments contains three non-null sets, for instance, $Pow(\Theta_T) = 2^{|\Theta_T|} = \{T, \neg T, (T, \neg T)\}$.

SelCSP framework evaluates two types of beliefs to compute reputation of any provider p_k:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

- *State-based belief*: It is the belief which c_j has on a given state of trustworthiness with respect to p_k's reputation.
- *General belief*: It is the overall belief that c_j has towards p_k's global reputation.

For ease of reference, we will use the notation d_i to represent the i^{th} element in trust domain $\mathbb{D}$ and the corresponding frame of discernment as Θ_{d_i}. Let W be the set of witnesses registered to our framework. SelCSP computes belief, disbelief, and uncertainty measures of any witness $w_j \in W$ regarding the hypothesis: "reputation of p_k is d_i" as [15] [40]:

$$\begin{aligned}\chi^{p_k}_{w_j}(d_i) &= m^{w_j}_{\Theta_{d_i}}(\{d_i\})\\ \chi^{p_k}_{w_j}(\neg d_i) &= m^{w_j}_{\Theta_{d_i}}(\{\neg d_i\})\\ \chi^{p_k}_{w_j}(d_i, \neg d_i) &= m^{w_j}_{\Theta_{d_i}}(\{d_i, \neg d_i\})\end{aligned} \tag{9}$$

where, $m^{w_j}_{\Theta_{d_i}}(\{d_i\})$ is the belief mass adopted by the witness w_j.

Belief mass assignment (BMA) of an atomic set $x_i \in 2^{|\Theta|}$ is interpreted as the degree of belief in assuming the state in question to be true. BMA on a non-atomic state $x_j \in 2^{|\Theta|}$ (formed by the union of two or more atomic sets) is interpreted as the belief that one of the elementary states it contains is true, but the observer is uncertain about which of them is true [15].

In SelCSP framework, belief mass assignment is evaluated from trust ratings given by witnesses, obtained from respective history of interaction H. For example, if any witness w_j has assigned rating corresponding to state d_i for p times, out of N interactions on different time intervals, BMA is computed following the reputation model proposed in [15] [44]:

$$m^{w_j}_{\Theta_{d_i}}(\{d_i\}) = \frac{p}{N+2} \tag{10}$$

Evaluation of uncertain measure is done as:

$$m^{w_j}_{\Theta_{d_i}}(\{d_i, \neg d_i\}) = \frac{2}{N+2} \tag{11}$$

Therefore, using Equations (10) and (11), disbelief measure is given as:

$$m^{w_j}_{\Theta_{d_i}}(\{\neg d_i\}) = 1 - (m^{w_j}_{\Theta_{d_i}}(\{d_i\}) + m^{w_j}_{\Theta_{d_i}}(\{d_i, \neg d_i\}) \tag{12}$$

Belief, disbelief, and uncertain measures for other witnesses can be computed using Equations (10), (12), and (11).

Overall belief towards provider p_k on state d_i from customer c_j's viewpoint is given by *Dempster's rule of combination* [43]. It aggregates two independent bodies of evidences (i.e. having different belief mass assignments) defined within the same frame of discernment by introducing an *orthogonal sum operator ($\bigoplus$)* [43].

Definition 4: (Dempster's rule of combination). Let β_1 and β_2 be local belief functions of two sources over Θ, with the belief mass assignments m^1_Θ and m^2_Θ respectively. If the atomic sets be given as $x_1, x_2, \ldots, x_k$ and $y_1, y_2, \ldots, y_l$ respectively, then the combined BMP $m^{1,2}_\Theta = m^1_\Theta \bigoplus m^2_\Theta : 2^{|\Theta|} \mapsto [0,1]$ is defined by:

$$m^{1,2}_\Theta(\Phi) = 0$$

$$m^{1,2}_\Theta(x) = m^1_\Theta(x) \bigoplus m^2_\Theta(x) = \frac{\sum_{i,j,x_i \cap y_j = x} m^1_\Theta(x_i).m^2_\Theta(y_j)}{1 - \sum_{i,j,x_i \cap y_j = \phi} m^1_\Theta(x_i).m^2_\Theta(y_j)}$$

In this work, we use the orthogonal sum operator as:

$$\mathcal{S}^{p_k}_{c_j}(d_i) = \chi^{p_k}_{w_1}(d_i) \oplus \chi^{p_k}_{w_2}(d_i) \oplus \ldots \oplus \chi^{p_k}_{w_{|W|}}(d_i) \tag{13}$$

Similarly overall disbelief measure towards state d_i from c_j's perspective is given as:

$$\mathcal{S}^{p_k}_{c_j}(\neg d_i) = \chi^{p_k}_{w_1}(\neg d_i) \oplus \chi^{p_k}_{w_2}(\neg d_i) \oplus \ldots \oplus \chi^{p_k}_{w_{|W|}}(\neg d_i) \tag{14}$$

Function $\mathcal{S}^{p_k}_{c_j}(d_i)$ and $\mathcal{S}^{p_k}_{cj}(\neg d_i)$ are used to compute the reputation towards provider p_k over state of trustworthiness d_i. We term this as *state-based reputation vector* as it computes the reputation score pertaining to a specific hypothesis (i.e. if a given state of trustworthiness is true/false). These functions, in reality, contradict the general belief on the agent and their difference will give state-based reputation [14]. Hence,

$$\xi^{p_k}_{c_j}(d_i) = \mathcal{S}^{p_k}_{c_j}(d_i) - \mathcal{S}^{p_k}_{c_j}(\neg d_i) \tag{15}$$

A formal definition in support of this reputation evaluation scheme is as follows:

Definition 5: (State-based reputation vector). Given a customer c_j that wants to compute the reputation of a provider p_k, a state-based reputation vector model $SREPUTE$ is a four-tuple $SREPUTE$ = ($\mathcal{S}$, d_i, $\mathbb{D}$, ξ), where $\mathcal{S}$ is a function that evaluates belief and disbelief measures, d_i is the state from the trust domain $\mathbb{D}$ under consideration, and ξ is a function to evaluate the state-based reputation vector.

