Journal of Cloud Computing
a SpringerOpen Journal

REVIEW Open Access

Trust as a facilitator in cloud computing: a survey

Sheikh Mahbub Habib*, Sascha Hauke, Sebastian Ries and Max Mühlhäuser

Abstract

Cloud computing offers massively scalable, elastic resources (e.g., data, computing power, and services) over the internet from remote data centres to the consumers. The growing market penetration, with an evermore diverse provider and service landscape, turns Cloud computing marketplaces a highly competitive one. In this highly competitive and distributed service environment, the assurances are insufficient for the consumers to identify the dependable and trustworthy Cloud providers.

This paper provides a landscape and discusses incentives and hindrances to adopt Cloud computing from Cloud consumers' perspective. Due to these hindrances, potential consumers are not sure whether they can trust the Cloud providers in offering dependable services. Trust-aided unified evaluation framework by leveraging trust and reputation systems can be used to assess trustworthiness (or dependability) of Cloud providers. Hence, cloud-related specific parameters (QoS+) are required for the trust and reputation systems in Cloud environments. We identify the essential properties and corresponding research challenges to integrate the QoS+ parameters into trust and reputation systems. Finally, we survey and analyse the existing trust and reputation systems in various application domains, characterizing their individual strengths and weaknesses. Our work contributes to understanding 1) why trust establishment is important in the Cloud computing landscape, 2) how trust can act as a facilitator in this context and 3) what are the exact requirements for trust and reputation models (or systems) to support the consumers in establishing trust on Cloud providers.

Keywords: Cloud computing, Cloud taxonomy, Trust evaluation, Reputation system, Trust management, Trust models

Introduction

Cloud computing offers dynamic, scalable, shared, and elastic resources (e.g., computing power, storage, software, etc.) over the internet from remote data centres to the users (e.g., business organizations, government authorities, individuals, etc.). The opportunities afforded by cloud computing are too attractive for the consumers (which we also refer to as "customers") to ignore in today's highly competitive service environments (which we also refer to as "marketplaces"). The way to realizing these opportunities, however, is not free of obstacles.

The highly distributed and non-transparent nature of cloud computing represents a considerable obstacle to the acceptance and market success of cloud services. Potential users of these services often feel that they lose control over their data and they are not sure whether cloud providers can be trusted. Particularly, they are concerned and confused about the capabilities of Cloud providers [1]. Additionally, a recent survey [2], 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. The business market is growing rapidly with new players entering the Cloud computing marketplaces and it is expected that Cloud providers are going to compete for customers by providing services with similar primary functionality. However, there can be huge differences regarding the provided quality level of those services. Thus, there will be a need to reliably identify the dependable service providers in such a competitive marketplace [3]. The ability to do so will establish confidence of the consumers in adopting

*Correspondence: sheikh.habib@cased.de
Technische Universität Darmstadt/CASED, Telecooperation Group, Darmstadt, Germany

cloud-based services and support consumers in selecting the appropriate service providers.

Similar issues of establishing trust and confidence are already known from the Internet of Services (as well as from P2P and eCommerce). Trust and reputation (TR) systems [4] are successfully used in numerous application scenarios to support users in identifying the dependable (or trustworthy) providers, e.g., on eBay, Amazon, and app markets for mobile applications. Related concepts are needed to support customers in selecting appropriate trustworthy Cloud providers. Industry experts and academic researchers have already coined the need for regulation, monitoring and trust establishment in the Cloud computing environments, as outlined exemplarily in the following. The need for a third party assurance body to accredit Cloud providers is mentioned in [5]. In [6], the author has discussed ways for evaluating the service quality of Cloud providers based on parameters like response time, availability and elasticity. A recent article [1] has highlighted the challenges and given an outline of solutions using emerging technologies for establishing trust in Cloud computing. Another article [7] has discussed several security and privacy challenges in Cloud computing environments and suggested considering a trust-based framework for supporting adaptive policy integration. Additionally, a number of research articles aimed at revealing security weaknesses [8,9], providing security guidance [10], and giving recommendations [11] regarding Cloud computing. Most of the articles mentioned above outline different challenges and possible solutions or recommendations regarding security, privacy, and trust issues in Cloud computing. However, there are only a few research articles that focus on the evaluation of Cloud providers or on finding appropriate solutions to establish confidence and trust between the consumers and the Cloud providers. We focus on this particular issue in this paper.

This article is the first survey focusing on the hindrances for adopting Cloud computing and how the trust concepts can support the consumers in overcoming these hindrances. Our work contributes to the understanding of why trust establishment is important in the Cloud computing landscape, how trust can act as a facilitator in this context to overcome the hindrances and what are the exact requirements for the trust and reputation models (or systems) in Cloud environments to support the consumers in establishing trust on Cloud providers. Particularly:

1. We propose a Cloud taxonomy to provide a clear idea about the involved players, their roles and offerings as well as the diversity of Cloud marketplaces in general.
2. We classify the current trends of trust establishment in Cloud computing. By analysing them in the context of a healthcare provider (a potential Cloud consumer) we identified the limitations of these trends.
3. We classify the QoS+ [12] parameters (in the sense of consumers' requirements) in terms of their information sources (based on the Cloud taxonomy) and approaches (based on the current trends) to derive the information.
4. We identified the required properties of TR models in Cloud environments for integrating the QoS+ parameters and outline the corresponding challenges.
5. We characterize the existing TR models and systems based on the essential properties. We also discuss each model's and system's strengths and weaknesses based on the property characterization.

The rest of the paper is organized as follows: Section "Cloud computing landscape" gives a brief introduction to Cloud computing. Section "Adoption of cloud computing" briefly depicts the incentives and hindrances to adopt Cloud computing and discusses how trust concepts is used to mitigate those hindrances. Section "Trust in cloud computing" describes the importance of trust concepts for service provider selection with an example and analyse the current trends for trust establishment. Section "TR models for cloud marketplaces: requirements and challenges" provides a list of relevant parameters (i.e., QoS+) and required properties along with their corresponding challenges for trust models in Cloud environments. Section "Survey and analysis of TR Systems/Models" surveys and analyses the existing trust models and systems. Finally, we present our concluding remarks in Section "Conclusions".

Cloud computing landscape

This section describes the landscape of Cloud computing from our perspective. In particular, it illustrates the building blocks and a taxonomy of Cloud computing.

Cloud computing building blocks

The basic building blocks of Cloud computing are illustrated in the following three sub-sections named:

- Service delivery models,
- Service deployment models, and
- Cloud entities

Before describing the building blocks, we give a brief overview of Cloud computing.

Definition

Defining *Cloud computing* stringently has not been an easy task in IT industry. However, IBM, Forrester Research, NIST (National Institute of Standards and Technology) and ENISA (European Network and Information Security Agency) came up with concrete definitions

[11,13,14]. While these definitions show a significant degree of overlap, each leaves out one or another attribute that the others demand and which we consider essential in order to define *Cloud computing* clearly. Thus, we propose to define *Cloud computing* by adopting those existing definitions as follows:

Definition 1 (Cloud Computing)**.** Cloud computing is a computing paradigm that involves data and/or computation outsourcing over the network (Intranet or Internet) based on virtualization and distributed computing techniques, especially fulfilling the following five special attributes:

1. *Multitenancy or sharing of resources:* Multiple users share resources at the network, host and application level.
2. *Elasticity:* Users can rapidly increase or decrease their resources (e.g., computing, storage, bandwidth, and etc.) whenever they need.
3. *Broad network of access:* Resources can be accessed from heterogeneous thin or thick client platforms (e.g., smartphones, notebooks, PDAs, and etc.)
4. *Pay-as-you-go feature:* Users pay only what they use in terms of computing cycles or usage duration.
5. *On-demand self-provisioning of resources:* Users can provision the resources on self-service basis whenever they want.

Service delivery models

Cloud computing enables and facilitates the provisioning of numerous kinds and diverse flavours of services. It is however possible to group these services as per the mode of their delivery. According to the NIST [14], Cloud services are delivered within three types of delivery models which are SaaS, PaaS, and IaaS. Aside from these three categories, three further service delivery models have been introduced in a distinguished talk by industry expert Stephen Hanna of Juniper Networks [15]. Adopting all these categories, Cloud service delivery models are categorized in six types which are Software as a Service (SaaS), Data as a Service (DaaS), Network as a Service (NaaS), Platform as a Service (PaaS), Identity and Policy Management as a Service (IPMaaS), and Infrastructure as a Service (IaaS). For further details regarding specific delivery models we refer the readers to [14,15].

Deployment models

Cloud deployment models are basically categorized into four different types [14] based on specific requirements of the consumers. These are: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud. For further details, we refer the readers to [14].

Cloud entities

Cloud providers and consumers are the two primary entities in the business market. However, aside from these, brokers and resellers are two other emerging entities in Cloud computing market [12]. Recently, NIST has mentioned Cloud Auditors and Cloud Carriers as further two entities (or actors) in their updated reference architecture of Cloud computing [16]. The different types of Cloud entities are briefly discussed in the following.

Cloud Providers (CPs) Cloud providers host and manage the underlying infrastructure and offer Cloud services (e.g., SaaS, PaaS, and IaaS) to consumers, service brokers or resellers. Note that Cloud Brokers (CBs), Cloud Resellers (CRs), and Cloud Consumers (CCs) may act as CPs in certain contexts, which are discussed in the following sections.

