Journal of Cloud Computing
a SpringerOpen Journal

RESEARCH Open Access

Trust mechanisms for cloud computing

Jingwei Huang* and David M Nicol

Abstract

Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self assessment by providers of cloud services. We begin this paper with a survey of existing mechanisms for establishing trust, and comment on their limitations. We then address those limitations by proposing more rigorous mechanisms based on evidence, attribute certification, and validation, and conclude by suggesting a framework for integrating various trust mechanisms together to reveal chains of trust in the cloud.

Keywords: Trust, Cloud computing, Trust mechanisms, Reputation, QoS, SLA, Transparency-based trust, Formal accreditation, Cloud audit, Policy-based trust, Evidence-based trust, Attribute certification

Introduction

Cloud computing has become a prominent paradigm of computing and IT service delivery. However, for any potential user of cloud services, they will ask "can I trust this cloud service?" Furthermore, what exactly does "trust" mean in the context of cloud computing? What is the basis of that trust? If the attributes of a cloud service (or a service provider) are used as evidence for trust judgment on the service (or provider respectively), on what basis should users believe the attributes claimed by cloud providers? Who are authorities to monitor, measure, assess, or validate cloud attributes? The answers to those questions are essential for wide adoption of cloud computing and for cloud computing to evolve into a trustworthy computing paradigm. As addressed in [1], "the growing importance of cloud computing makes it increasingly imperative that we grapple with the meaning of trust in the cloud and how the customer, provider, and society in general establish that trust."

The issues and challenges of trust in cloud computing have been widely discussed from different perspectives [2-10]. A number of models and tools have been proposed [11-13]. Each contributes a partial view of cloud trust, but lacking still is a complete picture illustrating how cloud entities work together to form a "societal" system, with a solid grounding in trust, serving to facilitate trusted paths to trusted cloud services. The NIST Cloud Computing Reference Architecture [14] identified cloud brokers and cloud auditors as entities who conduct assessment of cloud services; however, there are few studies on trust relation analysis and the chains of trust from cloud users to cloud services (or providers) through those intermediary cloud entities. In this paper, we investigate trust mechanisms for the cloud, present our vision of the "societal systems mechanisms" of trust and a framework for analyzing trust relations in the cloud, and suggest trust mechanisms which combine attribute certification, evidence-based trust and policy-based trust.

Because of the criticality of many computing services and tasks, some cloud clients cannot make decisions about employing a cloud service based solely on informal trust mechanisms (e.g. web-based reputation scores); these decisions need to be based on formal trust mechanisms, which are more certain, more accountable, and more dependable. Here, the word "formal" is meant to carry the sense of "official" assessment in a society. In our suggested cloud trust mechanisms, the attributes of a cloud service (or its provider) are used as evidence for the user's trust judgment on the service (or provider), and the belief in those attributes is based on "formal" certification and chains of trust for validation.

In this paper, we focus somewhat informally on the conceptual basis for analysis of trust in the cloud; we do not at this time address mathematical modeling, which would involve many more precise details, formal languages, and specific use cases. With respect to terminology, an "entity" is an autonomous agent; a "cloud entity" refers to an entity in the cloud, such as a cloud provider, a cloud user, a cloud broker, and a cloud auditor; "semantics of trust" refers to

*Correspondence: jingwei@iti.illinois.edu
Information Trust Institute, University of Illinois at Urbana-Champaign 1308 West Main Street, Urbana, Illinois 61801, USA

precisely defined meaning of trust, including the relations among the components of trust.

This paper is organized as the following sections: (1) we define the *semantics of trust*; (2) we review the *state-of-the-art trust mechanisms* for cloud computing; (3) we discuss *policy-based trust judgment*, which is a real formal trust mechanism used in Public Key Infrastructure (PKI) practice. By policy-based trust, a cloud service or service provider can be trusted if it conforms to a trusted policy; (4) we present a general structure of *evidence-based trust*, by which particular attributes of a cloud service or attributes of a service provider are used as evidence for trust judgment; (5) we discuss *attribute assessment and attribute certification*, by which some attributes of a cloud service (or service provider) are formally certified, and the belief in those attributes is based on formal certification and chains of trust for validation; (6) we present an integrated view of the trust mechanisms for cloud computing, and analyze the trust chains connecting cloud entities; (7) finally, we give a summary and identify further research.

Semantics of trust

The term "trust" is often loosely used in the literature on cloud trust, frequently as a general term for "security" and "privacy", such as [4]. What exactly does "trust" mean?

Trust is a complex social phenomenon. Based on the concepts of trust developed in social sciences [15,16], we use the following definition [17]:

> *Trust is a mental state comprising: (1)* ***expectancy*** *- the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2)* ***belief*** *- the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; (3)* ***willingness to take risk*** *- the trustor is willing to take risk for that belief.*

It is important to understand that the expected behavior of trustee is beyond the trustor's control; the trustor's belief in that expected behavior of trustee is based on the trustee's capability, goodwill (including intension or motivation), and integrity. The integrity of the trustee gives the trustor confidence about the predictability of the trustee's behavior.

We identify two types of trust, based on the trustor's expectancy: *trust in performance* is trust about what the trustee performs, whereas *trust in belief* is trust about what the trustee believes. The trustee's performance could be the truth of what the trustee says or the successfulness of what the trustee does. For simplicity, we represent both as a statement, denoted as a Boolean-type term, x, called a reified proposition [18]. For the first case, x is what the trustee says; for the second, x represents a successful performance, which is regarded as a statement that the trustee made, describing his or her performance. A *trust in performance* relationship, $trust\_p(d, e, x, k)$, represents that trustor d trusts trustee e regarding e's performance x in context k. This relationship means that if x is made by e in context k, then d believes x in that context. In first-order logic (FOL),

$$trust\_p(d, e, x, k) \equiv madeBy(x, e, k) \supset believe(d, k\dot{\supset}x) \tag{1}$$

where $\dot{\supset}$ is an operator used for reified propositions to mimic the logical operator for implication, $\supset$. A *trust in belief* relationship, $trust\_b(d, e, x, k)$, represents that trustor d trusts trustee e regarding e's belief (x) in context k. This trust relationship means that if e believes x in context k, then d also believes x in that context:

$$trust\_b(d, e, x, k) \equiv believe(e, k\dot{\supset}x) \supset believe(d, k\dot{\supset}x). \tag{2}$$

Trust in belief is transitive; *trust in performance* is not; however, *trust in performance* can propagate through *trust in belief*. A more detailed account can be found in [17,19].

From the definition above, the trustor's mental state of belief in his expectancy on the trustee is dependent on the evidence about the trustee's competency, integrity, and goodwill. This leads to logical structures of reasoning from belief in evidence to belief in expectancy. We will discuss this later in § 'Evidence-based trust'.

The semantics of trust in the context of cloud computing has the same semantic structure as stated above; what still needed are the specific expectancy and the specific characteristics of cloud entities's competency, integrity, and goodwill in the context of cloud computing. We will discuss further in § 'Evidence-based trust'.

State-of-the-art trust mechanisms in clouds

In this section, we discuss existing trust mechanisms in the cloud. From the discussion, we will see that each of the mechanisms addresses one aspect of trust but not others.

Reputation based trust

Trust and reputation are related, but different. Basically, trust is between two entities; but the reputation of an entity is the aggregated opinion of a community towards that entity. Usually, an entity that has high reputation is trusted by many entities in that community; an entity, who needs to make trust judgment on an trustee, may use the reputation to calculate or estimate the trust level of that trustee.

Reputation systems are widely used in e-commerce and P2P networks. The reputation of cloud services or cloud service providers will undoubtably impact cloud users' choice of cloud services; consequently, cloud providers

try to build and maintain higher reputation. Naturally, reputation-based trust enters into the vision of making trust judgment in cloud computing [11,13,20].