For different elements in the trust domain, individual state-based reputation vectors are computed. Therefore, c_j's general belief on provider p_k's global reputation is given by the following model:

Definition 6: (Aggregated reputation vector). Given a customer c_j that wants to compute the reputation of a provider p_k, an aggregated reputation vector model $AREPUTE$ is a three-tuple $AREPUTE$ = (R, $\mathbb{D}$, π), where R is a set of state-based reputation vectors for states in $\mathbb{D}$, and π is a function that evaluates the overall reputation vector.

An unbiased approach is adopted in computing the overall reputation by taking a mean of the sum of all state-based reputation vectors. The function is given in Equation (16).

$$\pi(c_j, p_k) = \frac{1}{|\mathbb{D}|} \sum_{i=1}^{|\mathbb{D}|} \xi^{p_k}_{c_j}(d_i) \tag{16}$$

Combining Equations (8) and (16), trustworthiness of a service provider p_k as perceived by a customer c_j over temporal window τ is given as:

$$\mathcal{T}^\tau(c_j, p_k) = \begin{cases} \mathcal{G}^\tau(c_j, p_k) & \text{If } C1 \text{ is true} \\ \pi(c_j, p_k) & \text{Otherwise} \end{cases}$$

In the following section, we describe our approach towards estimating competence of service provider from its SLA guarantees. We revisit the contributions of this section as: estimation of belief on two types of reputation has been proposed: (i) state-based reputation, (ii) aggregated reputation, and formulating the corresponding mathematical equations.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

VII. Estimating Cloud Service Provider's Competence

In cloud marketplace, vendors negotiate service quality levels with customers by means of SLA. Different vendors offer different SLA structures, service offerings, performance levels, and negotiation opportunities. SLA can be used to select a service provider on the basis of data protection, continuity, and cost [45]. A typical SLA will contain the following [46]: (i) a set of services which the provider will deliver, (ii) a complete, specific definition of each service, (iii) responsibilities of the provider and the consumer, (iv) a set of metrics to measure whether the provider is offering the services as guaranteed, (v) exclusion clauses, (vi) an auditing mechanism to monitor the services, (vii) the remedies available to consumer and provider if the terms are not satisfied, and (ix) how SLAs will change over time.

Service qualities which provider guarantees to offer through SLA are measured by some metrics based on which its monitoring and auditing may be done. These metrics are known as *SLA parameters*. Each high-level SLA parameter is a function of one or more *key performance indicators (KPIs)* [47] [48] which are composed, aggregated, or converted to form the former. A precise and unbiased SLA helps to generate trust relationship among customer and provider. However, present day cloud SLAs contain vague clauses which do not convince the customers regarding assurances and compensations following a violation, if occurs [2]. Majority of cloud service providers guarantee "availability" of service. However, other than "availability" there exists other SLA parameters whose inclusion is necessary to render completeness to any SLA. This is because, consumers not only demand availability guarantee but also other performance related assurances which are equally business critical [49].

Therefore, it is essential to establish a standard set of parameters for cloud SLAs, since it reduces the perception of risk in outsourced services [31]. Based on the *QoS+* parameters proposed in [17] [2] in conjuncture with *Cloud Controls Matrix (CCM)* [50], we propose a set of SLA parameters whose transparency will enable customer to determine competence of any service provider (refer to Table II). We consider these parameters to be standard ones, and are valid across different cloud delivery models. For each parameter (in Table II), a number of low-level *controls* have been identified. According to NIST recommendations given in [51], cloud providers need to address these controls to implement the parameters. These controls meet the requirements derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures or organizational mission/business case needs. For a given parameter, all controls simultaneously need to satisfy the standards specified in [51]. Therefore, if a provider does not present relevant information about SLA parameters in terms of the recommended controls, we assumed that its SLA lacks transparency. In this work, transparency measures if the perception of risk in outsourced service gets reduced on the basis of standards, best practices, policies, procedures, and negotiated guarantees documented in service level agreement (SLA).

In SelCSP, we assign three qualitative attributes: *high, moderate,* and *low*, to denote transparency of controls. Such assignment is done at par with the *baseline* for different controls [51]. Security control baseline serves as the starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. For estimating the likelihood of any control being transparent, SelCSP assigns probability values to each of the qualitative categories: *1.0 for high, 0.5 for moderate, and 0.1 for low*. In ideal situation, any SLA is expected to contain the parameters given in Table II, however, their relevance varies with the type of services and guarantees the provider offers. Hence, to compute transparency of an SLA, as all parameters are not relevant for all service guarantees, we consider a balanced approach by taking the mean transparency of all parameters.