Cloud Brokers (CBs) Generally, two types of brokers in a Cloud market can be distinguished. Firstly, there are brokers that concentrate on negotiating relationships between consumers and providers without owning or managing the Cloud infrastructure. They provide, for example, consultancy services to the potential CCs for moving their IT resources into a suitable Cloud. Secondly, there are brokers that add extra services on top of a CPs' infrastructure / platform / software to enhance and secure the Cloud environment for the consumers. For example, a broker might offer identity and access management service on top of CP's basic service offerings to consumers. As an example, such a broker may develop APIs in order to make Cloud services interoperable and portable. In both cases, the broker act as a CP that offer value added or bundled services to the CCs. DaaS, IPMaaS and NaaS are three types of service delivery models that offer services on top of other services (e.g., SaaS, PaaS, and IaaS). Thus, the CPs, that offer add-on services (e.g., DaaS, IPMaaS, and NaaS), plays the role as a broker in Cloud computing market.

Cloud Resellers (CRs) Resellers provide services on behalf of a Cloud provider. They can become an important factor in the Cloud market when CPs expand their businesses into new markets, for instance across continents. CPs may choose local IT consultancy firms or resellers of their existing products to act as resellers for their Cloud-based products in a particular region. Thus, on the one hand, resellers may realize business opportunities of massive Cloud investments rolling into their market, for instance in order to harness strategic partnerships, establish themselves in a new business field or supplement their existing infrastructures. On the other hand, CPs can use the brand recognition, marketing and

reselling expertise of the resellers to strengthen their position in the Cloud market. In the case of reselling the Cloud services and offering customer support on behalf of a provider, a reseller may act as a CP to Cloud consumers.

Cloud Consumers (CCs) CCs can be broadly categorized into two types: i) end consumers and ii) Cloud-based service providers (CbSPs). Business organizations, government authorities, educational institutions, and individuals belong to the category of end consumers who may use Cloud services to meet their business, national, educational and personal needs (without offering any new services to others). On the other hand, CbSPs offer new services to the consumers that are entirely hosted in Cloud. The role of CbSPs is different than that of the CBs, as CBs just offer the add-ons on the top of existing services, where as CbSPs develop their own business model based on the services they offer (cf. Figure 1).

Cloud Auditors (CAs) Auditors conduct independent assessment of other entities (including Cloud Carriers) in terms of Cloud services, information systems operations, performance and security of the Cloud implementations. For example, a Cloud auditor can make assessment of security controls in the information system to determine the level of controls implemented correctly or not. Based on the assessment they issue a particular audit certificate which is extremely important for the consumer who outsource in-house application to the Cloud.

Cloud Carriers (CCas) These intermediate entities ensure seamless service provisioning by providing connectivity among Cloud entities. For example, CCas provide network, telecommunication and other devices for accessing Cloud services. Network and telecommunication operators are also part of this category as they ensure service distribution through their network.

In the next section, Cloud taxonomy is provided to give a clear picture of the Cloud computing marketplaces.

Taxonomy of the cloud computing market

Existing Cloud taxonomy [17] by OpenCrowd community covers three basic service delivery models (e.g., SaaS, PaaS, IaaS) and Cloud softwares to provide an extensive list of CPs. We further extend the taxonomy by including the Cloud entities and other service delivery models (e.g., NaaS, IPMaaS, and DaaS) to provide a more concrete picture of Cloud computing marketplaces.

According to OpenCrowd's Cloud taxonomy, CPs are classified into four categories based on the type of services they offer. In this taxonomy, providers of three non-canonical service models – DaaS, NaaS and IPMaaS – are missing. Moreover, except CPs, the other Cloud entities mentioned in section "Cloud entities" are not part of the taxonomy. Our objective is to provide a taxonomy where all the entities can be incorporated based on the types of services they are related with. We omit the category "Cloud softwares" as the providers belong to that category easily fit into our taxonomy with extended service delivery models.

The Cloud taxonomy (cf. Figure 1) illustrates the entities of today's Cloud marketplaces. The entities are categorized based on the roles they are playing in Cloud marketplaces. Each of the entities is further categorized based on the types of services they are offering or consuming. A brief discussion regarding the taxonomy is given as follows.

In the first row, CPs are listed according to the service delivery models (see section "Service delivery models"). In each of the service delivery models, there are various types of services that are offered by the CPs. For example, it can be seen that Zoho offers a particular type of *SaaS* products, *desktop productivity*, but is not one of the companies providing, for instance, *social networks* as a service.

In the second row, CBs are listed according to the types of services they are brokering. For example, Right Scale provides a Cloud management platform which gives consumers the flexibility of managing their infrastructures (e.g., virtual OS images) hosted by different Cloud infrastructure providers.

In the third row, CRs are listed under the respective CPs for whose offerings they act as resellers. Only a few of the CPs publicize a list of their resellers.

In the fourth row, CCs are depicted according to the business model they follow. For example, Animoto, a video rendering service provider hosted in the Amazon Cloud (thus, acting as a service provider to its customers, but consuming Cloud-based computing services from Amazon), is offering rendering services to its end consumers for creating video slides from the given images. End consumers, however, consume Cloud services but do not provide Cloud services to other customers as part of their primary business model. For example, educational institutions (e.g., Chalmers University of Technology or the University of Amsterdam), business organizations (e.g., Eli Lilly [15]) and government authorities (e.g., Los Angeles city government [18]) use Cloud resources for their IT needs but not selling the services outside their boundary or to the consumers outside the organizations.

In the fifth row, a range of cloud audit standards (or services) are listed according to the audit related resources from the Cloud Security Alliance [19]. Note that the list is not limited to these standards or services.

The Cloud taxonomy presented here gives a clear idea about the diversified market structure of Cloud computing. This obviously appear as one of the incentives for the consumers to adopt Cloud computing business model through many alternatives. However, there are

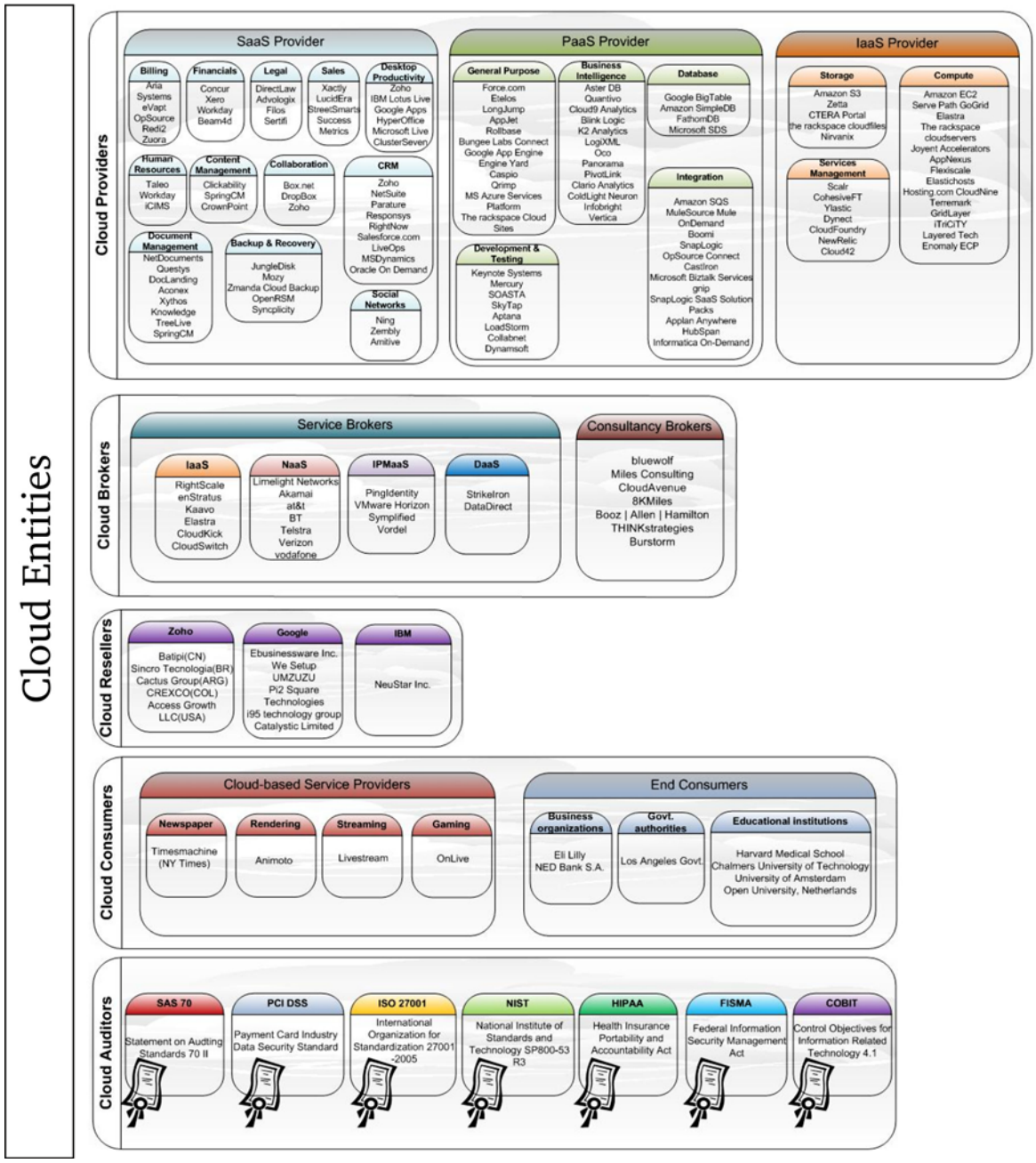

Figure 1 Cloud taxonomy.

service providers of different service quality and the non-transparent nature of Cloud computing introduce considerable obstacles which make the consumers sceptic to adopt Cloud computing as a part of their business model.