Reputation is typically represented by a comprehensive score reflecting the overall opinion, or a small number of scores on several major aspects of performance. It is unrealistic to ask a large number of cloud users to rate a cloud service or service provider against a large set of complex and fine-grained criteria. The reputation of a cloud service provider reflects the overall view of a community towards that provider, therefore it is more useful for the cloud users (mostly individual users) in choosing a cloud service from many options without particular requirements. Reputation may be helpful when initially choosing a service, but is inadequate afterwards. In particular, as a user gains experience with the service, the trust placed on that service meeting performance or reliability requirements will evolve based on that experience.

SLA verification based trust

"Trust, but verify" is a good advice for dealing with the relationships between cloud users and cloud service providers. After establishing the initial trust and employing a cloud service, the cloud user needs to verify and reevaluate the trust. A service level agreement (SLA) is a legal contract between a cloud user and a cloud service provider. Therefore, quality of service (QoS) monitoring and SLA verification is an important basis of trust management for cloud computing. A number of models that derive trust from SLA verification have been proposed [12,13].

A major issue is that SLA focuses on the "visible" elements of cloud service performance, and does not address "invisible" elements such as security and privacy. Another issue is that many cloud users lack the capability to do fine grained QoS monitoring and SLA verification on their own; a professional third party is needed to provide these services. In a private cloud, there may be a cloud broker or a trust authority (e.g. RSA's CTA, to be discussed later in § 'Cloud transparency mechanisms'), whom is trusted in the trust domain of the private cloud; so the trusted broker or trust authority can provide the users in the private cloud the services of QoS monitoring and SLA verification. In a hybrid cloud or interclouds, a user within a private cloud might still rely on the private cloud trust authority to conduct QoS monitoring and SLA verification; however, in a public cloud, individual users and some small organizations without technical capability may use a commercial professional cloud entity as trust broker. We discuss this in § 'Trust as a service'.

Cloud transparency mechanisms

Transparency and accountability are a recognized basis for gaining trust on cloud providers. To increase transparency of the cloud, the Cloud Security Alliance (CSA) launched the "Security, Trust & Assurance Registry (STAR)" program [21], a free publicly accessible registry which allows cloud service providers to publish self-assessment of their security controls, in either a "Consensus Assessments Initiative Questionnaire (CAIQ)" or a "Cloud Controls Matrix (CCM)", which embody CSA published best practices. CAIQ contains over 140 questions which cloud users or auditors may ask; CCM is a framework describing how a cloud provider aligns with the CSA security guide [22]. Examples of cloud providers' self-assessments can be found at the CSA STAR website [23]. STAR is a useful source for users seeking cloud services. However, the information offered is a cloud provider's *self*-assessment; cloud users may want assessments performed by some independent third-party professional organizations.

Different from STAR, CSC.com proposed [24] and CSA adopted the CloudTrust Protocol (CTP) [25], a request-response mechanism for a cloud user to obtain specific information about the "elements of transparency" applied to a specific cloud service provider; the elements of transparency cover aspects of configuration, vulnerability, audit log, service management, service statistics, and so forth. "The primary purpose of the CTP and the elements of transparency is to generate evidence-based confidence that everything that is claimed to be happening in the cloud is indeed happening as described, ..., and nothing else" [26]. CTP provides an interesting channel between cloud users and cloud service providers, allowing users internal observations of cloud service operations. However, like STAR, an essential weakness of CTP is that its information is provided by cloud service provider itself. Dishonest cloud service providers can filter out or change the data. From the point of view of a trust judgement, it raises questions of the data's reliability.

Trust as a service

We have already noted the need for employing third-party professionals for QoS monitoring and SLA verification. Independent assessment has utility in other aspects of cloud computing, as well.

RSA announced the *Cloud Trust Authority* (CTA) [27] as a cloud service, called Trust as a Service (TaaS) to provide a single point for configuring and managing security of cloud services from multiple providers. The initial release of the CTA includes: *identity service*, enabling single sign-on among multiple cloud providers, and *compliance profiling service*, enabling a user to view the security profiles of multiple cloud providers against a common benchmark. The CTA is a tool specialized on cloud trust management, and is developed from RSA's philosophy of "trust = visibility + control" [28]. As a cloud-based tool, the CTA could largely simplify cloud users' trust

management. However, a cloud user must still make trust judgment about the cloud service assertions streamed in the CTA, because those assertions were made by cloud service providers themselves. Most importantly, a cloud user needs to judge the trustworthiness of the CTA in role as an intermediary.

The essential issue of any TaaS mechanism is about what is the basis of the trust relation between cloud users and those commercial trust brokers. We will discuss the answers later in subsections 'Trust judgement on a cloud broker' and 'Trust judgment on a cloud service provider'.

Formal accreditation, audit, and standards

Because self-assessment exercises may be compromised by dishonesty, some argue that formal accreditation from a trusted independent authority is necessary for a healthy cloud market; some others argue that formal accreditation "would stifle industry innovation" [2].

External audits, attestations, or certifications for more general purpose (not specific to clouds) have been used in practice. Examples include: the ISO/IEC 27000 series, which are international information security management standards [29]; "Statement on Standards for Attestation Engagements No. 16" (SSAE 16) [30], which is an attestation standard for service organizations, put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). SSAE 16 is replacing the older standard "Statement on Auditing Standards No. 70" (SAS 70); "The International Standard on Assurance Engagements 3402" (ISAE 3402) [31], which is a globally recognized standard for assurance reporting on service organizations.

Specific to cloud computing, in addition to CTP and STAR (for self-assessment), CSA also launched the CloudAudit initiative, which provides a common interface and namespace for cloud providers to produce audit assertions, and allows cloud users to automate use of that data in their own audit processes. CloudAudit could facilitate automated cloud audit, conducted by cloud providers (for self-audit), cloud users (for cloud user-audit), and cloud auditors (for formal audit). CloudAudit, CCM, CAIQ, and CTP form the CSA Governance, Risk Management and Compliance (GRC) stack.

To ensure trustworthiness, the International Grid Trust Federation (IGTF) issued GFD-I.169 as guidelines for auditing the cloud/grid assurance bodies – the certification authorities (CAs) issuing X.509 certificates [32].

A formal process for assessment of cloud services and their providers by independent third parties, acceptable to both cloud users and providers, does not yet exist. Formal accreditation specific to independent third-party cloud assessors also does not exist.

Further discussion

A reputation-based trust mechanism reflects the overall view of a community towards a cloud service provider. It can help with cloud service selection; but is insufficient for other important purposes.

After establishing an initial trust on a cloud service, a cloud user needs to verify and re-evaluate that trust. QoS monitoring and SLA verification based trust mechanism can help to manage the existing cloud trust relations. The QoS/SLA mechanism can manage "visible" elements of the black box of a cloud service, such as performance; but it cannot help to manage the "invisible" elements inside a cloud service, such as privacy protection.

Cloud transparency mechanisms provide channels for cloud users to "observe" how cloud service providers operate. The mechanisms help to establish trust by making the cloud services more "visible". The essential issue of the transparency mechanisms is that the information is provided by cloud service providers themselves; thus we need to identify the basis for cloud users to trust them.

The TaaS mechanism provides cloud users a solution where the sophisticated tasks of cloud trust management can be delegated to third-party professionals. However similarly the basis for cloud users to trust them needs to be estabulished.

One possible solution to the problems posed in the above mechanisms is formal accreditation and audit. The mechanisms of formal accreditation and audit in the cloud do not exist yet and are still in discussion.