Overall competence ($\mathcal{C}$) of a service provider p_k in terms of any SLA ϕ is the mean of aggregated transparencies of all parameters (presented in Table II):

$$\mathcal{C}(p_k, \phi) = \frac{1}{n} \sum_{i=1}^{n} \lambda_{param_i}(\phi) \tag{17}$$

where, $param_i$ is the i^{th} parameter in the SLA ϕ, n is the total number of SLA parameters, $\lambda_{param_i}(\phi)$ is the transparency of parameter $param_i \in \phi$.

If it is assumed that the SLA of service provider will change over time, then a temporal constraint can be introduced in the following way:

$$\mathcal{C}^{t_i}(p_k, \phi) = \frac{1}{n} \sum_{i=1}^{n} \lambda^{t_i}_{param_i}(\phi) \tag{18}$$

where, t_i denotes the present time instant. To relate this with trust estimation scheme (discussed in Section V), we make $t_i \in \tau$.

Transparency of an SLA parameter depends on the probability values assigned by the SelCSP framework to its constituent controls. It is given by the following equation:

$$\lambda^{t_i}_{param_i}(\phi) = \prod_{j=1}^{m} \eta_j^{t_i}(\phi) \tag{19}$$

where, m represents the number of controls pertaining to the SLA parameter $param_i$, $\eta_j(\phi)$ is the probability value assigned to the j^{th} control at time t_i. Probability value assigned is either 1.0 or 0.5 or 0.1, corresponding to the qualitative categories high or moderate or low, respectively. All controls constituting a high level SLA parameter may or may not be relevant for different delivery models. For a given delivery model, if any control is irrelevant and hence, not provided, we will consider that its transparency has the default *low* qualitative attribute.

In Equation (5), we compute total interaction risk associated with a particular context of interaction, as a sum of perceived relational and performance risks. Relational risk is a function of customer's trust on service provider and importance of context. On contrary, performance risk is measured from competence of the provider, which in turn, is derived from

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

TABLE II
PROPOSED SLA PARAMETERS

Parameters	Controls
Security	User access authorization/restriction, User access revocation, Roles/Responsibilities, Segregation of duties, Encryption, Encryption key management, Vulnerability/Patch management, Anti-virus/malicious software, Audit tool access, Incident reporting, Network security, Remote user multi-factor authentication
Compliance	Audit planning, Independent audits, Third-party audits, Contract/authority maintenance, Intellectual property
Data Governance	Ownership, Classification, Handling/labeling, Retention policy, Secure disposal, Information leakage
Resiliency	Management Program, Impact analysis, Business continuity planning & testing, Environmental risks
Operations Management	Capacity/resource planning, Equipment maintenance

transparency of its SLA. Such risk is perceived to be high if a customer expects higher utility from present interaction. Substituting the expressions for trustworthiness and competence in in Equation (5), overall perceived interaction risk becomes,

$$\mathcal{R}^{t_i}(c_j, p_k, \phi, \alpha) = \mathcal{I}_{c_j}(\alpha).\frac{1}{\mathcal{T}^{\tau}_{c_j}(p_k, \alpha)} + \mathcal{U}_{c_j}(\alpha).\frac{1}{\mathcal{C}^{t_i}(p_k, \phi)} \tag{20}$$

where t_i is the current time instant such that $t_i \in \tau$ and $\mathcal{R}^{t_i}(c_j, p_k, \phi, \alpha)$ measures the level of interaction risk as perceived by customer c_j towards provider p_k in handling context α based on guarantees documented in SLA ϕ. The perceived interaction risk is normalized so that it acquires the values from the interval [0, 1].

It is evident from Equation (20), interaction risk becomes *infinite* if either trustworthiness ($\mathcal{T}^{\tau}_{c_j}(p_k, \alpha)$) or competence ($\mathcal{C}^{t_i}(p_k, \phi)$) or both becomes *zero*. Under this situation, for all practical purpose, perceived risk will attain maximum value (i.e. 1.0). Therefore, modified risk equation becomes:

$$\mathcal{R} = \begin{cases} 1 & \text{If } \mathcal{T}^{\tau}_{c_j}(p_k, \alpha) = 0,\ \mathcal{C}^{t_i}(p_k, \phi) = 0 \\ \mathcal{R}^{t_i}(c_j, p_k, \phi, \alpha) & \text{Otherwise} \end{cases}$$

We formally define interaction risk estimation mechanism as:

Definition 7: (Trust and Competence-based Risk). Given a customer c_j that wants to make decision regarding initiation of an interaction with a service provider p_k, a trust and competence-based risk estimator $TCRISK$ is a seven-tuple $TCRISK = (\alpha, \mathcal{I}, \mathcal{U}, \mathcal{T}, \mathcal{C}, \phi, \mathcal{R})$, where, α is the current context of interaction, $\mathcal{I}$ is the importance of the context subjective to c_j, $\mathcal{U}$ is the utility expected to be gained on context α by c_j, $\mathcal{T}$ is the degree of trustworthiness obtained by c_j towards p_k on context α, $\mathcal{C}$ is competence of p_k with respect to present SLA ϕ, and $\mathcal{R}$ is a function to evaluate the perceived interaction risk associated with p_k over context α.

For a given context, SelCSP computes interaction risk for all the service providers. A customer can choose ideal service provider for depleting their data and services by choosing the *minimum* value among them. In the next section, we describe a case study to demonstrate the usage of our framework, and analyze the results obtained from experiment to claim validity. Thus, in this section we propose SLA parameters and controls for cloud service delivery models, give a mathematical equation to evaluate transparency, and establish relationship between risk, trust, and competence.