Adoption of cloud computing

Cloud computing offers incentives for each of the Cloud entities. However, these incentives are not free of obstacles (hindrances for cloud adoption).

Incentives for cloud adoption

Primary incentives for Cloud entities depend on the role of these entities in the service provisioning process. In such a process, an entity is either a consumer or provider of a particular service. The immediate benefit for entities fulfilling the provider role, i.e., CPs, CBs, CRs, and CCas primarily lies in enabling their business and offering new business opportunities. Organizational CPs stand to gain from providing Cloud services, generating profit

by making their expertise in IT and unused computing capabilities available to consumers.

From a Cloud Consumer (CC) point of view, the adoption of Cloud computing by individuals is already widespread. Organizational Cloud Consumers, ranging from start-ups to SMEs (Small and Medium-sized Enterprises) to large companies and NGOs (Non-Government Organizations), are outsourcing IT resources in the Cloud in order to leverage a number of key benefits, ultimately related to both cost and capabilities. We see the following key benefits: cost reduction, dynamic resource sharing, pay-per-use, fast roll out of new services, dynamic resource availability which are detailed in [12].

Hindrances for cloud adoption

As outlined above, CCs, particularly on the institutional level, can leverage considerable benefits by switching to applications run in the Cloud. This has prompted Gartner Inc. to identify Cloud computing as one of the top strategic technologies for the year 2010 [20], thereby further highlighting the importance for companies and other institutional consumers.

However, actual adoption of Cloud computing by businesses is still lagging. A number of concerns contribute to this, generally showing that confidence in the new technology still has to grow. Some of these concerns have been identified in recent articles. Researchers from the RAD lab of UC Berkeley, for instance, have identified 10 specific concerns (i.e., availability, data lock-in, data confidentiality & auditability, data transfer bottlenecks, etc.) [21] regarding the adoption of cloud-based services. Recently, another group of researchers identified a number of threats and risks (i.e., security & privacy threats, weak Service Level Agreements (SLAs), lack of reliability, etc.) to adopt cloud-based services and discussed how these affect the consumers' trust on cloud providers [12]. As a further example, another survey [22] about Cloud computing, from the perspective of SMEs, shows that security and the liability for incidents involving the infrastructure are major concerns for potential Cloud consumers among SMEs at present.

With enterprises hesitant to move into Cloud computing, CPs are unable to realize the full potential of the Cloud market. By identifying and addressing customer concerns, CPs have thus the opportunity to increase their profits. The same reasoning also applies to potential CBs and CRs. They do, however, act in a dual role, both consuming Cloud Services and providing them. They have, as service providers, a vested interest to attract customers to their offerings. However, they are not controlling the entire service provisioning process because they have to rely on the CPs that supply the services they expand or resell. The Cloud enables their business models, while at the same time, concerns regarding Cloud adoption hamper their success.

The issues faced by both providers and prospective consumers of Cloud services boil down to an unwillingness on the part of the consuming party to depend on the providing party. Thus, the overall acceptance, and thus the success of enterprise service provisioning in Cloud computing, hinges on whether or not consumers are willing to relinquish control over potentially business relevant information, data or internal processes. Often, losing this control exposes the depending party to a considerable risk if internal, sensitive data is divulged or (time-critical) services are not being rendered adequately by the provider. In order to overcome this significant challenge, consumers have to be put in a position where they can reliably assess the dependability of a service provider [3]. At the same time, service providers have to be able to truthfully represent their dependability. If both these objectives can be achieved, consumers have a basis for making well-founded decisions about whether or not to depend on a particular service providers.

Trust as a facilitator

Predicting the future behaviour of a partner in a situation involving uncertain outcomes is usually achieved, in social contexts, through the concept of trust. Various factors contribute to the establishment of a trust relationship between two partners, ranging from general assumptions about the legal or social environment, to the immediate public reputation of each of the partners, to concrete, actual prior experiences made during previous interactions [23]. Particularly the last factor, direct prior experience, represents a strong indicator of the dependability of a potential partner.

In the Cloud environment, however, entities potentially initiate transactions with each other without having had prior contacts. Due to the resulting lack of direct experience shared among a particular pairing of consumer and provider, consumers often hold insufficient information for reliably predicting the quality of a service and the trustworthiness of its provider. Lack of experience with a service provider, for instance regarding data privacy and security policies, thus represents a specific hurdle to the adoption of Cloud computing.

This situation is exacerbated by CPs seemingly giving overcommitted assurances while at the same time limiting liability for failure to achieve the assured levels of service in their SLAs. In other words, providers today tend to make promises that they are unwilling to back up. Several CPs, for instance, promise high availability, such as 100% or 99.99% availability of a service – the latter translates to 52 minutes downtime a year. In the light of recently reported Cloud service outages [24]), this seems unreasonably optimistic (if not to say, wholly unrealistic).

Thus, Cloud Providers currently do not represent their dependability truthfully. The lack of *meaningful* information results in *mis*trust. Dedicated trust management, in the sense of [25], leveraging trust and reputation concepts, is required to permit consumers to fully embrace Cloud Computing.

Trust and the related concept of reputation are two essential mechanisms in the facilitation of decision making in many economic and social fields, from ancient fish markets to modern eCommerce. In order to be applicable, however, the somewhat broad term 'trust' has to be specified a bit further. A common definition of trust [4,26,27] in computational applications describes it is a subjective expectation of one entity about another within a specific context at a given time. Thus, trust can serve as an estimation of future behavior.

Reputation is defined as what is believed about an entity's standing by the community [4]. This belief can be derived from previous experience, using past behavior to predict future actions. This experience can be either direct or indirect. Direct experience connotes what has been learned by an evaluating entity about another from previous interactions between these two entities. Meanwhile, indirect experience is built from either (*a*) observations of interactions between the entity under evaluation and a third or (*b*) recommendations given to the evaluating entity by another member of its community. Usually, determining trust, i.e., computing a subjective expectation of another entity's future actions, is based upon the reputation that entity has – thus, reputation directly affects trust. However, trust, as a subjective, dyadic relation between entities, also affects reputation. Trust represents the opinion of one entity towards a specific other, while the collective opinions of (all) entities constitute reputation. Thus, trust affects the reputation of an entity and vice versa [28].

Reputation clearly is an important aspect of trust establishment, a fact evident in the numerous reputation-based computational trust models in existence [4]. It is, however, not the only important one. Aside from reputation, the intentions, capabilities and competencies of the partners in a potential interaction also contribute to the assessment of trust. A consumer, for instance, is more likely to trust a service provider to deliver a satisfactory performance, if the service provider can credibly represent its ability to meet the consumer's requirements. It can do so by relying on its public standing and general history of delivering a service well, i.e. its reputation. However, it can also provide documents, certificates or audits to show that its capabilities are sufficient for the consumer.

Trust in cloud computing

Trust issues become particularly important when data processing is decentralized across geographically dispersed data centres and resources are distributed beyond a definable and controllable perimeter, which is especially true in the Cloud computing scenario. In the next section, we illustrate an example to show the importance of trust establishment in Cloud computing, in particular establishing trust on Cloud providers.

Motivating example

The example we illustrate here is of a healthcare provider who wants to outsource their in-house application that deal with medical records to a Cloud-based service. The main goal is to minimize the IT expenditure as well as allow seamless access to these medical records using the Cloud-based service to doctors, patients, and insurance companies. The medical records consist of private information and by outsourcing them in a Cloud-based service one has to make sure that the most dependable Cloud provider host the service. The healthcare provider require assurances regarding compliance (e.g., HIPAA (Health Insurance Portability and Accountability Act)), data protection through security and privacy controls, geographical location (data should not leave the political border) and high availability of the services. The healthcare provider considers the CPs trustworthy if they are dependable in fulfilling the assurances.

Since the Cloud computing market for offering medical record services is competitive, the healthcare provider is facing the challenge of selecting a potential provider that is best-suited and most appropriate for them, from numerous alternatives. Assume that all of these providers have the same functionality and provide the assurances according to the healthcare provider's requirements. In order to select the trustworthy Cloud provider, the consumer (i.e., the healthcare provider) has to compare the offered services or solutions independently which is, in fact, a cumbersome task. This task includes analysing the SLAs and finding out the clauses according to their requirements, checking whether the provider abide by the specific audit standards or studying the CAIQ (Consensus Assessments Initiative Questionnaire) [29] from STAR (Security, Trust & Assurance Registry) [30] by CSA (Cloud Security Alliance) to learn about the present security controls of the Cloud provider.

Current trends for trust establishment

There are ad-hoc approaches to support the consumers in selecting trustworthy (or dependable) CPs. We classify and briefly analyse these approaches as follows.

- **SLAs:** In practice, one way to establish trust on CPs is the fulfilment of SLAs. SLA validation [31] and monitoring [32] schemes are used to quantify what exactly a CP 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 CPs 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 [33] for establishing standardized SLAs, this initiative is far from implementation in practice.