In the rest of this paper, we continue to explore the cloud trust mechanisms by borrowing policy-based trust mechanism from PKI, combined with evidence-based trust and attribute certification and validation.

Policy-based trust

We earlier identified the need for "formal" trust mechanisms in cloud computing. In a related sphere, PKI is a widely used mature technology that employs "formal" trust mechanisms to support digital signature, key certification and validation, as well as attribute certification and validation. Can we apply trust ideas used in PKI to establish "formal" trust mechanisms to the cloud?

To simplify the discussion, consider the example illustrated in Figure 1. Alice has a digital document supposedly signed by Bob using his private key K_b'. To validate, she needs Bob's public key K_b. Assume that Alice trusts only her trust anchor certification authority CA_1, and she knows only K_1, her trust anchor's public key. In order for her to verify the signature on the document as being Bob's, she needs to discover a certification path (a chain of certificates) from CA_1 to CA_3 who has issued Bob's public key certificate. As shown in the figure, Alice uses CA_1's public key K_1 to validate CA_2's public key K_2; because Alice trusts CA_1 on public key certification, and CA_2's public

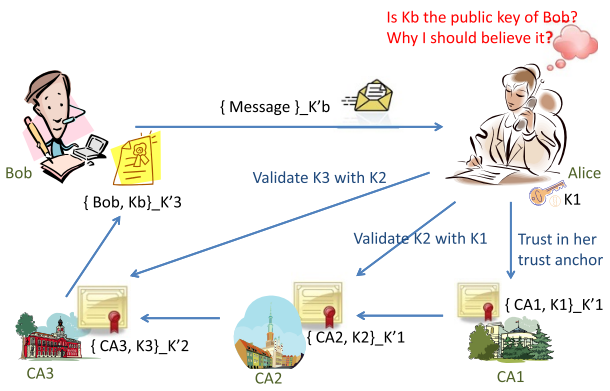

Figure 1 PKI trust example. This example reveals trust relations in public key certification and validation.

key is certified by CA_1, Alice can believe that CA_2's public key is K_2; then Alice uses K_2 to validate CA_3' public key K_3; and finally uses K_3 to validate Bob's public key K_b. The main issue is *why Alice should believe* K_3 *is* CA_3*'s public key and* K_b *is Bob's public key*?

Essentially, to infer belief in a statement "Bob's key is K_b", Alice needs to trust CA_3, the creator of that assertion, with respect to the truth of the statement; however, this raises questions that ask about the foundation of that trust, and how the trust is inferred or calculated. Some research suggests that the trust comes from recommendations along the chain of certificates by those certificate issuers [33]; but the practice of digital certification and validation in real PKI systems suggests that *the trust comes from compliance with certain certificate policies*.

As specified in IETF RFC 5280 [34], in addition to the basic statement that binds a public key with a subject, a public key certificate also contains a certificate policy (CP) extension. For a public key certificate issued to a CA, the certificate means that the issuing CA who conforms to the specified CP asserts that the subject CA has the certified public key, and the subject CA also adheres to the specified CP. As a result, to infer Alice's belief in CA_3's key and Bob's key, she must trust that CP in the sense that any CA conforming to that CP will generate valid public key certificates. There are more complex and interesting issues in PKI trust [35], but for the purpose of this paper, we will not go further.

In summary, as PKI is currently practiced, trust in a certification authority (CA) with respect to issuing and maintaining valid public key certificates is based on the CA's conformance with certain certificate policies. Certificate policies play a central role in PKI trust. We call this trust mechanism as *policy-based trust*.

Evidence-based trust

We now discuss using attributes as evidence to make trust decision.

From the definition of trust given in § 'Semantics of Trust', a trustor's belief in the expected behaviour of trustee is based on the evidence about the trustee's attributes of competency, goodwill, and integrity, with respect to that expectation. Formally, we could express a general form of evidence-based trust as follows:

$$believe(u, attr_1(s, v_1)) \wedge ... \wedge believe(u, attr_n(s, v_n)) \rightarrow trust\_*(u, s, x, c) \quad (3)$$

which states that if an individual u believes a subject s has attribute $attr_1$ with value v_1, ..., attribute $attr_n$ with value v_n, then u trusts (either *trust in belief* or *trust in performance*) s with respect to x, the performance of s or information created or believed by s, in a specific context c.

An entity's belief in an attribute assessment is dependent on whether the entity trusts the entity who makes that attribute assessment. Formally, based on the definition of trust-in-performance, formula (1) in § 'Semantics of Trust', we could have

$$trust\_p(u, a, attr(s, v), c) \wedge madeBy(attr(s, v), a, c) \wedge inContext(c) \rightarrow believe(u, attr(s, v)), \quad (4)$$

which states that if an individual u trusts an attribute authority a to make assertions about a subject s has attribute $attr$ with value v in a specific context c, a specific assertion $attr(s, v)$ is made by a in context c, and the context c is the case, then u believes that assertion. In the formula, $attr(s, v)$ is a reified proposition represented as a term. Since not only the attributes of a cloud service may be assessed and certified, but also the attributes of a cloud entity may be assessed and certified, in the above formula, we may use $attr(e, v)$ to state that cloud entity e has attribute $attr$ with value e. In this way, a logic formula similar to (4) can describe the relation from trust in a cloud auditor to the belief in the certified attribute of a cloud entity such as a service provider.

To use attributes as evidence in trust judgment, we organize the relevant attributes in a two-dimension space: (1) one dimension goes along the domain of the trustor's expectation on the trustee, in the context of cloud computing, including aspects of performance, security, and privacy; (2) another dimension goes along the source of trust, that is, what makes the trustor trust the trustee, including the trustee's competency (capability), integrity (consistency in performance and principles), and goodwill (motivation or intension).

Figure 2 illustrates a spectrum of attributes in cloud computing. Most commonly considered ones fall in the category of competency; attributes that reflect integrity and goodwill are frequently neglected, and should be included in trust judgment. To neglect these is to implicity assume that trust does not depend on them, or if it

Domain-specific expectation	Sources of trust		
	Competency	Good will / intention	Integrity / consistency
Performance	Availability; Reliability; ...	<Constant efforts to improve performance>	<Consistency shown by historic data>
Security	Security cert; Security breach rate; ...	<Constant efforts to improve security>	<Consistency shown by historic data>
Privacy	Privacy regulation compliance; Privacy violation rate; ...	<Constant efforts to improve privacy>	<Consistency shown by historic data>

Figure 2 Attributes for evidence-based trust. The attributes used for evidence-based trust judgment can be organized in two dimensions: (1) sources of trust, including competency, goodwill, and integrity; (2) domain-specific expectation.

does, that dependence is satisfied. Characterization and quantification of integrity and goodwill is an interesting research challenge. A trustee's historical behavior might reflect integrity; goodwill might be quantified as performance improvements are measured, and cloud users' feedback.

Different cloud users may have different trust policies, involving different trust attributes. A common trust *framework* supports evidence-based trust judgment for different users and different policies. The connection between evidence-based trust and policy-based trust is that the belief that an entity conforms to a trusted policy implies the belief that the entity has a set of attributes associated with that policy.

Attribute assessment and certification

When the attributes of a cloud service (or cloud entity) are used as evidence to make trust judgment on the service (or entity), the sources of attribute assessment must be trustworthy, and those attributes need to be distributed in a trustworthy way. In the following, we first discuss the source of attribute assertions and then we discuss attribute certification as a formal approach to deliver cloud attributes.

Sources of cloud attribute assessment

Assessment of attributes may come from several sources: the cloud user, other peer users, the service provider, cloud auditor/accrediator, and cloud broker. We discuss each of them in turn.