VIII. RESULT AND DISCUSSION

We have implemented the proposed framework using *Java* programming language and have simulated the following case study to demonstrate provider selection mechanism through SelCSP.

A. Case Study

Let us consider that at present six SaaS cloud service providers (CSPs) are registered with SelCSP framework. The CSPs are denoted as *CSP1, CSP2, CSP3, CSP4, CSP5,* and *CSP6* respectively. A customer X, who is also registered with SelCSP, wants to choose ideal service providers for business outsourcing. The customer has set three qualitative levels for both *Importance* ($\mathcal{I}$) and *Utility* ($\mathcal{U}$) of a context: *high (H), medium (M), low (L)*. The values assigned to these levels are 0.95, 0.55, and 0.25 respectively. These values have been given as input to SelCSP framework. Combination of $\mathcal{I}$ and $\mathcal{U}$ produces nine different contexts of interaction given as: (a) email and office productivity, (b) billing, (c) customer relationship management (CRM), (d) collaboration, (e) content management, (f) document management, (g) human resources, (h) sales, and (i) enterprise resource planning (ERP). Now, X wants to determine which among the above six CSPs are ideal for different contexts, such that the former can serve its clients in a cost-effective and efficient manner. Under such situation, X requests SelCSP framework to recommend service provider which is both trustworthy as well as competent for a given context.

SelCSP estimates trustworthiness (refer Section VIII-B) and competence (refer Section VIII-C) for all the service providers under nine different contexts. Using the above estimates, perceived interaction risk is evaluated. It may be observed in Sections IV, V, and VI, that multiple parameters are required for risk, trust, and reputation estimates, respectively. However, a user does not have to input all these parameters. For example, in general trust vector scheme (Definition 2), there are six parameters, out of which user has to input only two (contexts and feedbacks) of them. State-based reputation vector (Definition 5) constitutes four parameters, and the user has to input only the particular state from trust domain.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

Most of these parameters which are to be input by user are either subjective or has to be chosen from a predefined set. For example, in risk estimation scheme (Definition 7), user inputs context from a set of contexts (A), while the values for importance ($\mathcal{I}$) and utility ($\mathcal{U}$) are given from subjective judgment.

Figure 2 shows the risk, trust, and competence values for all contexts mentioned above. As explained earlier, one of the objectives of our framework is to evaluate interaction risk of any service provider based on its trust and competence. Hence, under a given context, SelCSP recommends a provider with whom the risk of interaction is minimum. In Figure 2, we observe different risk values for each provider under varying context. Assuming that SelCSP will recommend service providers with minimal interaction risk, the following CSPs will be chosen for nine contexts:

- *CSP6*: for contexts (c), (d), (e), (g), and (i)
- *CSP1*: for contexts (b) and (f)
- *CSP4*: for context (a)
- *CSP5*: for context (h)

In the following subsections we discuss the methodology used to compute trust and competence and also attempted to validate our approach against publicly available data and reported works.

B. Validation of Trust and Reputation Estimations

In this section, we focus on validating and analyzing the behaviors of proposed trust and competence estimation schemes. Primary objective of our experiment is to establish the fact that the trust and competence values generated by SelCSP are similar to those generated by reported works. It acts as evidence that our evaluation sub-modules produce valid results, which eventually leads to generation of correct interaction risk-based recommendations towards different cloud service providers.

Epinions is a popular product review site that has a pool of individual reviewers who provide information in form of trust (-1 to 1) on other users and feedback ratings (1 to 5) on entities/items to help consumers in making better purchase decisions. In [52], the authors have collected ratings from Epinions and made them available in the public domain [8]. The data set has 49,290 users, 139,738 items, and 664,824 trust feedbacks. In SelCSP framework, we compute trustworthiness of a provider based on feedbacks from customers. Moreover, our framework also aims at supporting customers in selecting cloud provider based on interaction risk. Owing to these similarities, we have chosen Epinions dataset to validate our trust evaluation mechanism. Similar attempt by using Epinions data has also been observed in [26], where the authors have studied the performance of their *credibility model* in the context of providing feedbacks to cloud services.

We have selected six arbitrary entities from Epinions data set for our experiment. These entities correspond to CSPs considered in our case study (refer Section VIII-A). Each item has been rated by multiple users, within 1 to 5. Following the reputation model proposed in [15] [44], we consider ratings 1 and 2 to be penalty points and 3-5 to be reward points. Trust values of all six entities are evaluated using the above model. For computing the trust values through SelCSP framework from both direct interaction and witness feedbacks, we consider the following:

- Items 1 and 2: Direct interaction ratings available
- Items 3, 4, 5, and 6: Feedbacks/referrals from other sources are to be considered

In case of items 1 and 2, we assume that the ratings have been assigned at different time intervals, the first rating being the oldest one, and normalize them such that they take values from the interval [0, 2]. For a particular item, we take the probabilities of occurrences of different ratings as the distribution function. Taking temporal window $\tau = 10$ and weighing factor $\omega = 3.75$, the trust values are computed. For other items, we follow the model proposed in [15] [44], where belief mass is calculated from the number of reward and penalty points. Similar to previous approach, ratings 1 and 2 are penalties and 3-5 are rewards. Finally, these belief masses are combined and a reputation value is obtained. Comparison between two sets of trust scores are depicted in Figure 3. As