- **Audits:** CPs 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 [34] and most of the CPs are not willing to share the audit reports, which also leads to a lack of transparency.
- **Measuring & Ratings:** Recently, a Cloud marketplace [35] has been launched to support consumers in identifying dependable CPs. They are rated based on a questionnaire that needs to be filled in by current CCs. In the future, Cloud Commons aims to combine consumer feedback with technical measurements for assessing and comparing the trustworthiness of CPs. Furthermore, there is a new commercial Cloud marketplace named SpotCloud [36] that provides a platform where CCs can choose among potential providers in terms of cost, quality, and location. Here, the CPs' ratings are given in an Amazon-like "star" interface with no documentation on how the ratings are computed.
- **Self-assessment Questionnaires:** The CSA proposed a detailed questionnaire for ensuring security control transparency of CPs – called the CAIQ (Consensus Assessment Initiative Questionnaire). This questionnaire provides means for assessing the capabilities and competencies of CPs in terms of different attributes (e.g., compliance, information security, governance). However, the CSA metrics working group does not provide any proposals for a metric to evaluate CAIQ yet. This is necessary for comparing the potential CPs based on the answered assessment questionnaire stored in the STAR. Furthermore, the information stored in the STAR repository can be checked against the CCM (Cloud Control Matrix) [19]. This will provide the assurance whether services offered by the CPs comply with the industry-accepted security standards, audits, regulations, control frameworks (cf. Figure 1) or not.

Limitations of current trends

The trends currently followed by the CPs are mostly ad-hoc. These trends are either considering technical and functional features or the user feedback for establishing trust on CPs. Thus, these trends are lacking a unified approach (i.e., trust evaluation framework) where all these trends can be considered complementary to support the consumers in evaluating the providers and selecting the most trustworthy (or dependable) one. Moreover, the current approaches (e.g., analysing the SLAs or studying the audit reports) are time consuming and cumbersome. Therefore, the CCs (e.g., the healthcare provider) may skip the idea of outsourcing the in-house application to the Cloud. Figure 2 visualizes the current trends for trust establishment from the perspective of the healthcare provider.

In the next section, the technical solutions are envisioned to overcome the limitations of current trends and support the consumers in selecting trustworthy providers.

Overcoming the limitations of current trends

To overcome the limitations of the current trends the technical solutions should go beyond simply selecting a service provider based upon purely technical features, such as classical QoS (quality of service) parameters. Rather, trust has to be established, both regarding individual service providers and the Cloud computing paradigm in general. This trust extends to CPs supplying reliable services, maintaining confidentiality, integrity and availability, conforming to contracts and SLAs, etc. On a more abstract plane, consumers have to trust that Cloud computing is a secure and economically sound paradigm in order to facilitate Cloud computing as a business model. On a technical, but also on a commercial side, trust has to be made measurable, in order to represent it in decision making contexts (e.g., for provider selection). If Cloud services are not transparent with regard to their features (e.g., security, service performance, geographical location,etc.), underlying service compositions and the technical infrastructure, trust and quality cannot be factored to decision making processes (e.g., provider selection). Lack of transparency of a service creates an asymmetry between consumer and provider. The consequences of such an asymmetry have been described by Ackerloff in his article *A Market for Lemons* [37]. While the original example describe the effects with regard to the sale of used cars, the results are nonetheless transferable to modern eCommerce. In [37], expensive but high quality products are driven out of the market in favour of low-cost alternatives, because customers are unable to assess the reliability of the sellers. In another article [5], the author points out a

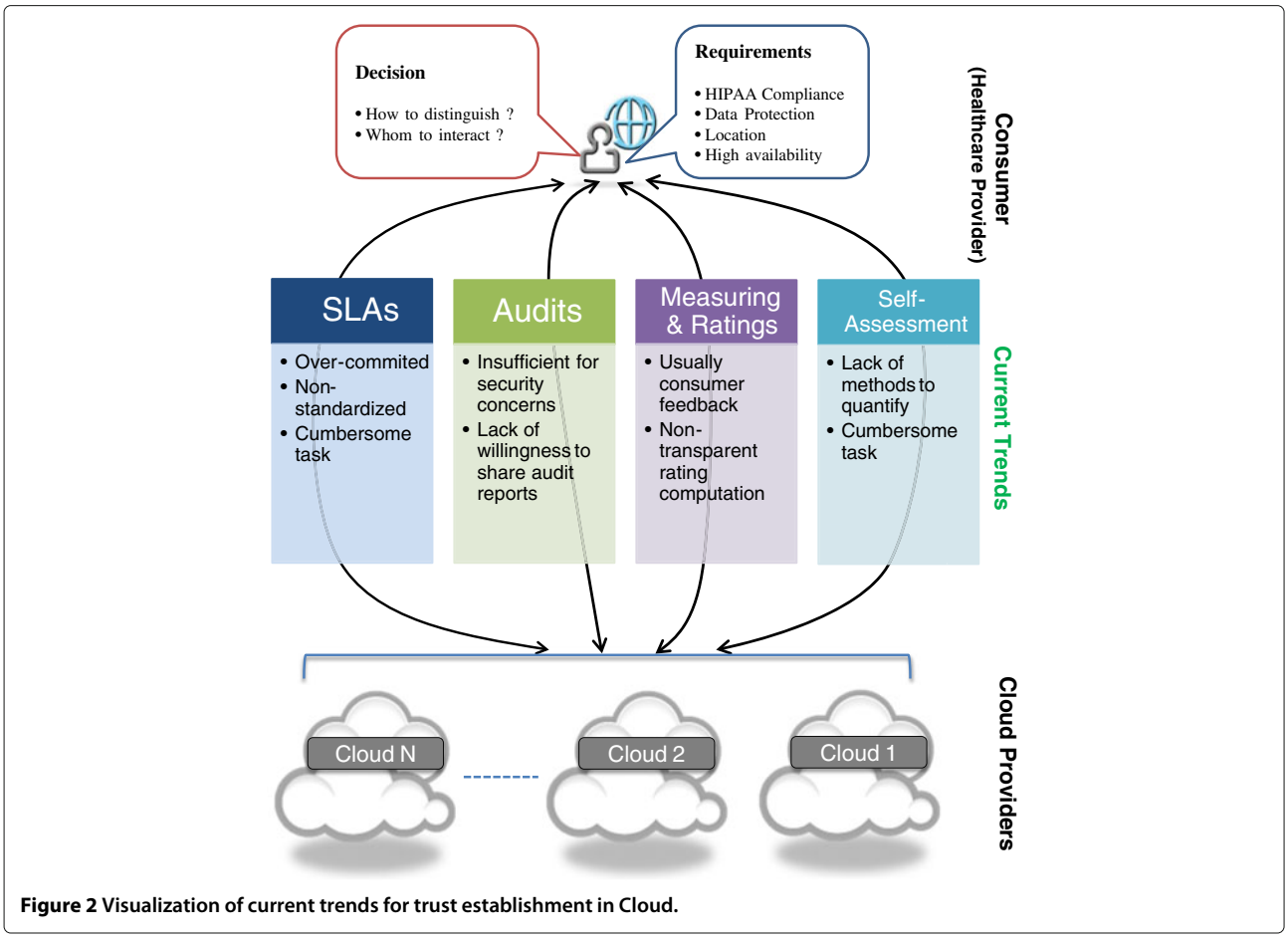

Figure 2 Visualization of current trends for trust establishment in Cloud.

typical scenario where a Cloud provider can offer a "wonderfully" secure service while another may not. In analogy to the market of lemons example, if the latter charges half the price, the majority of organizations will opt for this cheaper competitor as there is no practicable way to explore the difference. To assist customers in exploring the differences and selecting the most trustworthy Cloud provider, a trust-aided unified evaluation framework is needed. Trust and Reputation (TR) models used in various application environments represent a promising and essential basis for such a framework .

Figure 3 visualizes the trust-aided technical solution for supporting the consumers (e.g., healthcare provider) in interacting with the most trustworthy Cloud provider.

TR models for cloud marketplaces: requirements and challenges

TR models have been proven useful for decision making in numerous service environments (e.g., e-commerce, p2p networks, product reviews) [4,38]. The concepts have also been adapted in grid computing [39,40], inter-cloud computing environments [41], and selecting web services [42]. These trust models mainly consider interaction experiences and behavioural (e.g., p2p networks) or technical (e.g., grid computing, web services) observations for selecting trustworthy entities. Both of these aspects and related parameters are equally important to consider when selecting trustworthy service providers in Cloud marketplaces.

Cloud based services are hosted in massively distributed and complex systems (highly abstract and non-transparent). Because of this distributed complex service oriented architecture, consumers have to consider the parameters which are related to both aspects (i.e., interaction experiences and technical) for current TR models in numerous service environments. Moreover, TR models for Cloud computing environments need to take specific cloud-related parameters into account for trustworthy service provider selection. These parameters go beyond the usual QoS parameters [43], which are considered when selecting web service providers.

