Building Trust in the Cloud: Mechanisms and Strategies for Secure Cloud Computing

Kaustav Roy , Shivnath Ghosh

Department of CSE, Brainware University, Kolkata

kr.cs@brainwareuniversity.ac.in ,dsg.cs@brainwareuniversity.ac.in

Abstract

Trust plays a pivotal role in cloud computing, where it heavily relies on the perception of reputation and self-evaluation conducted by cloud service providers. This article initiates by conducting a comprehensive examination of current trust-establishing mechanisms while shedding light on their inherent constraints. Subsequently, we tackle these limitations by introducing more robust mechanisms that rely on substantiating evidence, attribute certification, and validation. We propose a framework that integrates diverse trust mechanisms to uncover interconnected trust chains within the cloud environment. To facilitate these trust mechanisms, we introduce a general structure for evidence-based trust judgment. This structure enables the inference of trust in cloud entities based on belief in their associated attributes. We define attributes within a two-dimensional space, considering the domain of expectancy and the source of trust, which includes competency, integrity, and goodwill. Furthermore, we outline the need for future research on mathematically formal frameworks for reasoning about trust. This entails developing models, languages, and algorithms to support the computation and analysis of trust in cloud computing. By adopting a comprehensive perspective and providing an abstract framework, this work aims to contribute to the deeper understanding and advancement of trust mechanisms in the cloud.

Keywords: Attribute certification; Cloud computing; Reputation perception; Trust chains; Trust mechanisms

Introduction

Cloud computing has emerged as a dominant paradigm in computing and the delivery of IT services. However, prospective users of cloud services often question the trustworthiness of such services. Defining the concept of "trust" within the

context of cloud computing and establishing its basis become critical considerations. When users rely on the attributes of a cloud service or provider as evidence for trust assessment, they need assurance regarding the validity of these claimed attributes. It becomes essential to determine the authorities responsible for monitoring, measuring, assessing, and validating cloud attributes. These answers are pivotal for the widespread adoption of cloud computing and for its evolution into a reliable computing paradigm. As highlighted in [1], "the increasing significance of cloud computing necessitates a comprehensive understanding of trust in the cloud and how trust is established by customers, providers, and society at large."

The issues and challenges associated with trust in cloud computing have been extensively examined from various perspectives [2–8], leading to the proposal of several models and tools [8–10]. Each contributes to a partial understanding of trust in the cloud. However, a comprehensive depiction of how different cloud entities collaborate to form a "societal" system grounded in trust, thereby facilitating trusted pathways to reliable cloud services, is still lacking. The NIST Cloud Computing Reference Architecture identifies cloud brokers and cloud auditors as entities responsible for assessing cloud services. However, there is limited research on analyzing trust relationships and trust chains from cloud users to cloud services (or providers) through these intermediary cloud entities. In this paper, we delve into the investigation of trust mechanisms for the cloud. We present our perspective on the "societal systems mechanisms" of trust and propose a framework for analyzing trust relationships within the cloud. Additionally, we suggest trust mechanisms that combine attribute certification, evidence-based trust, and policy-based trust.

Due to the critical nature of numerous computing services and tasks, certain cloud clients cannot rely solely on informal trust mechanisms, such as web-based reputation scores, when making decisions about adopting a cloud service. Instead, they require formal trust mechanisms that offer greater certainty, accountability, and reliability. Here, the term "formal" implies an "official" assessment within a society. In our proposed cloud trust mechanisms, the attributes of a cloud service or its provider serve as evidence for the user's trust evaluation, and trust in these attributes is established through formal certification and validation using trust chains. This paper primarily focuses on the conceptual foundation for analyzing trust in the cloud, adopting a relatively informal approach. It does not presently address mathematical modeling, which would involve more precise details, formal languages, and specific

use cases. Within the context of this paper, an "entity" denotes an autonomous agent, while a "cloud entity" refers to an entity operating within the cloud, such as a cloud provider, cloud user, cloud broker, or cloud auditor. The term "semantics of trust" encompasses precisely defined meanings of trust, including the relationships among trust components.