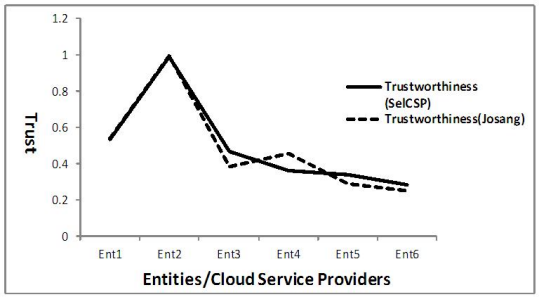


Fig. 3. Comparison of Trust

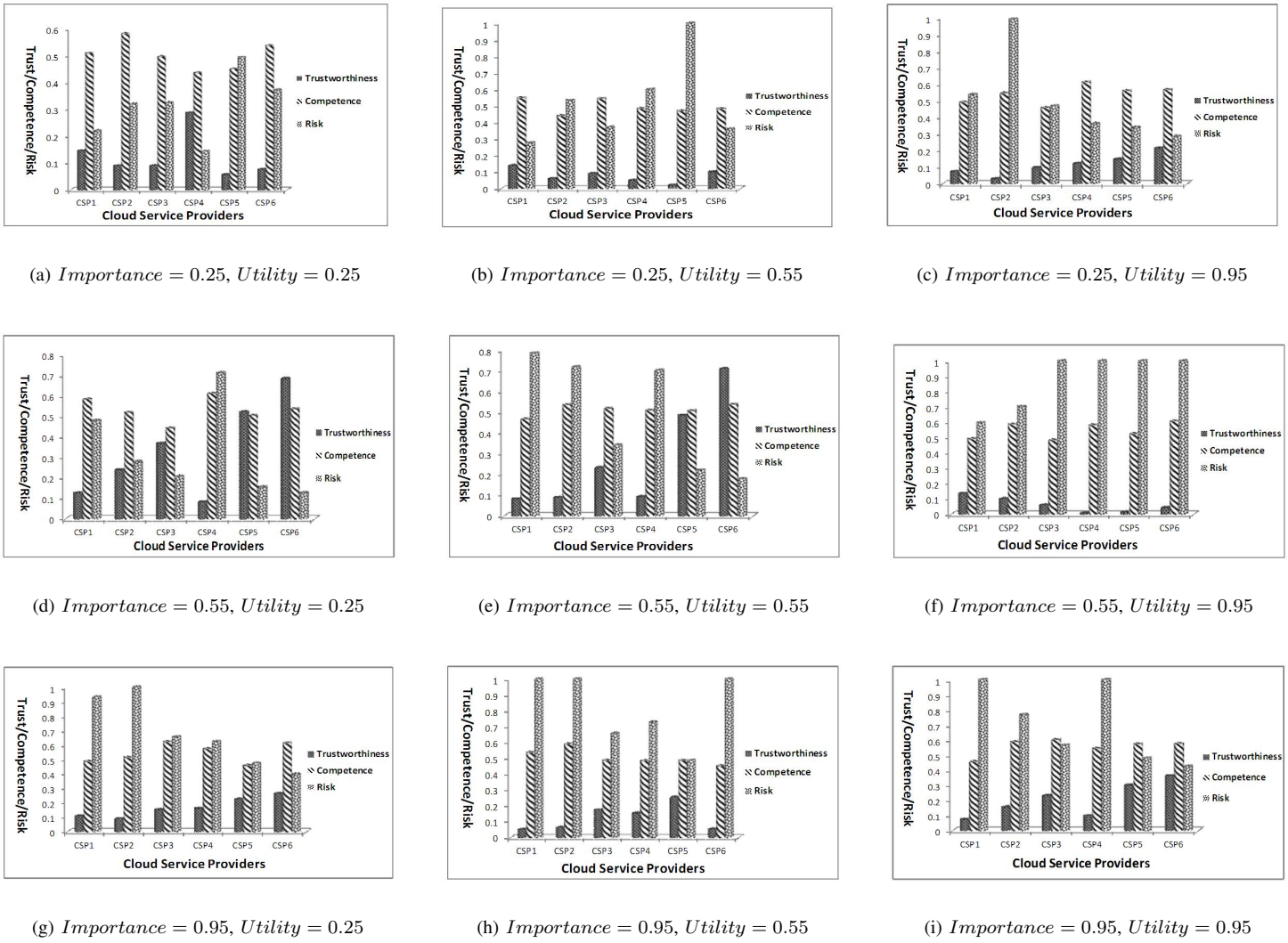
evident from Figure 3, trustworthiness measures obtained from Epinions as well as the ones generated by the proposed SelCSP framework, are more or less equivalent for most of the entities. For some entities (*Ent3* to *Ent6*), we observe that trust values are different. For all these entities, direct interaction ratings were not available and the framework has to depend on their reputations obtained from other sources. In practical sense, customers have higher trust on products which they have used in the past, than the ones on whose reputation they have to believe in.

C. Validation of Competence Estimation

In [31], the author has computed transparency of six independent cloud service providers from their self-service portals and published web contents. In this work, we use the same information and compute transparency with respect to SLA standards recommended by NIST. In ideal scenario, it is desirable that the service providers follow SLA standards recommended by NIST [50] [51]. However, in practical scenario, we find that these SLAs are customized to accommodate service provider's management policies. SLA related information available from their portals are customized according to our parameters and given as input to the SelCSP framework. Transparencies of

[8] http://www.trustlet.org/wiki/Downloaded_Epinions_dataset

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing



(a) $Importance = 0.25$, $Utility = 0.25$ (b) $Importance = 0.25$, $Utility = 0.55$ (c) $Importance = 0.25$, $Utility = 0.95$

(d) $Importance = 0.55$, $Utility = 0.25$ (e) $Importance = 0.55$, $Utility = 0.55$ (f) $Importance = 0.55$, $Utility = 0.95$

(g) $Importance = 0.95$, $Utility = 0.25$ (h) $Importance = 0.95$, $Utility = 0.55$ (i) $Importance = 0.95$, $Utility = 0.95$

Fig. 2. Variation of Trustworthiness, Competence, Risk under different Contexts

these CSPs obtained from [31] and SelCSP are plotted in Figure 4.