QoS+ Parameters for TR models

Recently, researchers proposed QoS+ (beyond the usual QoS) parameters for TR models in Cloud environments [12]. These parameters are identified based on the state-

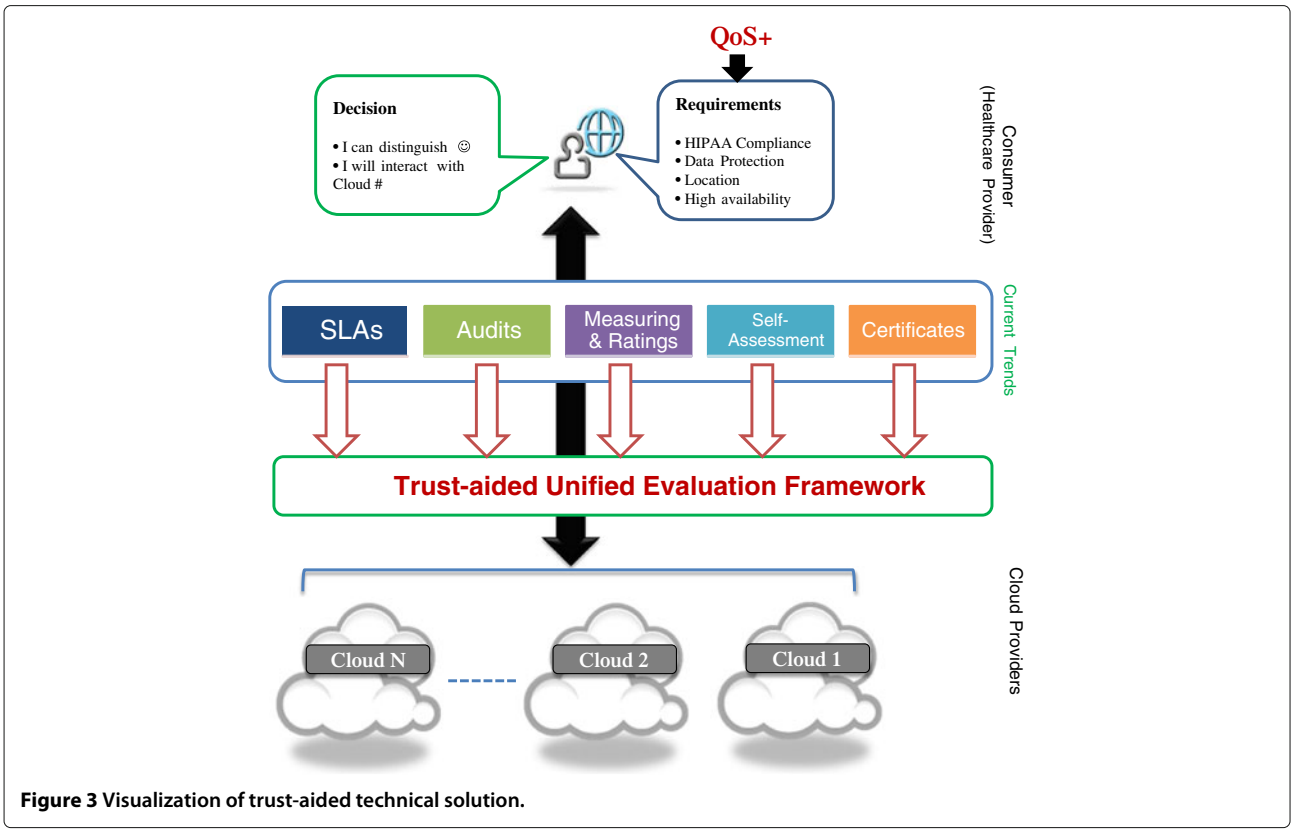

Figure 3 Visualization of trust-aided technical solution.

of-the-art survey of threats and risks discussed in [12]. Moreover, a recent article [3] published a list of functional and non-functional trust affectors based on a extensive survey conducted among the Cloud entities. This survey clearly shows the consumers' interest and need of reckoning the trust affectors for establishing trust on Cloud providers. The QoS+ parameters map quite closely to the trust affectors identified in the survey article. The mapping shows the usefulness and absolute need of such parameters for selecting trustworthy service providers in Cloud environments. Therefore, considering the cloud-specific parameters (i.e., QoS+) for trust models in Cloud environments in turn support the consumers to know the capabilities and competencies of the CPs before interacting with them.

TR models require direct and indirect information (i.e., experiences, observations, opinions) regarding the QoS+ parameters for trust computation and evaluation phase. The information about the parameters are often available from multiple entities and parties (e.g., CPs, CCs, CAs, CBs, CCas). They provide the information through different measures or approaches. Hence, the approaches followed in current trends (cf. Section "Current trends for trust establishment") are considered complimentary for trust establishment. In Table 1 , the QoS+parameters are listed along with their corresponding sources of information, the existing approaches used for deriving the information. The parameters are discussed briefly in the following:

1. **SLAs:** The entities that are providing services are required to follow standardized SLA, e.g., proposed by Cloud Computing Use Cases community [33]. The SLA specification of CPs then can be assessed based on the compliance to the standardized format. This compliance is further factored into trust assessment of CPs. The information regarding the SLAs is considered to be direct, as these agreements are usually between the corresponding entities (e.g., CCs and CPs, CPs and CBs, CPs and CCas).
2. **Compliance:** CPs use audit standards as an assurance for the existence of technical (e.g., security) and organizational controls related to their offered services. The CAs assess these controls and issue certificates for the CPs based on the assessment reports. Otherwise, the information about those controls are provided by CPs in the STAR repository and can be checked against the CCM initiated by CSA. The results about the audit compliance can be obtained directly from the CPs or indirectly from the CSA.

Table 1 QoS+ Parameters: information sources and approaches

QoS+ Parameters	Who provide the information?	How to derive the information?
SLA	CPs, CBs, CCs, CCas	Standardized SLAs
Compliance	CAs, CSA	Audit Standards, CCM
Portability Interoperability Geographical Location	CPs	SLAs
Customer Support	CCs, CPs, CBs, CCas	SLAs, User Feedback
Performance	CBs, Independent Third-party, CCs, CPs	Measurement, User Feedback
Federated IdM	CPs	SLAs
Security	CSA, CPs, CAs	CSA CAIQ, Certificate-based Attestation mechanism, Audits
User Feedback	CCs	Measurement and Ratings (User Feedback)
Service Deployment Models Service Delivery Models	CCs, CBs, CRs	Context Dependency and Similarity techniques

3. **Portability, Interoperability, and Geographical Location:** The information regarding these parameters are directly obtainable from the CPs. The existence of terms and clauses related to these parameters documented in the SLAs are the valid form of information in this case.
4. **Customer Support:** CPs usually provide assurances about terms and clauses related to "customer support" in their SLAs. TCBs and CCas are also required to include similar terms in their SLAs for their respective consumers (e.g., CPs or CBs or CCs). The SLA-based terms and clauses can be complemented by considering experiences from the existing consumers and factor into overall trust computation of CPs or CCas.
5. **Performance:** In Cloud computing environments, the information about the performance related parameter (e.g., availability, latency, bandwidth, elasticity) is obtained using service monitoring technologies. CPs and CBs usually provide the application for monitoring such parameters which are usually used after the service provisioning contract. CCs also can hire the independent third-party brokers (if required) to monitor those parameters before provisioning the services. In this case, the monitored or observed data regarding the performance parameters can be compared among the potential providers or with the agreed data stated in the SLAs to validate them [44]. The validation result (i.e., success or failure) or the comparison of performances then may influence the evaluation of trustworthiness of CPs.
6. **Federated IdM:** The information regarding this particular parameter is provided by the CPs through their SLAs. This parameter is required for the federated enterprises using common cloud-based services.
7. **Security:** CCs want to know about the existence of certain security controls when outsourcing their IT resources to the cloud. The CSA initiated CAIQ [29], a self-assessment questionnaire designed for the CPs to document their security controls, to increase transparency between the providers and consumers by publishing it in a public repository. Moreover, CPs host services in trusted virtualized platforms using the trusted computing (TC) technology. In a distributed service environments (e.g, Cloud computing), consumers can learn about the security or non-security related behaviour of the software components running on those platforms using remote-attestation mechanism, e.g., [45].
8. **User Feedback:** Feedback, recommendation, reviews from the consumers are valuable for service selection in e-marketplaces. This concept is also adapted in Cloud marketplaces (e.g., CloudCommons, SpotCloud) where CCs share their experiences about the cloud services they provisioned. The information about their experiences may appear as quantitative (e.g., satisfaction score) and/or qualitative (e.g., reviews) forms. Consumers' experiences can be used to evaluate the CPs as a whole or with respect to each QoS+ parameter.
9. **Service Deployment and Delivery Models:** Trust models are usually context-specific and it is important to consider in the TR models for service selection in Cloud environments. The service delivery models (cf. Section "Service delivery models") and service deployment models (cf. Section "Deployment models") should be factored as a contextual parameter in trust models. Hence, the

context dependency and similarity techniques [46,47] are considered complementary for the trust models in Cloud environments.

Properties and challenges of TR models

TR models require specific properties to incorporate QoS+ parameters for trust establishment in Cloud environments. The integration of these parameters into a TR model specifically tailored to the use in Cloud environments introduces further challenges. The following sections comprise essential properties and related challenges for consideration:

1. **Multi-faceted Trust Computation:** The computation of trust should consider the parameters listed in Section "QoS+ Parameters for TR models", which refer to the competencies and capabilities of a service provider in certain aspects, for instance, providing security measures, accreditation, bandwidth or customer support. Integrating these different aspects brings up multi-faceted challenges regarding computation of trust, which are as follows.
    - Multi-criteria: The assessment of the trustworthiness of an entity should consider all relevant parameters, which usually means to take into account multiple parameters describing different qualities of a service (composition) or its provider. Especially the aggregation of objective parameters (e.g., expert ratings or real-time measurements) and subjective parameters (e.g., recommendations by other consumers) is a major challenge.
    - Multi-root: When integrating multiple parameters into a TR model, one has to consider that the quantitative or qualitative information, being factored into the trust establishment process, can be derived from different roots. Furthermore, one has to consider that those roots might have very different characteristics; for instance, information derived from a trusted platform module (TPM) or certificates provided by a property attestation authority (sometimes referred to as hard trust) need to be handled differently from trust information derived from user feedback (sometimes referred to as soft trust). Therefore, the combination of information from different roots poses another major challenge.
    - Multi-context: As a single service provider may offer different services that require different competencies, a computational model should be able to reflect the context in which a service provider has established trust. In Cloud computing, the different context can refer to different service delivery models. For example, a service provider might be trustworthy in delivering SaaS but not PaaS or IaaS. Moreover, if a trust model is able to consider that an entity has different trust values in different contexts, the model should be able to reason about the overall trustworthiness of an entity, or about the trustworthiness of a newly deployed service (e.g., based on the knowledge which components that are already used in other contexts are re-used for the new service).
2. **Customization and Aggregation:** Another issue that is relevant when selecting or designing of trust or reputation mechanism relates to how much customization should be supported and where should the trust values be aggregated.
    - Trust Customization (Global reputation vs Local/Subjective trust values): When trust is derived from different parameters, it is possible to consider *subjective* interests and requirements that *dependent* on the entity evaluating the trustworthiness of a service provider. This leads to a *local* (subjective) trust value. However, a *global* trust value is independent from who evaluates trustworthiness of a service provider.
      On the one hand, the *local (i.e., subjective)* trust values provide means for considering the preference of each user in detail. Customization allows users to define the parameters relevant for trust establishment from their point of view, to weight the parameters according to his preferences and to consider which sources of information the user believes to be more trustworthy. For example, one customer might give preference (a higher weight) to security measures, whereas for another customer a high-quality customer support is more important.
      On the other hand, service providers might be more interested in the calculation of a *global trust (or reputation)* value, as this might be more directly influenced and observed by the companies.
    - Trust Aggregation (Centralized vs Decentralized): Usually, there are two different fundamental approaches to store and aggregate trust-related information;
      The first one is to host the information in a *centralized* repository, the other is to use a