Cloud user observation

If a cloud user has already interacted with a cloud service or a cloud service provider, then the experience will be the user's direct basis for cloud attribute assessment. Experience is a fundamental factor of trust, and this kind of trust, called "interpersonal trust", has long been studied in both social sciences and computing science.

The advantage of using direct interaction experience is that the data used are first-hand and may be most relevant; the disadvantage is that the data accumulated are limited with respect to the sample size and the range of the usage of the cloud service. A specific user's experience is just one piece of the information revealing the trustworthiness of a cloud service.

Opinions of other peer users

When a cloud user has only limited direct experience with a cloud service (or none at all), other peer users' opinions could be an important source of cloud attribute assessment. The major issues are: can those peer reviewers be trusted with respect to their opinions on the cloud service? and how can those different opinions be aggregated?

There are at least two basic approaches to solving the problem: social network based and reputation based.

Social network based approach A cloud user takes one or more trusted friends' opinions, and combines them with that user's personal trust in each of those friends. That user may not have a direct trust relation with a "popular" reviewer, but the user may derive an indirect trust relation with that reviewer through a trust network [17,36], which is a specific form of social networks, comprising of only trust relations. The social network based approach is an analogue of how a person initially trusts an entity, unknown before in the real world. Models in this category are heuristic. Typically, one asks only a small number of trusted friends for their opinions. When a large number of peer users' opinions are involved, the approach becomes reputation based.

Reputation based approach A typical methodology is to aggregate a large number of peer user's ratings, often seen in e-commerce product/service ratings. The advantage is that the data used for assessment may cover many more situations and have a wider time-window of observations; this approach can have a much wider view on the cloud service (or its provider) than a single user does. On the other hand, some weaknesses exist: a large number of raters are required for meaningful and objective ratings; the raters and users should have a common understanding of the attribute semantics and the corresponding measurement; this approach is suitable for the purpose of overall rating, or is limited to rating a small number of attributes; the trustworthiness of individual voter are rarely taken into account; usually, as in e-commerce, the reputation of product/service is calculated by an organization in a centralized manner, so the organization may

manipulate the calculation, and the calculating service may become a single point of attack.

Statements from cloud service provider

Some cloud service attributes may be specified, promised, or revealed by its provider. In "service specification" and advertisements, a service provider will specify the featured attributes of a cloud service; the attributes of the service stated in a SLA are the promises of that service provider to that user. Through the CloudTrust Protocol (CTP) [26], cloud users can request and get a response from the provider about "the elements of transparency", the information concerning the compliance, security, privacy, integrity, and operational security history.

However, information about the attributes of a service given by the service provider are usually not directly believed by the first-time users. Sometimes a user may believe a service provider's statements or promises, based on the brand name or reputation of that service provider, or based on the user's past experience of interaction. In any case, the stated attributes are an important part of the watch-list in cloud service monitoring, and they are used to verify whether the service provider behaves as trusted. The conclusion of the verification will be used by the users to build or revise their trust in that service provider.

In general, the statements or promises about the attributes of a cloud service given by a cloud service provider itself need to be verified before used for decision making, and cloud attribute assertions from third party independent professional organizations are expected, which we discuss in the following subsections 'Assessment of cloud auditor/accreditor' and 'Observation of cloud brokers'.

Assessment of cloud auditor/accreditor

NIST identifies a cloud auditor as "a party that can conduct independent assessment of cloud services, information system operations, performance, and security of a cloud implementation. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc." [14]. Obviously, cloud audit is an important channel of cloud attribute assessment. A limitation of cloud auditing is that the trust assessment reflects only the state at the time of the audit. Trust changes dynamically, as a function of dynamic monitoring of behavior.

A cloud auditor's assessment is usually regarded as a reliable information source for trust judgment. To some cloud users, a cloud auditor as a third-party professional organization may be a satisfactory trust root. However, to some others, the trustworthiness of a cloud auditor also needs to be evaluated by looking into the auditor's attributes and/or policies. Since cloud audit is an important mechanism to ensure trustworthiness of clouds, each cloud auditor should be periodically audited and/or accredited by a professional association such as Auditing Standards Board of AICPA.

In formal accreditation, an entity who provides a professional service is assessed against official standards, and is issued with certification of its competency, authority, or credibility. The certification is provided by an accreditor, who is a third party independent authorized accreditation organization, and who is also accredited by a national standard body or professional association. If formal accreditation is applied to clouds, the cloud attribute assessment from a formal accreditation will be another important information source for cloud trust judgment.

Accreditation is somewhat similar to audit. In both cases an entity is assessed by an independent third party; however, there are subtle differences. First, they may have different focusing aspects of assessment. Accreditation focuses on the qualification of the accredited entity with respect to conducting a specific type of professional services; audit focuses on assessing the performance of the audited entity with respect to the common requirements of a society and/or the professional standards of a professional community. Secondly, audit typically takes place annually or once per half year; accreditation takes place in a longer period (e.g. every 5 years).

In summary, in context of cloud computing, the assessments by audit and accreditation are objective and "formal", but they are not real-time information as from real-time monitoring.

Observation of cloud brokers

Cloud brokers play an important role. By the NIST definition [14], a cloud broker is "an entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers." A cloud broker may provide services in three categories [14]: (1) service intermediation: for a given cloud service, to provide value-added additional services such as performance monitoring and security management; (2) service aggregation: to provide an integrated service by aggregating several cloud services from different providers; (3) service arbitrage: to select proper cloud services in an integrated service, based on the quantified evaluation of the alternative cloud services. The observation of a cloud broker can be an important source of cloud attribute assessment.

The advantages of broker observation include: real-time cloud service performance monitoring; feedback from many peer users; an ability to monitor and evaluate a collection of the same category of cloud services from different providers. A cloud broker potentially has a relatively complete picture of a cloud service.

However, again the question arises whether a cloud broker can be trusted with respect to assessing cloud

attributes. This depends on the relationship between broker and providers, and between broker and users. A tight business relation with some cloud providers may make the brokers' opinion be not as objective as the one made in formal audit or accreditation.

From the perspective of cloud market mechanism we imagine that if a cloud broker represents a cloud provider, then the cloud broker may provide information which favors that cloud provider; however, if a broker is independent, and its business depends on the trust relations with users, the broker is more motivated to find and provide information being truly helpful for cloud users. This situation may occur when a cloud broker serves as a gateway for a large number of cloud users in the cloud market. Consistent with the above view, we further imagine that if a cloud broker is highly trusted by some cloud users (especially, end cloud users), the broker may become those cloud users' trust anchor, taking care of trust management for those cloud users.

In order to ensure that a cloud broker behaves as a trustworthy cloud entity, cloud users will expect to learn how a cloud broker works, whether the broker is neutral, what policies the broker follows, and whether the broker has certain attributes that can be used as evidence to judge its trustworthiness. Therefore, essentially a cloud broker is also expected to be formally audited and/or accredited either.

Attribute certification

In addition to X.509 identity (public key) certification, there also exists X.509 *attribute certification* [37]. Public key certification is used in authentication; attribute certification is used for both authentication and authorization. An attribute certificate (AC) is a statement digitally signed by the AC issuer to certify that the AC holder has a set of specified attributes. The certified attributes can be access identity, authentication information (e.g. username/password pairs), group membership, role, and security clearance [37]. An AC mainly contains the following fields: unique AC identifier, AC holder, AC issuer, attribute-value pairs, valid period, the Id of the algorithm used to verify the signature of the AC, and extensions, which mainly include AC targeting – a list of specified servers or services where the AC can be used, and CRL (Certificate Revocation List) distribution points.

The current IETF X.509 AC standard [37] might be considered for use in cloud attribute certification, but it has several limitations.