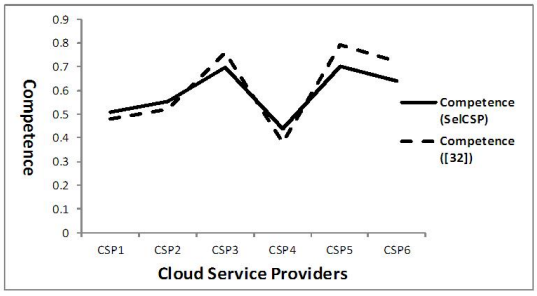


Fig. 4. Comparison of CSP Competence

As evident in Figure 4, competence values based on transparency of respective SLAs are almost similar for *CSP1*, *CSP2*, *CSP3*, and *CSP4*, whereas they vary in contexts of *CSP5* and *CSP6*. This variation in transparency is attributed by differences in the mode of assessment followed in two procedures. In [31], the scoring system is strictly binary and deals only with *security*, *privacy*, *external audits or certification*, and *service levels* offered by SLA. Moreover, while assessing these parameters, NIST recommendations and standards have not been taken into account. Whereas, in our competence estimation, SLAs are assessed based on NIST recommended SLA parameters and respective controls. It is also more granular in terms of assigning values for computing overall degree of transparency. Hence, owing to this stringent assessment, SLAs of *CSP5* and *CSP6* have been found to be less competent with respect to results presented in [31].

D. Analysis of Behavior of Estimation Schemes

In Sections VIII-B and VIII-C, we have attempted to validate our proposed trustworthiness and competence estimation mechanisms with respect to publicly available data and reported works. In this section, variation of trustworthiness, competence, and overall interaction risk under different contexts have been studied.

As observed in Figure 2, for each context, overall risk value rises if trustworthiness and/or competence of service providers diminishes and vice-versa. However, one significant observation is that even if two providers have similar competence, the one with higher trustworthiness yields lesser interaction risk. This trend has been detected in multiple contexts and for multiple service providers. From these observations, we convey that for interactions, *trusted providers with less competence* are preferable to *distrusted ones with higher competence*. This is attributed by the fact that *competent but distrusted* agents have the potential to cause damages of higher impact than the ones who are *trusted but incompetent*. For example, in the first case, customer's data/applications may be misappropriated leading to its business and goodwill loss. Whereas in the second case, it may be that data gets lost owing to provider's lack of disaster recovery strategy. However, in the second case, data may be recovered if backups are available either in provider or customer end. Hence, our risk-based provider selection scheme captures real-life interaction scenario, demonstrating how risk of interaction with providers varies with their trustworthiness and competence.

IX. Conclusion

Cloud computing is an evolving paradigm, where new service providers are frequently coming into existence, offering services of similar functionality. Major challenge for a cloud customer is to select an appropriate service provider from the cloud marketplace to support its business needs. However, service guarantees provided by vendors through SLAs contain ambiguous clauses which makes the job of selecting an ideal provider even more difficult. As customers use cloud services to process and store their individual client's data, guarantees related to service quality level is of utmost importance. For this purpose, it is imperative from a customer's perspective to establish trust relationship with a provider. Moreover, as customers are outsourcing their businesses onto a third-party cloud, capability or competence of CSP determines if former's objectives are going to be accomplished. In this work, we propose a novel framework, SelCSP, which facilitates selection of trustworthy and competent service provider. The framework estimates trustworthiness in terms of context-specific, dynamic trust and reputation feedbacks. It also computes competence of a service provider in terms of transparency of SLAs. Both these entities are combined to model interaction risk, which gives an estimate of risk level involved in an interaction. Such estimate enables a customer to make decisions regarding choosing a service provider for a given context of interaction. A case study has been described to demonstrate the application of the framework. Results establish validity and efficacy of the approach with respect to realistic scenarios. In future, we aim at using this risk-based provider selection to ensure secure multi-domain collaboration in cloud environment.

Acknowledgement

The authors would like to thank the anonymous reviewers for careful reviews and valuable suggestions that helped improve the quality of the manuscript. The work of N. Ghosh was partially supported by TCS Research Scholarship grant and that of S. K. Das by the US National Science Foundation grants under award numbers CNS-1355505, IIS-1404673 and CNS-1404677.

References

[1] Y. Chen, V. Paxson, and R. H. Katz, "What's New About Cloud Computing Security," University of California at Berkeley, USA, Tech. Rep. UCB/EECS-2010-5, 20 January 2010.

[2] S. K. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011, pp. 933–939, doi: 10.1109/TrustCom.2011.129.

[3] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," *IT Professional, IEEE Journals & Magazines*, vol. 12, no. 5, pp. 20–27, October 2010, doi: 10.1109/MITP.2010.128.

[4] J. Lin, C. Chen, and J. Chang, "Qos-aware data replication for data intensive applications in cloud computing systems," *IEEE Transactions on Cloud Computing*, vol. 1, no. 1, pp. 101–115, January-June 2013.