decentralized approach. Both have distinct advantages and disadvantages: In *centralized* trust models – requiring a trusted third party – users cannot manipulate the data except by providing ratings to the central system. The aggregation methodology can be kept secret and the individual ratings of an entity are (usually and ideally) not published or distributed. However, the trusted authority hosting the centralized repository may manipulate the results and represent a single point for attacks. *Decentralized* trust models do not require a trusted third party, however, one has to trust in the mechanisms which are used for distributing the ratings and to consider the costs for distributing the ratings among the entities. The latter can be solved by applying algorithms that aggregate the individual ratings by only communicating with an entity's local neighbourhood [48]. A disadvantage of *decentralized* models is that preserving privacy is much harder as more information is distributed between the participating entities.

3. **Trust Evaluation:** For complex, distributed environments (e.g., Cloud computing) we introduce a categorization of mechanisms that are relevant for trust evaluation that – to the best of our knowledge – have not been discussed in this context before:

    - Black box approach: Following this approach, the trustworthiness of an entity or a service is evaluated taking into account only the observed output, for example by only considering user feedback. Models in this class treat the service as a black box, and do not require (or consider) any knowledge about the internal processes and components of the service.
    - Inside-out approach: Following this approach, the trustworthiness of an entity or a service is derived based on the knowledge about the architecture of the service and the trustworthiness of its components (or subsystems). For recent approaches following this idea, see [49,50].
    - Outside-in approach: A model that is following this approach requires knowledge about the internal architecture of a service and its components as input as well as information stating the observed behaviour of the overall service. The goal of this kind of model is to derive the trustworthiness of internal components of a service composition based on its external behaviour (cf. [51]). This is far from trivial, but can be successful when some components are re-used in multiple services and if certain errors in the behaviour of the service composition can be backtracked to the originating component.

4. **Transferring Trust between Contexts:** As stated above, customer trust in a service provider depends on the specific application context or the scope of interaction. Transfer of trust across those contexts is a significant challenge for trust and reputation systems. Consider, for example, a service provider offering an email service and a video rendering service – both belonging to the SaaS category. Both application contexts require different competencies, for example spam protection and storage for the email context, whereas for video rendering context, latency, bandwidth and parameters dealing with performance matters (e.g., response time, CDN (Content Delivery Node) facilities, etc.) are important. Here, transferring trust established in one context (email) to the other one (video rendering) is not a trivial task, and could, for instance, be supported by combining the outside-in and the inside-out evaluation.
5. **Attack Resistance:** As soon as the influence of trust and reputation models on the decision of customers will grow, the interests in manipulating those values in Cloud environment will grow accordingly, as already seen in other service environments earlier [52]. A number of different attacks (e.g., playbooks, proliferation attacks, reputation lag attacks, false praise or accusation (collusion), whitewashing (re-entry), sybil attacks, etc.) against trust and reputation systems have been discussed [52,53]. These types of attacks will also be of concern when designing trust and reputation system for Cloud computing environments. Thus, attack resiliency is a central design goal for developers of these kind of systems.
6. **Transparent Trust Representation:** The derived trust values or reputation scores must be transparent to and comprehensible enough for the consumers, so that they can easily and confidently make trust-based decision. To make the trust values transparent and comprehensible, users need to be supplied with an intuitive representation of trust together with enough information regarding the relevant parameters.

In the next section, we survey and summarize state-of-the-art trust and reputation systems and models from different fields of application. Particularly, attention is given to the characteristics of the models whether they satisfy the above mentioned properties whole or in part.

Survey and analysis of TR systems/models

There are a number of commercial TR models, as well as numerous proposals in different research communities, targeting various application areas (e.g. eCommerce, product review sites, Peer to Peer (P2P) networks, Online Social Networks (OSNs), Wireless Sensor Networks (WSNs), ubiquitous and grid computing). In the following, we choose seventeen promising models from different application fields for our analysis with respect to the properties mentioned in section "Properties and challenges of TR models": eBay [54], Epinions [55], Beta reputation [56], CertainTrust [27,28], FIRE [57], EigenTrust [58], socialREGRET [59,60], TidalTrust [61], RFSN [62], GridEigenTrust [63], Abawajy's model [41], TESM [45], Unitec [64], BNTM [65], Buchegger's model [66], Billhardt's model [67], Hang's model [51].

Trust customization and *trust aggregation* properties are the two most generic properties for *TR* models in commercial applications or research community proposals. Most of the commercial *TR* models (e.g., *eBay*, *Epinions*) support a single *reputation (i.e., Global trust)* score for each customers; this score is calculated and stored in a centralized system. Most of the TR models proposed by the research community support *local (subjective)* trust values considering the customer preference in detail while measuring the trustworthiness of a service provider except *Eigentrust*, *GridEigentTrust*, *Abawajy's model*, and *Unitec*. However, all the TR models from the research community, we surveyed, support distributed computation and storage for trust-related information.

Most of the TR models, either in commercial applications or proposed by the research community, consider trust information from just a single *root (soft trust)*. However, only two trust models (*FIRE* and *TESM*) from the research community consider two roots (from soft and hard trust) in trust computation. Regarding *trust evaluation*, most TR models (commercial and research proposals) use the *black box approach*. A few models from the research community, notably *GridEigenTrust* and *TESM*, evaluate trust using the *inside-out approach*. One particular among the surveyed models, (*Hang's model*), uses the *outside-in approach* for trust evaluation.

Taking *multiple criterias* into account, when calculating trust in TR models, is not common in the trust community. Commercial applications (e.g., *eBay* and *Epinions*) support multi-criterial computation of trust. However, eBay's seller ratings, displayed in four distinct categories (i.e., item described, communication, shipping time, shipping and handling charges), don't affect the general rating system (i.e., categorical ratings are not taken into account to compute the overall rating). Only four models – (*socialREGRET*, *Abawajy's model*, *TESM*, and *BNTM*) – proposed by the research community, support multiple criteria in trust computation.

Commercial models like *Epinions* aggregate trust ratings from *multiple contexts* to provide an overall reputation score for an entity. However, commercial models like *eBay* and most of the TR models proposed by the research community, do not support the feature. A few TR models from the research community (e.g., *GridEigenTrust* and *BNTM*) consider trust values from *multiple contexts* to compute an overall trust score. However, neither *GridEigenTrust* nor *BNTM* can *transfer trust* across contexts. Conversely, *Billhardt's model* does not support the *multi-context* feature but is capable of transferring trust across contexts. Thus, significant improvement is needed regarding TR models for Cloud environments that are to support both features.

Most of the trust models are subject to different kinds of attacks, while a few of them are resistant to particular attacks like false praise or accusation (FPA), sybil and whitewashing attacks. Thus, we limit our scope to those three attacks to keep the comparisons concise in Table 2. *CertainTrust* model is resistant to sybil and FPA attacks, while *EigenTrust* is resistant to sybil and *Buchegger's model* and *socialREGRET* are resistant to FPA attacks only. None of the models are resistant to whitewashing attacks.

Commercial models like *eBay* and *Epinions* provide a graphical interface (e.g., star rating) together with detailed information (e.g., detailed seller ratings, detailed opinions) to the customers. On the one hand, the graphical interface in commercial models does not provide comprehensive trust information but with the help of detailed information the models mitigate that problem. On the other hand, most of the trust models from the research community do not provide a graphical interface for trust representation except the *CertainTrust* model and the *Beta reputation system*.

Table 2 summarizes the comparison among *TR* models from commercial applications and research community's proposals with respect to the above mentioned trust properties.