First, the standard does not include important attributes needed in the cloud context. Extensions are possible to deal with this, but still no standards regarding service performance, security, and privacy. Second, with respect to attribute certification, the real authority behind attribute assertion is the entity who really knows the certified entity. For example, with respect to the role or membership of an entity in a specific organization, that organization is naturally the authority to state that attribute. From this point of view, we should discern the difference between "*attribute assertion authority*" (AAA) and *attribute certification authority* (ACA, i.e. AC issuer). We use AA (Attribute Authority) to refer to an entity who is both AAA and ACA. In the context of clouds, who plays the role of AA? From our earlier discussion, it is obvious that the most reliable sources for attribute assertion/assessment are independent third-party professional organizations such as cloud auditors and accreditors, and even cloud brokers.

Finally, current IETF X.509 AC standard [37] adopts a simple trust structure where "one authority issues all of the ACs for a particular set of attributes". In cloud applications (except for small scale private clouds) an AC issuer may be frequently outside the trust boundary of an AC user. Therefore, mechanisms for cross-domain attribute certification and validation are necessary for both hybrid cloud and public cloud.

An integrated view

Earlier, we envisioned that the attributes of a cloud service (or cloud entity) can be used as evidence for a cloud user to make trust judgment on the service (or entity); we discussed the sources of cloud attribute assessment and *attribute certification*; we also revealed that PKI in practice uses policy-based trust mechanism, which might be used in cloud computing either. In this section, we put together all those mechanisms, including: reputation based, SLA verification based, transparency based, formal accreditation and audit, as well as the suggested policy-based, evidence-based, and cloud attribute certification, to construct an overall framework for analyzing and modeling trust chains among cloud entities.

Figures 3, 4, 5 and 6 illustrate the dependence between the trust placed in various cloud entities and the sources of evidence for trust judgment. In these figures, the left part illustrates trust placed on different types of cloud entities; the right part illustrates trust mechanisms to be used, which are also the sources of evidence to support trust judgment; the arrows represent dependence relations between them; the dependence relations together form the chains of trust in the cloud. The six mechanisms shown in those pictures are an abstraction of typical mechanisms; a real system support trust judgment in practice may involve several mechanisms. For example, a cloud reputation system may calculate reputation scores, and also provide assessed attributes from brokers and users' reviews. The three mechanisms in the lower-right part with dotted border-lines are suggested ones and do not exist yet. Most mechanisms may support trust judgment on different types of cloud entities, but note that for

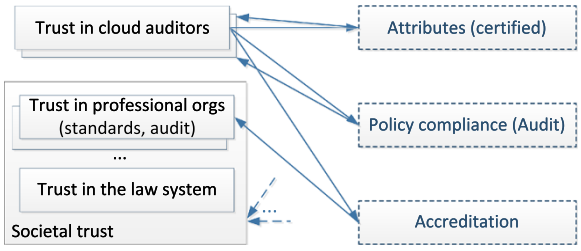

Figure 3 Evidence and chains for trust judgment on a cloud auditor. Trust placed in a cloud auditor is based on one or more of: (1) accreditation, which is further based on the trust placed on professional organizations making standards and audit/accreditation, – a part of societal trust; (2) policy compliance, which is audited by another trusted auditor; (3) attributes, certified by another trusted auditor.

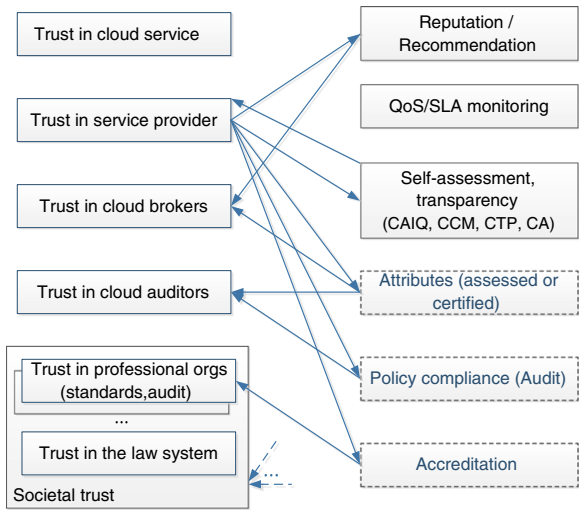

Figure 5 Evidence and chains for trust judgment on a cloud service provider. Similar to the structure of trust judgment on cloud broker showed in Figure 4.

a same mechanism, the contents to be examined for a specific type of cloud entity could be different from the ones for another types of entities. For example, when applied to a cloud service provider, "policy compliance audit", refers to evaluation of a cloud service provider's conformance to its cloud service policy; however, when applied to a cloud auditor, it refers to the evaluation of a cloud auditor conformance to a cloud audit policy.

Now we discuss each trust judgment task in turn.

Societal trust

Societal trust is foundational in all trust models that include individuals and organizations; cloud computing is no exception. Each individual in a society has to place trust in some basic parts of the society. Examples include: trust in the law system and government to maintain social order; trust in some professional services; trust in professional organizations with respect to creating and maintaining specific professional services standards. In the cloud context, examples of professional organizations might include AICPA, NIST (National Institute of Standards and Technology), IGTF (International Grid

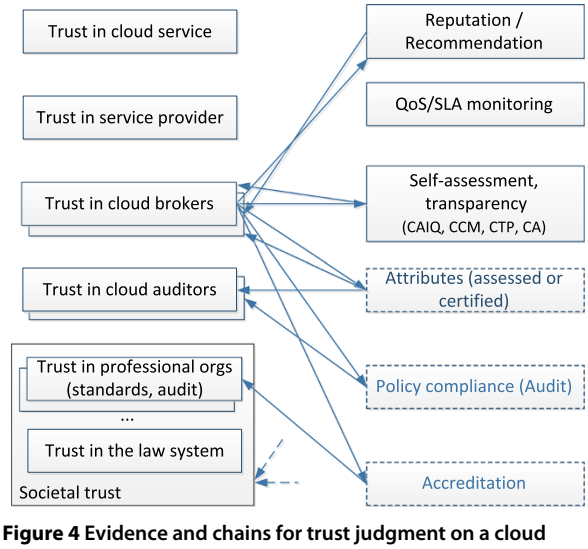

Figure 4 Evidence and chains for trust judgment on a cloud broker. Trust placed in a cloud broker is based on one or more of: (1) accreditation; (2) policy compliance; (3) certified attributes; (4) self-assessment and information revealing, which is based on the trust placed in this broker with respect to telling truth; (5) reputation calculated or recommendation made by another trusted broker.

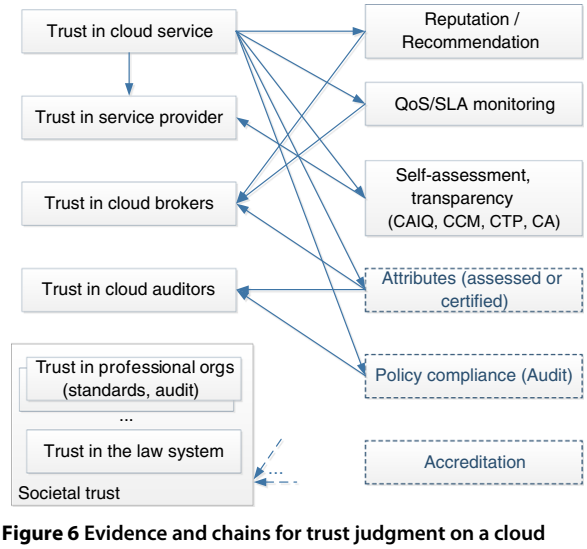

Figure 6 Evidence and chains for trust judgment on a cloud service. Trust placed in a cloud service is based on one or more of: (1) cloud service provider, whom is trusted; (2) policy compliance; (3) certified attributes; (4) QoS monitoring and SLA verification, which are conducted by a trusted party such as a trusted broker; (5) reputation calculated or recommendation made by a trusted broker.