[5] D. Gambetta, "Can we trust trust?" in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. Department of Sociology, University of Oxford: Basil Blackwell, 1990, ch. 13, pp. 213–237, available at: http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf.

[6] D. H. Mcknight and N. L. Chervany, "The meanings of trust," Management Information Systems Research Center, University of Minnesota, Technical Report MISRC Working Paper Series 96-04, 1996.

[7] D. Manchala, "Trust metrics, models and protocols for electronic commerce transactions," in *18th International Conference on Distributed Computing Systems*, 1998.

[8] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *Second International Conference on Trust Management*, T. Dimitrakos, Ed., Oxford, March 2004.

[9] L. Freeman, "Centrality on social networks," *Social Networks*, vol. 1, pp. 215–239, 1979.

[10] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Communications Surveys and Tutorials*, vol. 3, 2000.

[11] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems, Elsevier*, vol. 43, no. 2, pp. 618–644, March 2007, doi:10.1016/j.dss.2005.05.019.

[12] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: empirical analysis of ebays reputation system," in *The Economics of the Internet and ECommerce*, ser. Advances in Applied Microeconomics, M. Baye, Ed., vol. 11. Elsevier Science, 2002, pp. 127–157.

[13] A. Withby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in bayesian reputation systems," in *7th International Workshop on Trust in Agent Societies (AAMAS04)*. ACM, 2004.

[14] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, ser. AAMAS '02. Bologna, Italy: ACM, July 2002, pp. 294–301, doi: 10.1145/544741.544809.

[15] A. Jøsang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–311, June 2001.

[16] J. Sabater and C. Sierra, "Regret: a reputation model for gregarious societies," in *4th International Workshop on Deception, Fraud and Trust in Agent Societies, in the 5th Int. Conference on Autonomous Agents (AGENTS01)*. Montreal, Canada: ACM Press, 2001, pp. 61–69.

[17] S. K. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," in *2010 7th International Conference on Ubiquitous Intelligence Computing and 7th International Conference on Autonomic Trusted Computing (UIC/ATC)*. IEEE Computer Society, 2010, pp. 410–415, doi: 10.1109/UIC-ATC.2010.48.

[18] I. M. Abbadi and A. Martin, "Trust in the cloud," *Information Security Technical Report*, vol. 16, no. 3, pp. 108–114, 2011, doi: 10.1016/j.istr.2011.08.006.

[19] H. Takabi, J. B. D. Joshi, and G. J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security and Privacy, IEEE Computer Society Digital Library*, vol. 8, no. 6, pp. 24–31, November/December 2010.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2014.2328578, IEEE Transactions on Cloud Computing

[20] H. Sato, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," in *Proceedings of 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT)*. IEEE, 2010, pp. 121–124.

[21] G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in *Proceedings of the 2011 ACM Symposium on Applied Computing*. ACM, 2011, pp. 1739–1745.

[22] I. M. Abbadi and M. Alawneh, "A framework for establishing trust in the cloud," *Computers & Electrical Engineering*, 2012.

[23] P. Arias-Cabarcos, F. Almenárez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero, "A metric-based approach to assess risk for on cloud federated identity management," *Journal of Network and Systems Management*, pp. 1–21, 2012.

[24] X. Li, L. Zhou, Y. Shi, and Y. Guo, "A trusted computing environment model in cloud architecture," in *Proceedings of 2010 International Conference on Machine Learning and Cybernetics (ICMLC)*, vol. 6. IEEE, 2010, pp. 2843–2848.

[25] M. Alhamad, T. Dillon, and E. Chang, "A trust-evaluation metric for cloud applications," *Proceedings of International Journal of Machine Learning and Computing*, vol. 1, no. 4, pp. 416–421, 2011.

[26] T. Noor and Q. Sheng, "Trust as a service: a framework for trust management in cloud environments," *Web Information System Engineering–WISE 2011*, pp. 314–321, 2011.

[27] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment," in *CloudCom 2009*, ser. LNCS. Springer-Verlag, Berlin/Heidelberg, 2009, vol. 5931, pp. 69–79.

[28] Y. Liu, A. H. Ngu, and L. Z. Zeng, "Qos computation and policing in dynamic web service selection," in *Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters*. ACM, 2004, pp. 66–73.

[29] E. M. Maximilien and M. P. Singh, "A framework and ontology for dynamic web services selection," *Internet Computing, IEEE*, vol. 8, no. 5, pp. 84–93, 2004.

[30] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012–1023, 2013.

[31] W. A. Pauley, "Cloud Provider Transparency: An Empirical Evaluation," *Security Privacy, IEEE*, vol. 8, no. 6, pp. 32–39, November/December 2010.

[32] T. K. Das and B.-S. Teng, "Trust, control, and risk in strategic alliances:an integrated framework," *Organization Studies*, vol. 22, no. 2, pp. 251–283, March 2001, doi: 10.1177/0170840601222004.

[33] T. K. Das and B. S. Teng, "Risk Types and Inter-firm Alliance Structures," *Journal of Management Studies*, vol. 33, no. 6, pp. 827–843, November 1996.

[34] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," National Institute of Standards and Technology (NIST), Technology Administration, US Department of Commerce, NIST Special Publication 800-30, July 2002.

[35] J. G. March and Z. Shapira, "Managerial perspectives on risk and risk taking," *Management science*, vol. 33, no. 11, pp. 1404–1418, 1987.