Discussion

From the analysis of different *TR* models in the previous section, it can be evidenced that most of the models we surveyed in this paper need significant improvement to be used in the Cloud computing environments. Specifically, multi-faceted trust computation and *transfer of trust* properties are important in order to accommodate different service delivery contexts and multiple parameters that are needed to establish trust on Cloud providers. Trust evaluation approaches, especially the *outside-in* approach, are essential to evaluate the trustworthiness of Cloud providers of complex composite services or distributed systems. Thus, trust evaluation approaches should consider the trustworthiness of underlying subsystems and components of complex

Table 2 Characterization of existing trust and reputation (TR) models and systems

Properties	Trust computation			Trust customization	Trust aggregation	Trust evaluation	Transfer trust across contexts	Attack resistance (FPA/S/W)[3]	Transparent trust information[4] (UI/C)
TR models	Multi-criteria	Multi-root (S/H)[1]	Multi-context	Global trust (G) vs Local trust (L)	Centralized (C) vs Decentralized (D)	(Bb vs Io vs Oi)[2]			
eBay	N	S/-	N	G	C	Bb	No	-/-/-	UI/C
Epinions	Y	S/-	Y	G	C	Bb	No	-/-/-	UI/C
Beta Reputation	N	S/-	N	G	C	Bb	No	-/-/-	UI/-
CertainTrust	N	S/-	N	L	D	Bb	No	FPA/S/-	UI/C
FIRE	N	S/H	N	L	D	Bb	No	-/-/-	-/-
EigenTrust	N	S/-	N	G	D	Bb	No	-/S/-	-/-
socialREGRET	N	S/-	N	L	D	Bb	No	FPA/-/-	-/-
TidalTrust	N	S/-	N	L	D	Bb	No	-/-/-	-/-
RFSN	N	S/-	N	L	D	Bb	No	-/-/-	-/-
GridEigenTrust	N	S/-	Y	G	D	Io	No	-/-/-	-/-
Abawajy's model	N	S/-	N	G	C	Bb	No	-/-/-	-/-
TESM	Y	S/H	N	L	D	Io	No	-/-/-	-/-
Unitec	N	S/-	N	G	D	Bb	No	-/-/-	-/-
BNTM	Y	S/-	Y	L	D	Bb	No	-/-/-	-/-
Buchegger's model	N	S/-	N	L	D	Bb	No	FPA/-/-	-/-
Billhardt's model	N	S/-	N	L	D	Bb	Yes	-/-/-	-/-
Hang's model	N	S/-	N	L	D	Oi	No	-/-/-	-/-

[1](S=Soft trust; H=Hard trust).
[2](Bb=Black box; Io=Inside-out; Oi=Outside-in).
[3](FPA=False Praise Accusation; S=Sybil attack; W=Whitewashing attack).
[4](UI=User Interface; C=Comprehensiveness).

systems. Attack resistance is also an essential property for trust models in general. Trust model in Cloud environments should also possess this property to ensure reliable trust score for consumers. Finally, consumers need an intuitive trust representation (graphical interface with comprehensive trust information) which is also very important in terms of transparency and usability. All these specific properties are essential for integrating in a unified trust evaluation framework (cf. Figure 3) (i.e., trust management system [25]) by means of TR models.

Conclusions

This article is the first survey focusing on the technical solution to the obstacles for adopting Cloud computing by means of TR models and systems. We provide a extended Cloud taxonomy to better understand the diversified market structure and how it is related to the adoption of Cloud computing. We have discussed the necessity of trust establishment and its influence on the adoption of Cloud computing from the perspective of Cloud entities. We have classified the current trends of trust establishment and identified their limitations by means of a use case where a healthcare provider face the challenge of selecting the most trustworthy Cloud provider. We have demonstrated the value of unified trust evaluation framework (i.e., a trust management system) by means of TR models and their required properties for establishing trust in Cloud environments. These properties and corresponding challenges are valuable for future research in designing trust-aided evaluation framework for Cloud environments.

TR models and systems provide mean for trustworthy interactions in online communities. Understanding the existing models/systems and their comparison in terms of required properties is an important first step towards developing robust systems in the future. This article has aimed to provide rigid properties to compare the existing models/systems and bring understanding of these systems to a broader Cloud computing community, including trust-aided system developers and practitioners.

Abbreviations

TR: Trust and Reputation; SaaS: Software as a Service; PaaS: Platform as a Service; IaaS: Infrastructure as a Service; DaaS: Data as a Service; NaaS: Network as a Service; IPMaaS: Identity and Policy Management as a Service; VPN: Virtual Private Lan; CPs: Cloud Providers; CBs: Cloud Brokers; CRs: Cloud Resellers; CCs: Cloud Consumers; OS: Operating System; IT: Information Technology; SLAs: Service Level Agreements; SMEs: Small and Medium-sized Enterprises; HIPAA: Health Insurance Portability and Accountability Act; CAIQ: Consensus Assessments Initiative Questionnaire; STAR: Security, Trust & Assurance Registry; CSA: Cloud Security Alliance; SAS 70: Statement on Auditing Standards (SAS) No. 70; FISMA: Federal Information Security Management Act; ISO 27001: International Organization for Standardization 27001; CCM: Cloud Control Matrix; PCI: Payment Card Industry; NIST: National Institute of Standards and Technology; QoS: Quality of Service; TPM: Trusted Platform Module; CDN: Content Delivery Node; P2P: Peer to Peer; OSN: Online Social Networks; WSN: Wireless Sensor Networks.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

SMH carried out the studies of cloud computing, trust and reputation models from various application fields, drafted the manuscript, and coordinated the task among authors. SH has critically reviewed the paper and drafted the manuscript, especially the "Adoption of cloud computing" section. SR has critically reviewed the paper and drafted the article, especially the trust related sections. MM has contributed to the concept of "trust in cloud computing" and reviewed the manuscript. All authors read and approved the final manuscript.

Authors' information

Sheikh Mahbub Habib is a doctoral researcher at the Center for Advanced Security Research Darmstadt (CASED) and research assistant at the Telecooperation Lab (TK) of Technische Universitt Darmstadt Germany. He is working on computational trust models and how those models can be adapted in trust management for complex distributed service environments (e.g., cloud computing). Earlier, he earned M.Sc. in Networks and Distributed Systems, specializing in security and distributed systems from Chalmers University of Technology Sweden. His current research interests includes trust and reputation models, logical reasoning of trust, trust management techniques, trust enhanced security techniques and their application in complex distributed systems.

Sascha Hauke is a doctoral researcher and research assistant at the Center for Advanced Security Research Darmstadt (CASED) and the Telecooperation Lab (TK) of Technische Universitt Darmstadt, Germany. He is working on developing techniques for extending reputation-based trust models into advanced trust management solutions. He received the degree of Diplom-Informatiker (Dipl.-Inform.) from the Westflische Wilhelms-Universitt Mnster (WWU), specializing in machine learning, soft computing and linguistics. His current research interests include reputation-based trust management, the application of machine learning techniques for prediction and their application in service oriented environments.

Sebastian Ries was born in 1979. At the time of writing this article, he was the coordinator of the research area Secure Services at the Center for Advanced Security Research Darmstadt (since 2009). Furthermore he was the head of the research group Smart Security & Trust at the Telecooperation Lab (TK), Technische Universität Darmstadt, Germany, since 2008, and a principle investigator at CASED since 2010. He obtained his Doctor and Diploma degrees in Computer Science from Technische Universität Darmstadt obtained in 2009 and 2005, respectively. He was awarded with research scholarships by the German National Science Foundation (DFG) and CASED, while preparing his dissertation. His research interests include trust and reputation models, trust establishment in complex systems, as well as challenges in the fields of identity management, privacy, and usable security.

Max Mühlhäuser is a full professor at the Technische Universitt Darmstadt, Germany, where he heads the Telecooperation Lab (TK) and coordinates a division of the Center for Advanced Security Research Darmstadt (CASED). After his doctorate and a leading position in industrial research, he held permanent or visiting professorships in Kaiserslautern (D), Karlsruhe (D), Linz (A), Montral, Sophia Antipolis (F), and San Diego. With his team, he covers a broad range of Ubiquitous Computing research topics in three complementary fields: 1) ubiquitous interaction issues such as interaction concepts for future devices, proactive, context aware, and multi device interaction; 2) issues of large scale networks (OSN, P2P, WSN) and smart spaces such as middleware, context and location awareness, discovery and composition, and knowledge work; 3) ubiquitous privacy and trust, and resilience for critical infrastructures.

Acknowledgements

This work is supported by Center for Advanced Security Research Darmstadt (CASED). Additionally, the authors would like to thank the anonymous reviewers for their comments and suggestions to enhance the quality of this manuscript.