Trust Semantics Analogy

The term "trust" is often used loosely in cloud trust literature, sometimes encompassing concepts of "security" and "privacy" [11]. However, it is important to clarify the precise meaning of "trust."

Trust is a multifaceted social phenomenon. Drawing on trust concepts from the social sciences, we adopt the following definition [12]:

Trust is a mental state characterized by: (1) Expectancy - the trustor anticipates specific behavior from the trustee, such as the provision of accurate information or effective cooperation. (2) Belief - the trustor believes that the expected behavior will occur based on evidence of the trustee's competence, integrity, and goodwill. (3) Willingness to take risk - the trustor is willing to take risks based on this belief.

It is crucial to recognize that the expected behavior of the trustee is beyond the trustor's control. The trustor's belief in the trustee's expected behavior is established upon the trustee's competence, goodwill (including intentions and motivations), and integrity. The trustee's integrity instills confidence in the trustor regarding the predictability of the trustee's conduct.

We identify two types of trust based on the trustor's expectancy: trust in performance pertains to the trustee's actions, while trust in belief pertains to the trustee's convictions. The trustee's performance can involve the truthfulness of their statements or the successful execution of their tasks. For simplicity, we represent both scenarios as reified propositions denoted by a Boolean term, x [13]. In the first case, x represents what the trustee says, while in the second case, x denotes a successful performance described by the trustee. A trust in performance relationship, trust_p(d, e, x, k), signifies that trustor d trusts trustee e with regards to their performance x in context k. This relationship indicates that if x is attributed to e in context k, then d believes x in that context. In first-order logic (FOL):

$$trust\_p(d, e, x, k) \equiv madeBy(x, e, k) \supset believe(d, k \supset\!\!\cdot\ x) \quad (1)$$

Here, $\supset\!\!\cdot$ is an operator used for reified propositions, simulating the logical implication operator, $\supset$. A trust in belief relationship, trust_b(d, e, x, k), signifies that trustor d trusts trustee e with regards to their belief (x) in context k. This trust relationship implies that if e believes x in context k, then d also believes x in that context:

$$trust\_b(d, e, x, k) \equiv believe(e, k \supset\!\!\cdot\ x) \supset believe(d, k \supset\!\!\cdot\ x) \quad (2)$$

Trust in belief is transitive, while trust in performance is not. However, trust in performance can propagate through trust in belief. A more comprehensive explanation can be found in [14, 15].

Based on the above definition, the trustor's mental state, characterized by belief in their expectations of the trustee, depends on evidence related to the trustee's competence, integrity, and goodwill. This gives rise to logical reasoning structures that connect belief in evidence to belief in expectations. We will explore this further in the section on "Evidence-based trust."

The semantics of trust within the realm of cloud computing follow the same structural framework outlined above. However, what remains to be established are the specific expectations and characteristics of cloud entities' competency, integrity, and goodwill in the context of cloud computing. We will delve into this discussion in the section on "Evidence-based trust."

Methodology

Here we described and discussed trust mechanisms for cloud computing:

Reputation-Based Trust

Trust and reputation are interconnected but distinct concepts. Trust primarily exists between two entities, whereas the reputation of an entity represents the collective opinion of a community towards that entity. Typically, an entity with a high reputation is trusted by many members within the community. When a trust judgment needs to be made regarding a trustee, an entity may utilize reputation to calculate or estimate the level of trust in that trustee.

Reputation systems have widespread use in e-commerce and P2P networks. The reputation of cloud services or cloud service providers significantly influences the decision-making process of cloud users when selecting cloud services. Consequently, cloud providers strive to establish and maintain a favorable reputation. Naturally, reputation-based trust plays a role in the assessment of trust within cloud computing [16, 17].