[36] S. P. Marsh, "Formalizing trust as a computation concept," Ph.D. dissertation, Department of Computing Science and Mathematics, University of Stirling, April 1994.

[37] L. Rasmusson and S. Jansson, "Simulated social control for secure internet commerce," in *Proceedings of the 1996 workshop on New security paradigms*, ser. NSPW '96. New York, NY, USA: ACM, 1996, pp. 18–25. [Online]. Available: http://doi.acm.org/10.1145/304851.304857

[38] D. Kovac and D. Trcek, "Qualitative trust modeling in soa," *Journal of System Architecture, Elsevier*, vol. 55, no. 4, pp. 255–263, April 2009.

[39] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "NIST cloud computing reference architecture," *NIST special publication*, vol. 500, p. 292, 2011.

[40] K. Sentz and S. Ferson, "Combination of evidence in dempster-shafer theory," Sandia National Laboratories, Albuquerque, New Mexico, Tech. Rep. SAND 2002-0835, April 2002.

[41] G. Shafer, *A mathematical theory of evidence*. Princeton university press Princeton, 1976, vol. 76.

[42] J. Gordon and E. H. Shortliffe, "The dempster-shafer theory of evidence," in *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project 3*, 1984, ch. 13, pp. 832–838.

[43] I. Ruthven and M. Lalmas, "Using dempster-shafer's theory of evidence to combine aspects of information use," *Journal of Intelligent Information Systems*, vol. 19, no. 3, pp. 267–301, November 2002, doi: 10.1023/A:1020114205638.

[44] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, 2002, pp. 41–55.

[45] K. Buck and D. Hanf, "Cloud SLA Consideration for Gevernment Consumer," System Engineering at Mitre, Tech. Rep. Case: 10-2902, September 2010, *Available at http://www.mitre.org/work/tech_papers/2010/10_2902/.*

[46] "Cloud Computing Use Cases White Paper - Version 4.0," July 2010, *Available at : http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper–4_0.pdf*, accessed on August 2011.

[47] I. Brandic, V. C. Emeakaroha, M. Maurer, S. Dustdar, S. Acs, A. Kertesz, and G. Kecskemeti, "LAYSI - A Layered Approach for SLA-Violation Propagation in Self-Manageable Cloud Infrastructures," in *Proceedings of the 2010 34th IEEE Annual Computer Software and Applications Conference Workshops (COMPSACW)*, 19–23 July 2010, pp. 365–370, *DOI : 10.1109/COMPSACW.2010.70.*

[48] V. C. Emeakaroha, I. Brandic, M. Maurer, and S. Dustder, "Low Level Metrics to High Level SLAs - LoM2HiS Framework:Bridging the Gap Between Monitored Metrics and SLA Parameters in Cloud Environments," in *Proceedings of International Conference on High-Performance Computing and Simulation (HPSC)*, June 28 – July 2 2010, pp. 48–54, *DOI : 10.1109/HPCS.2010.5547150.*

[49] G. S. Machado and B. Stiller, "Investigation of an SLA Support System for Cloud Computing (SLACC)," *PIK (Praxis der Informationsverarbeitung und Kommunikation)*, vol. 34, no. 2, pp. 80–86, June 2011, *DOI : 10.1515/piko.2011.014.*

[50] CSA, "Cloud controls matrix," https://cloudsecurityalliance.org/research/ccm/, September 2012.

[51] "Recommended security controls for federal information systems and organizations," National Institute of Standards and Technology (NIST), Computer Security Division, Information Technology Laboratory, NIST Special Publication 800-53 Revision 3, August 2009.

[52] P. Massa and P. Avesani, "Trust-aware bootstrapping of recommender systems," in *ECAI Workshop on Recommender Systems*, August, pp. 29–33.

Nirnay Ghosh is pursuing PhD from the School of Information Technology (SIT) under Indian Institute of Technology (IIT), Kharagpur, India. His broad area of research includes security in cloud computing, trustworthy selection of service provider for secure multi-domain interoperations. Prior to this, he received MS (by research) degree in Information Technology from Indian Institute of Technology, Kharagpur and BTech degree in Computer Science & Engineering from West Bengal University of Technology (WBUT), India. He has an IEEE student membership and published six international conference papers, one journal paper, and one book chapter during course of his MS program.

Soumya K. Ghosh is a Professor at the School of Information Technology, IIT Kharagpur. Prior to joining IIT Kharagpur, Dr. Ghosh worked for Indian Space Research Organization in the area of Satellite Remote Sensing and GIS. He did his M. Tech and PhD in Computer Science & Engineering from the Indian Institute of Technology (IIT) Kharagpur, India. His research interests include network security through attack modeling, formal verification of security policies, trust modeling, security in cloud computing, spatial information retrieval and knowledge discovery. He has published over 100 articles in journals and conference proceedings. He is a member of IEEE.

Sajal K. Das is the Chair of Computer Science Department and Daniel St. Clair Endowed Chair at the Missouri University of Science and Technology. Prior to that he was a Distinguished Scholar Professor of Computer Science and Engineering and the Founding Director of the Center for Research in Wireless Mobility and Networking (CReWMaN) at the University of Texas at Arlington (UTA). His current research interests include wireless and sensor networks, mobile and pervasive computing, cyber-physical security, distributed and cloud computing, biological and social networks, applied graph theory and game theory. Dr. Das has published more than 500 technical papers and 47 invited book chapters in these areas, holds five US patents, and received nine Best Paper Awards in international conferences.