Received: 1 January 2012 Accepted: 25 June 2012
Published: 23 August 2012

References

1. Khan KM, Malluhi Q (2010) Establishing trust in cloud computing. IT Professional 12: 20–27
2. Fujitsu Research Institute (2010) Personal data in the cloud: A global survey of consumer attitudes. Technical Report, Fujitsu Research Institute
3. Uusitalo I, Karppinen K, Juhola A, Savola R (2010) Trust and cloud services - an interview study. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, p. 712–720
4. Jøsang A, Ismail R, Boyd C (2007) A survey of trust and reputation systems for online service provision. Decision Support Syst 43(2): 618–644
5. Everett C (2009) Cloud computing - a question of trust. Computer Fraud & Security 2009(6): 5–7
6. Mouline I (2009) Why assumptions about cloud performance can be dangerous to your business. Cloud Comp J 2(3): 24–28
7. Takabi H, Joshi J, Ahn G (2010) Security and privacy challenges in cloud computing environments. Security Privacy. IEEE 8(6): 24–31
8. Ristenpart et al. (2009) Hey, you, get off of my cloud! exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM CCS 2009. ACM Press, Newyork, p. 199–212
9. Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In:Proceedings of the 2009 ACM workshop on Cloud computing security. ACM Press, p. 85–90
10. CSA (2009) Security guidance for critical areas of focus in cloud computing v2.1. Technical report, Cloud Security Alliance
11. ENISA (2009) Cloud computing- benefits risks and recommendations for information security. Technical report, ENISA
12. Habib SM, Ries S, Muhlhauser M (2010) Cloud computing landscape and research challenges regarding trust and reputation. Ubiquitous Autonomic and Trusted Computing, Symposia and Workshops on, 410–415
13. Bias R (2009) Challenges embracing cloud storage. SNIA Cloud Storage Summit- Winter Symposium 2009
14. Mell P, Grance T (2009) The nist definition of cloud computing. Nat Inst Standards Technol 53(6): 50
15. Hanna S (2009) Cloud computing: Finding the silver lining. http://www.ists.dartmouth.edu/events/abstract-hanna.html. Accessed 11 Aug 2012
16. National Institute of Standards and Technology (2011) Nist cloud computing reference architecture: Version 1. NIST Meeting Report
17. OpenCrowd Cloud taxonomy (2012) OpenCrowd Web Portal. http://cloudtaxonomy.opencrowd.com/taxonomy/ Accessed 30 July 2012
18. Schmitz R (2009) Los angeles moves to gmail and 'cloud' computing. http://www.npr.org/templates/story/story.php?storyId=114300948. Accessed 11 Aug 2012
19. CSA (2011) Cloud Controls Matrix. https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/ Accessed 15 July 2012
20. Gartner Inc. (2010) Gartner highlights key predictions for it organizations and users in 2010 and beyond. http://www.gartner.com/it/page.jsp?id=1278413. Accessed 11 Aug 2012
21. Armbrust et al. (2009) Above the clouds: A berkeley view of cloud computing. Technical report, EECS Department, University of California, Berkeley
22. ENISA (2009) An sme perspective on cloud computing-survey. Technical report, ENISA
23. McKnight DH, Chervany NL (1996) The meanings of trust. Technical report, Management Information Systems Research Center, University of Minnesota, USA
24. Mark Williams (2010) Reported cloud outages for Amazon, Google, Microsoft and Salesforce.com in 2008 and 2009. http://blog.muoncloud.com/2010/01/31/reported-cloud-outages-for-amazon-google-microsoft-and-salesforce-com-in-2008-and-2009/. Accessed 11 Aug 2012
25. Jøsang A, Keser C, Dimitrakos T (2005) Can we manage trust?. In: Herrmann P, Issarny V, Shiu S (eds) Trust Management, Third International Conference, iTrust 2005, 93–107. Proceedings, Springer, Paris, France, May 23-26, 2005
26. Gambetta D (2000) Can We Trust Trust? In: Trust: Making and Breaking Cooperative Relations, Department of Sociology, University of Oxford. pp. 213–237
27. Ries S (2009) Extending bayesian trust models regarding context-dependence and user friendly representation. In: Proceedings of the 2009 ACM Symposium on Applied Computing. ACM, New York. pp 1294–1301
28. Ries S (2009) Trust in Ubiquitous Computing. PhD thesis, Technische Universität Darmstadt
29. CSA (2011) Consensus Assessments Initiative. https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/ Accessed 15 July 2012
30. CSA (2011) Security, Trust & Assurance Registry. https://cloudsecurityalliance.org/research/initiatives/star-registry/ Accessed 25 July 2012
31. Haq IU, Brandic I, Schikuta E (2010) Sla validation in layered cloud infrastructures. In: GECON. Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg. 153–164
32. 3Tera Applogic (2009) 3tera's Cloud Computing SLA goes live. http://blog.3tera.com/computing/175/. Accessed 11 Aug 2012
33. Cloud Computing Use Cases Discussion Group (2010) Cloud computing use cases white paper Version 4.0. Cloud Computing Use Cases Discussion Group
34. SearchCIO (2009) Amazon gets SAS 70 Type II audit stamp, but analysts not satisfied. http://searchcloudcomputing.techtarget.com/news/1374629/Amazon-gets-SAS-70-Type-II-audit-stamp-but-analysts-not-satisfied Accessed 11 Aug 2012
35. Cloud Commons (2011) Cloud Commons Learn About SMI. http://beta-www.cloudcommons.com/web/cc/about-smi Accessed 15 July 2012
36. SpotCloud (2011) Cloud Capacity Marketplace. http://www.spotcloud.com/ Accessed 15 July 2012
37. Akerlof G (1970) A market for lemons. Q J Economics 84(3): 488–500
38. Ruohomaa S, Kutvonen L, Koutrouli E (2007) Reputation management survey In: The Second International Conference on Availability, Reliability and Security (ARES). pp 103–111
39. Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C (2010) Distributed trust management for validating sla choreographies. In: Grids and Service-Oriented Architectures for Service Level Agreements. Springer, US, pp 45–55
40. Teacy WTL, Patel J, Jennings NR, Luck M (2006) Travos: Trust and reputation in the context of inaccurate information sources. Autonomous Agents and Multi-Agent Syst 12(2): 183–198
41. Abawajy J (2009) Determining service trustworthiness in intercloud computing environments. Int Symp Parallel Architectures, Algorithms, and Networks 0: 784–788
42. Wang SX, Zhang L, Wang S, Qiu X (2010) A cloud-based trust model for evaluating quality of web services. J Comput Sci Technol 25: 1130–1142
43. Wang Y, Vassileva J (2007) A review on trust and reputation for web service selection. IEEE Computer Society, Washington. pp 25
44. Bin L, Lee G, Loughlin JO (2010) Towards application-specific service level agreements: Experiments in clouds and grids. In: Antonopoulos N Gillam L (eds) Cloud Computing. Volume 0 of Computer Communications and Networks. Springer, London, pp 361–372
45. Nagarajan A, Varadharajan V (2011) Dynamic trust enhanced security model for trusted platform based services. Future Gener Comput Syst 27: 564–573
46. Tavakolifard M, Knapskog S, Herrmann P (2008) Trust transferability among similar contexts. In: Proceedings of the 4th ACM symposium on QoS and security for wireless and mobile networks. ACM Press, Newyork, pp 91–97
47. Jeh G, Widom J (2002) Simrank: a measure of structural-context similarity. KDD '02. ACM, New York, pp 538–543
48. Gergö T (2007) Specification and state of the art report for the club concept. http://p2p-fusion.mokk.bme.hu/w/images/archive/9/92/20070614214657!Trust_systems.pdf Accessed 11 Aug 2012
49. Schryen G, Volkamer M, Ries S, Habib SM (2011) A formal approach towards measuring trust in distributed systems. In: Proceedings of the 2011 ACM Symposium on Applied Computing. SAC '11. ACM Press, Newyork, pp 1739–1745
50. Ries S, Habib SM, Mühlhäuser M, Varadharajan V (2011) Certainlogic: A logic for modeling trust and uncertainty (short paper). In: Trust and Trustworthy Computing. Volume 6740 of Lecture Notes in Computer Science. Springer, Berlin / Heidelberg, pp 254–261
51. Hang CW, Singh MP (2011) Trustworthy service selection and composition. ACM Transactions on Autonomous and Adaptive Systems Volume 6(Issue 1). Article 5, 17 pages

52. Kerr R, Cohen R (2009) Smart cheaters do prosper: defeating trust and reputation systems. In: AAMAS '09: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems, pp. 993–1000
53. Jøsang A, Golbeck J (2009) Challenges for robust of trust and reputation systems. In: Proceedings of the 5th Int. Workshop on Security and Trust Management (STM2009)
54. eBay Inc (2011) eBay homepage. http://www.ebay.com Accessed 20 July 2012
55. Epinions (2011) Epinions homepage. http://www.epinions.com Accessed July 20 2012
56. Jøsang A, Ismail R (2002) The beta reputation system. In: Proceedings of the 15th Bled Conference on Electronic Commerce
57. Huynh TD, Jennings NR, Shadbolt NR (2006) An integrated trust and reputation model for open multi-agent systems. Autonomous Agents and Multi-Agent Syst 13(2): 119–154
58. Kamvar SD, Schlosser MT, Garcia-Molina H The eigentrust algorithm for reputation management in p2p networks. ACM Press, Newyork, pp 640–651
59. Sabater J, Sierra C (2002) Reputation and social network analysis in multi-agent systems. In: Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1. ACM Press, pp. 475–482
60. Sabater J (2003) Trust and reputation for agent societies. Universitat Autnoma de Barcelona, Spain
61. Golbeck J (2005) Computing and Applying Trust in Web-Based Social Networks. University of Maryland, USA
62. Ganeriwal S, Balzano LK, Srivastava MB (2008) Reputation-based framework for high integrity sensor networks. ACM Trans Sen Netw 4(3): 1–37
63. von Laszewski G, Alunkal BE, Veljkovic I (2005) Towards reputable grids. calable Comput: Pract and Experience 6(3): 95–106
64. Kinateder M, Baschny E, Rothermel K Towards a Generic Trust Model Comparison of Various Trust Update Algorithms. In: Proceedings of the Third International Conference on Trust Management: iTrust'05; Rocquencourt, France, May 23-26, 2005. Springer-Verlag, Berlin, Heidelberg, pp 119–134
65. Wang Y, Vassileva J (2003) Bayesian network-based trust model. IEEE Computer Society, Washington, pp 372–378
66. Buchegger S, Le Boudec J Y (2004) A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks. In: P2PEcon 2004
67. Billhardt H, Hermoso R, Ossowski S, Centeno R (2007) Trust-based service provider selection in open environments. In: SAC '07: Proceedings of the 2007. ACM Symposium on Applied Computing. ACM Press, Newyork,. pp. 1375–1380

doi:10.1186/2192-113X-1-19
Cite this article as: Habib *et al.*: **Trust as a facilitator in cloud computing: a survey.** *Journal of Cloud Computing: Advances, Systems and Applications* 2012 **1**:19.