Trust Federation), and CSA (Cloud Security Alliance). We specifically assume that societal trust leads cloud users to put their trust in the accreditation of cloud entities including auditors, brokers, and service providers, with respect to the qualification of a cloud entity on corresponding professional services.

While we recognize societal trust as a root of cloud trust, a deeper treatment of societal trust is beyond the scope of our overview of trust in clouds.

Trust judgment on a cloud auditor

A cloud auditor is a professional independent assessor of cloud entities. An auditor conforms to professional policies and/or standards in his operations. Cloud auditors should be also externally audited periodically by audit professional organizations, to ensure they comply with established policies and standards.

One cloud user might place a cloud auditor in his trusted societal root, i.e., simply assume the auditor is trustworthy; another user may choose instead to make a trust judgment on a cloud auditor as they do on other cloud entities. By the semantics of trust given in § 'Semantics of Trust', for "trust in a cloud auditor", the **expectancy** of a cloud user on a cloud auditor is the objective and professional assessment on a cloud entity with respect to its cloud services against a specific set of standards; the belief in that expectancy is based on some **evidence** with respect to the auditor's competency, goodwill, and integrity. For this judgment, there may be several sources of information as shown in Figure 3, and they are discussed as follows:

- **Accreditation:** A cloud user may check whether a specific cloud auditor is formally accredited by an professional audit organization and/or a cloud computing professional organization. Belief in accreditation is further dependent on whether the cloud user trusts the formal accreditor – an audit professional organization such as ASB of AICPA.
- **Policy compliance audit:** A cloud auditor should conform to professional policies and/or standards in its audit operations, such as SAS 70, SSAE 16, and ISAE 3402; the auditor should assess a cloud entity against widely accepted policies; the quality of the audit operations of an auditor is also assessed through audit, conducted by a different auditor appointed by an professional audit organization. A cloud user may use the audit results as evidence for trust judgment. The cloud user's belief in the audit result is further dependent on the user's trust in the auditor conducting the audit.
- **Certified attributes:** In addition to accreditation and policy compliance, a cloud user may want to check the auditor's other attributes, such as the history of the auditor, experiences of those previously audited by that auditor, the history of the audit applied to the auditor. Some attributes may be contained in audit documents; some others may be certified (or assessed, verified, and digitally signed) by a peer auditor. The cloud user's belief in the certified attributes is dependent on the user's trust in the issuer of the certified attributes.

Trust judgment on a cloud broker

As discussed in § 'Observation of cloud broker', a cloud broker provides various intermediate services. Any cloud entity offering intermediated services may be regarded as a broker. Examples may include: "market" for cloud services such as SpotCloud [38], and TaaS such as CTA [27]. Note that an online reputation and ranking system for cloud services can also be regarded as a cloud broking service.

For the concept of "trust in a cloud broker", the **expectancy** of a cloud user on a cloud broker includes trustworthy value-added services such as bridging and aggregating services, security and identity management services, objective and precise evaluation of cloud services and their providers. To make evidence-based trust judgments, as illustrated by Figure 4, the evidence may include:

- **Accreditation:** Similar to cloud auditors, a cloud broker should be qualified for providing cloud broking services, through formally accreditation by a cloud computing professional organization.
- **Policy compliance audit:** A cloud broker should conform to certain policies and/or standards widely adopted or accepted by the cloud in the broker's operations; the quality of its operations should be audited by a cloud auditor. A cloud user may use the audit result as evidence for trust judgment. The cloud user's belief in the audit result is further dependent on the user's trust in the auditor conducting the audit.
- **Attributes (assessed or certified):** The attributes of a cloud broker on competency, goodwill, and integrity are important evidence for cloud users' trust judgment. In addition to the attributes assessed with respect to policy compliance, other attributes regarding performance, security, and privacy as discussed in § 'Evidence-based trust' may be also audited by a cloud auditor, or assessed and digitally signed by other cloud brokers, or reviewed and digitally signed by some cloud users. The cloud user's belief in the certified/assessed attributes is dependent on the user's trust in the issuer of the certified/assessed attributes.
- **Self-assessment and information revealing:** Cloud brokers as a special type of intermediated cloud

service providers should also adopt the CSA cloud transparency mechanisms to exercise self-assessment such as CAIQ and CCM, and information revealing as does in CTP (discussed in § 'Cloud transparency mechanisms'). The cloud user's belief in the information revealed by the broker is dependent on the user's trust in that broker with respect to telling the truth, which may be verified in a formal audit.

- **Reputation/recommendation:** Reputation and recommendation can be very helpful to new cloud users and/or the users who are planning to recompose their cloud services. The cloud user's belief in the reputation scores and recommendation is dependent on the user's trust in the source of the information, typically, a cloud broker.

Trust judgment on a cloud service provider

The trust **expectancy** of a user with respect to a provider is that the provider offers trustworthy cloud services. The evidence for trust judgment on a cloud service provider may include the following sources, as shown in Figure 5:

- **Accreditation**
- **Policy compliance audit**
- **Attributes (assessed or certified)**
- **Self-assessment and information revealing**
- **Reputation/recommendation**

All of the above mechanisms are similar to the ones applied to cloud brokers, save that the trustee is a cloud service provider rather than a cloud broker.

Trust judgment on a cloud service

We view a cloud service as an autonomous agent; and that "a cloud user trusts a cloud service" means that the user has the **expectancy** that the cloud service is trustworthy, which means that the cloud service has a set of attributes including reliability, availability, confidentiality, integrity, safety, and privacy; the user believes the expectancy to be true based on some **evidence**, from diverse sources, shown in Figure 6:

- **Trust based on the service provider:** by *trust in performance*, a user trusts a cloud service with respect to performance, security, and privacy, based on the identity of the provider. If the user trusts that the provider gives trustworthy cloud services, then the cloud service is trusted.
- **Policy compliance audit:** A cloud user may examine specific policies and/or standards applied to the service, and investigate the results of formal audits of the provider.
- **Attributes (assessed or certified):** A cloud user may examine the attributes of a cloud service regarding performance, security, and privacy, which may be audited by a cloud auditor, or assessed and digitally signed by cloud brokers, or reviewed and digitally signed by some cloud users. The belief in those attributes is dependent on the trust in the corresponding attribute assessor.
- **Self-assessment and information revealing:** A cloud user may study information about the service which is revealed by the service provider through cloud transparency mechanisms. The user's belief in the information is dependent on the user's trust in the cloud service provider with respect to telling the truth.
- **QoS monitoring and SLA verification:** QoS monitoring and SLA verification (a shorter term "QoS/SLA monitoring" is used in Figure 6) is an important source to verify trust and to adjust trust. If the monitoring is conducted by a cloud broker, then the belief in the results of monitoring is dependent on the trust in that broker with respect to objective and professional monitoring.
- **Reputation/recommendation:** a cloud user may trust a cloud service, based on a trusted cloud broker's recommendation. Similar to PKI trust, recommendation may be handled in two ways: one regards the "recommendation" as the broker's trust in that recommended service, and then derives indirect trust on that service through using *trust in belief* relation with the broker; another is (as in PKI practice) that the broker only certifies that that cloud service has certain attributes or conforms to certain policies, and cloud users to make their own decision whether to trust that service.

Further discussion

As seen above, the trust placed on a cloud entity may be dependent on several sources of evidence; however, it is unnecessary to use all of them; a cloud user may use one or more sources of evidence for trust judgment, dependent on the user's trust policy. For example, to decide whether to trust a cloud service provider, a cloud user may simply just check whether the provider passed the formal audit of a widely accepted cloud service policy, conducted by a trusted auditor.

In the discussion above, the trust mechanisms of reputation/recommendation, QoS monitoring and SLA verification, self-assessment and information revealing are already in development; formal accreditation is in discussion, but it does not exist yet; trust mechanisms of attribute assessment/certification, which is used for evidence-based trust judgment, and policy compliance

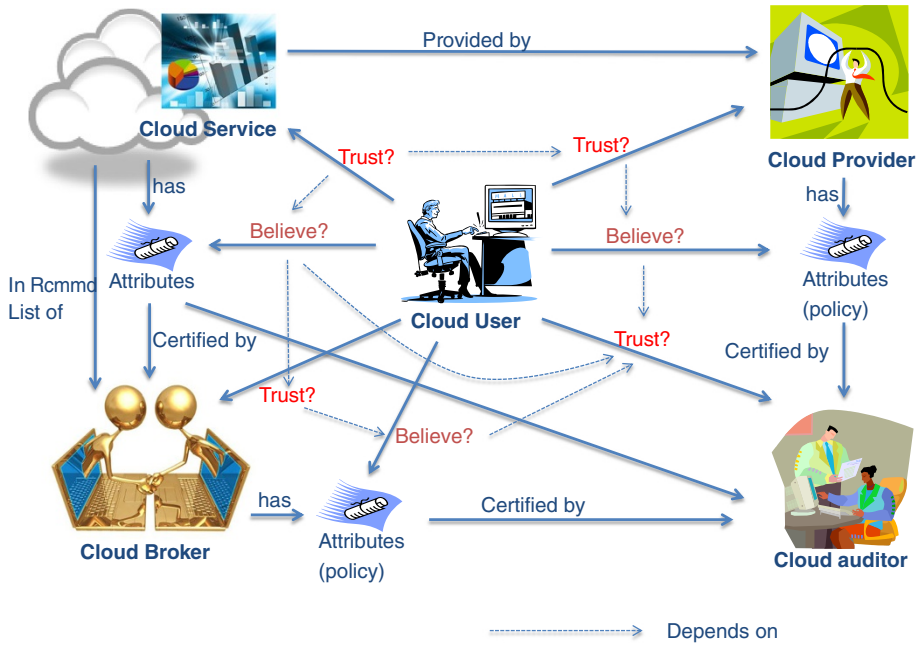

Figure 7 Chains of trust relations in clouds. This figure provides an integrated picture to illustrate the chains of trust relations from a cloud user to a cloud service and related cloud entities, where accreditation is omitted for simplicity.

audit, which is used for policy-based trust judgment, are what we suggest, and do not exist in the cloud yet; however policy-based trust has been successfully (more or less) used in PKI practice, and the practice is a proof of feasibility.

The mechanism of using attribute assessment/certification and evidence-based trust judgment could be complex, due to a possibly large set of attributes to consider and a possibly long chains of trust relations. Nevertheless, the policy-based trust judgment can be actually regarded as a simplified version of the attribute/evidence-based mechanism, in the sense that a widely accepted policy captures a set of key attributes.

In the above figures, the trust relations with various cloud entities, shown in the left part of the figures, are dependent on various sources of evidence, shown in the right part of figures; and the derivation of a source of evidence is dependent on some trust relations either. All those dependence relations form the chains of trust. Figure 7 illustrates some chains of trust focusing on policy-based and attribute/evidence-based mechanisms.

Summary and further research

Trust is a critical aspect of cloud computing. We examined and categorized existing research and practice of trust mechanisms for cloud computing in five categories– reputation based, SLA verification based, transparency mechanisms (self-assessment and information revealing), trust as a service, and formal accreditation, audit, and standards. Most current work on trust in the cloud focus narrowly on certain aspects of trust; our thesis is that this is insufficient. Trust is a complex social phenomenon, and a systemic view of trust mechanism analysis is necessary. In this paper we take a broad view of trust mechanism analysis in cloud computing and develop a somewhat informal and abstract framework as a route map for analyzing trust in the clouds. In particular, we suggest: (1) a policy-based approach of trust judgment, by which the trust placed on a cloud service or a cloud entity is derived from a "formal" audit proving that the cloud entity conforms to some trusted policies; (2) a "formal" attribute-based approach of trust judgment, by which particular attributes of a cloud service or attributes of a service provider are used as *evidence* for trust judgment, and the belief in those attributes is based on formal certification and chains of trust for validation. To support this mechanism, we propose a general structure of evidence-based trust judgment, which provides a basis to infer the trust in a cloud entity from the belief in the attributes that entity has, and in which, based on the semantics of trust, we define the attributes to be examined are in a space of two-dimensions – domain of expectancy and source of trust including competency, integrity, and goodwill.

Future research will focus on mathematically formal frameworks for reasoning about trust, including modeling, languages, and algorithms for computing trust.

Abbreviations

AA: Attribute Authority; AC: Attribute Certificate; AICPA: American Institute of Certified Public Accountants; ASB: Auditing Standards Board; CA: Certification Authority; CAIQ: Consensus Assessment Initiative Questionnaire; CCM: Cloud Control Matrix; CP: Certificate Policy; CSA: Cloud Security Alliance; CTA: Cloud Trust Authority; CTP: CloudTrust Protocol; GRC: Governance, Risk Management and Compliance; IETF: Internet Engineering Task Force; IGTF: International Grid Trust Federation; ISAE 3402: The International Standard on Assurance Engagements 3402; NIST: National Institute of Standards and Technology; PKI: Public Key Infrastructure; QoS: Quality of Service; SLA: Service Level Agreement; SSAE 16: Statement on Standards for Attestation Engagements No. 16; STAR: Security, Trust & Assurance Registry; TaaS: Trust as a Service.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

JH carried out the study of trust in clouds and drafted the manuscript; DMN helped develop the concepts, reviewed, and revised the manuscript. Both authors read and approved the final manuscript.

Authors' information

Jingwei Huang is a research scientist in Information Trust Institute, University of Illinois at Urbana-Champaign. He received his PhD from University of Toronto in 2008, and is a member of ACM and IEEE. His research mainly focuses on (1) formal theories of trust, including the formal semantics of trust, measurement of trust, calculus of trust, trust evolution, and trust mechanisms; (2) applications of formal trust models in distributed computing and open networks, such as trust in cloud computing; (3) information assurance, including security policies for cross-domain information sharing, and formal models combining role-based access control, mandatory access control, and attribute-based access control.

David M. Nicol is the Franklin W. Woeltge Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign, and Director of the Information Trust Institute. Previously he held faculty positions at the College of William and Mary and at Dartmouth College. His research interests include high-performance computing, simulation modeling and analysis, and security. He was elected Fellow of the IEEE and Fellow of the ACM for his contributions in those areas. He is co-author of the widely used textbook Discrete-Event Systems Simulation and was the inaugural awardee of the ACM Special Interest Group on Simulation's Distinguished Contributions Award, for his contributions in research, teaching, and service in the field of simulation.

Acknowledgements

This material is based upon research sponsored by the U.S. Air Force Research Laboratory (AFRL) and the U.S. Air Force Office of Scientific Research (AFSOR), under agreement number FA8750-11-2-0084. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. We would like to thank Professor Roy Campbell, Professor Ravishankar K. Iyer, Scott Pickard, and many others in ACC-UCoE (Assured Cloud Computing University Center of Excellence, a joint effort of AFSOR, AFRL, and UIUC) for their valuable discussion.

Received: 23 October 2012 Accepted: 9 April 2013
Published: 24 April 2013

References

1. Michael B (2009) In clouds shall we trust? IEEE Security and Privacy 7(5): 3–3. http://dx.doi.org/10.1109/MSP.2009.124
2. Everett C (2009) Cloud computing: A question of trust. Computer Fraud Security 2009(6): 5–7. http://dx.doi.org/10.1016/S1361-3723(09)70071-5
3. Garrison G, Kim S, Wakefield RL (2012) Success factors for deploying cloud computing. Commun ACM 55(9): 62–68. http://doi.acm.org/10.1145/2330667.2330685
4. Ghosh A, Arce I (2010) Guest editors' introduction: In cloud computing we trust - but should we? Secur Privacy, IEEE 8(6): 14–16. doi:10.1109/MSP.2010.177
5. Habib S, Hauke S, Ries S, Muhlhauser M (2012) Trust as a facilitator in cloud computing: a survey. J Cloud Comput Adv Syst Appl 1(1): 19. doi:10.1186/2192-113X-1-19, http://www.journalofcloudcomputing.com/content/1/1/19
6. Khan K, Malluhi Q (2010) Establishing trust in cloud computing. IT Prof 12(5): 20–27. doi:10.1109/MITP.2010.128
7. Michael B, Dinolt G (2010) Establishing trust in cloud computing. IANewsletter 13(2): 4–8. http://iac.dtic.mil/iatac/download/Vol13_No2.pdf
8. Park J, Spetka E, Rasheed H, Ratazzi P, Han K (2012) Near-real-time cloud auditing for rapid response. In: In: 26th International conference on advanced information networking and applications workshops (WAINA), pp 1252–1257. IEEE Computer Society, Washington, DC, USA. doi:10.1109/WAINA.2012.78
9. Pearson S (2011) Toward accountability in the cloud. Internet Comput IEEE 15(4): 64–69. doi:10.1109/MIC.2011.98
10. Takabi H, Joshi J, Ahn G (2010) Security and privacy challenges in cloud computing environments. Secur Privacy IEEE 8(6): 24–31. doi:10.1109/MSP.2010.186
11. Abawajy J (2011) Establishing trust in hybrid cloud computing environments. In: Proceedings of the 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications,. IEEE Computer Society, Washington, DC, USA. TRUSTCOM '11, pp 118–125. doi:10.1109/TrustCom.2011.18. http://dx.doi.org/10.1109/TrustCom.2011.18
12. Haq IU, Alnemr R, Paschke A, Schikuta E, Boley H, Meinel C (2010) Distributed trust management for validating sla choreographies. In: Wieder P, Yahyapour R, Ziegler W (eds). Grids and service-oriented architectures for service level agreements. Springer, US. pp 45–55. http://dx.doi.org/10.1007/978-1-4419-7320-7_5
13. Pawar P, Rajarajan M, Nair S, Zisman A (2012) Trust model for optimized cloud services(Dimitrakos T, Moona R, Patel D, McKnight D, eds.). Springer, Berlin Heidelberg. pp 97–112. http://dx.doi.org/10.1007/978-3-642-29852-3_7
14. NIST (2011) NIST cloud computing standards roadmap, NIST CCSRWG-092. first edition. NIST, Gaithersburg, MD,USA. http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Jul5A.pdf
15. Blomqvist K (1997) The many faces of trust. Scand J Manage 13(3): 271–286
16. Mayer R, Davis J, Schoorman F (1995) An integrative model of organizational trust: Past, present, and future. Acad Manage Rev 20(3): 709–734
17. Huang J, Nicol D (2010) A formal-semantics-based calculus of trust. Internet Comput IEEE 14(5): 38–46. doi:10.1109/MIC.2010.83
18. Shaoham Y (1987) Temporal logics in ai: Semantical and ontological considerations. Artif Intell 33: 89–104
19. Huang J, Fox MS (2006) An ontology of trust: formal semantics and transitivity. In: Proceedings of the ICEC'06, 259–270. ACM, New York, NY, USA. doi:10.1145/1151454.1151499
20. Hwang K, Kulkareni S, Hu Y (2009) Cloud security with virtualized defense and reputation-based trust mangement. In: Dependable, Autonomic and Secure Computing, 2009. DASC '09. IEEE Computer Society, Washington, DC, USA. Eighth IEEE International Conference on, pp 717–722. doi:10.1109/DASC.2009.149
21. CSA (2011) STAR (security , trust and assurance registry) program. Cloud Security Alliance. https://cloudsecurityalliance.org/star/. Accessed on 16 Oct. 2012
22. CSA (2011) Security guidance for critical areas of focus in cloud computing v3.0. Cloud Security Alliance. www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
23. CSA (2011) CSA: Security, trust and assurance registry. Cloud Security Alliance. https://cloudsecurityalliance.org/research/initiatives/star-registry/, Accessed on 16 Oct. 2012
24. Knode R (2009) Digital trust in the cloud. CSC.COM. http://assets1.csc.com/au/downloads/0610_20_Digital_trust_in_the_cloud.pdf
25. CSC (2011) Cloudtrust protocol (CTP). Cloud Security Alliance. https://cloudsecurityalliance.org/research/ctp/. Accessed on 16 Oct. 2012
26. Knode R, Egan D (2010) Digital trust in the cloud – A precis for the CloudTrust protocol (V2.0). CSC. https://cloudsecurityalliance.org/wp-content/uploads/2011/05/cloudtrustprotocolprecis_073010.pdf
27. RSA (2011) RSA establishes cloud trust authority to accelerate cloud adoption. RSA. http://www.rsa.com/press_release.aspx?id=11320

28. EMC (2011) Proof, not promises: Creating the trusted cloud. EMC. http://www.emc.com/collateral/emc-perspective/11319-tvision-wp-0211-ep.pdf
29. ISO (2005) ISO/IEC 27001:2005 information technology – security techniques – information security management systems – requirements. ISO. http://www.iso.org/iso/catalogue_detail?csnumber=42103. Accessed on 16 Oct. 2012
30. AICPA (2010) SSAE 16. AICPA. http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx. Accessed on 16 Oct. 2012
31. IAASB (2009) ISAE 3402. International Auditing and Assurance Standards Board. http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf. Accessed on 16 Oct. 2012
32. IGTF (2010) Guidelines for auditing grid cas version 1.0. IGTF. http://www.ogf.org/documents/GFD.169.pdf
33. Maurer UM (1996) Modelling a public-key infrastructure. In: In: ESORICS '96: Proceedings of the 4th European symposium on research in computer security. Springer-Verlag, London, pp 325–350
34. Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W (2008) Internet x.509 public key infrastructure certificate and certificate revocation list (CRL) profile. IETF. http://www.ietf.org/rfc/rfc5280.txt
35. Huang J, Nicol D (2009) Implicit trust, certificate policies and formal semantics of PKI. Information Trust Institute, University of Illinois at Urbana-Champaign
36. Ziegler CN, Lausen G (2005) Propagation models for trust and distrust in social networks. Inf Syst Front 7(4–5): 337–358. http://dx.doi.org/10.1007/s10796-005-4807-3
37. Farrell S, Housley R, Turner S (2010) An internet attribute certificate profile for authorization. IETF. http://www.ietf.org/rfc/rfc5755.txt
38. Enomaly Inc. (2010) SportCloud: Global market for cloud capacity. Enomaly Inc. http://spotcloud.com. Accessed on 18 Jan. 2013

doi:10.1186/2192-113X-2-9
Cite this article as: Huang and Nicol: **Trust mechanisms for cloud computing.** *Journal of Cloud Computing: Advances, Systems and Applications* 2013 **2**:9.