In general, reputation is represented by a comprehensive score that reflects the overall perception or a limited number of scores related to key performance aspects. It is impractical to expect a large number of cloud users to individually rate a cloud service or provider against an extensive and intricate set of criteria. The reputation of a cloud service provider serves as a collective viewpoint of the community towards that provider, making it more valuable for cloud users, particularly individual users, when selecting a cloud service without specific requirements. Reputation may be useful during the initial selection of a service, but it becomes inadequate as users gain experience. Specifically, as users interact with a service over time, the level of trust placed in that service to meet performance and reliability expectations evolves based on their firsthand experiences.

SLA Verification-Based Trust

The principle of "trust, but verify" offers valuable guidance when it comes to the relationship between cloud users and cloud service providers. Once an initial level of trust has been established and a cloud service is employed, it becomes essential for the cloud user to verify and reassess that trust. A service level agreement (SLA) serves as a legally binding contract between a cloud user and a cloud service provider. Consequently, the monitoring of quality of service (QoS) and the verification of SLAs form a crucial foundation for trust management in cloud computing. Various models have been proposed that derive trust from SLA verification [18, 19].

One major challenge is that SLAs primarily focus on the "visible" aspects of cloud service performance, often overlooking "invisible" elements such as security and privacy. Additionally, many cloud users lack the necessary capabilities to perform granular QoS monitoring and SLA verification independently, necessitating the involvement of professional third-party entities to provide these services. In the

context of a private cloud, a cloud broker or a trusted authority within the trust domain of the private cloud (such as RSA's CTA, to be discussed later in the section on "Cloud transparency mechanisms") can fulfill the role of conducting QoS monitoring and SLA verification for the users within the private cloud. In hybrid clouds or intercloud environments, a user within a private cloud may still rely on the private cloud's trusted authority to perform QoS monitoring and SLA verification. However, in a public cloud setting, individual users and small organizations without the technical capabilities may opt to utilize a commercial professional cloud entity as a trusted broker. We delve into this topic further in the section on "Trust as a service."

Cloud Transparency Mechanisms

Transparency and accountability serve as recognized foundations for establishing trust in cloud providers. In order to enhance transparency within the cloud, the Cloud Security Alliance (CSA) introduced the "Security, Trust & Assurance Registry (STAR)" program [20]. This program offers a publicly accessible registry where cloud service providers can publish self-assessments of their security controls using either the "Consensus Assessments Initiative Questionnaire (CAIQ)" or the "Cloud Controls Matrix (CCM)," which embody CSA's best practices. The CAIQ consists of over 140 questions that cloud users or auditors may pose, while the CCM is a framework outlining how a cloud provider aligns with CSA's security guidelines [21]. Examples of cloud providers' self-assessments can be found on the CSA STAR website. STAR serves as a valuable resource for users seeking cloud services. However, it's important to note that the information provided is based on self-assessment by the cloud provider, and users may desire assessments conducted by independent third-party professional organizations.

In contrast to STAR, CSC.com proposed and CSA adopted the CloudTrust Protocol (CTP). CTP is a request-response mechanism that allows cloud users to obtain specific information about the "elements of transparency" implemented by a particular cloud service provider. These elements of transparency encompass various aspects such as configuration, vulnerability, audit logs, service management, and service statistics, among others. The primary objective of CTP and the elements of transparency is to generate evidence-based confidence that everything occurring within the cloud aligns with the provider's description and nothing else. CTP

establishes an intriguing channel of communication between cloud users and service providers, enabling users to gain insight into the internal operations of cloud services. However, similar to STAR, a key drawback of CTP is that the information is provided by the cloud service provider itself, which introduces the possibility of dishonest providers filtering or altering the data. From a trust judgment standpoint, this raises concerns regarding the reliability of the data.

Results & Discussion

Earlier, we highlighted the necessity for "formal" trust mechanisms in cloud computing. In a similar context, Public Key Infrastructure (PKI) is a well-established technology that employs "formal" trust mechanisms to support digital signatures, key certification and validation, and attribute certification and validation. Can we apply the trust concepts utilized in PKI to establish "formal" trust mechanisms in the cloud?

To simplify the discussion, let's consider the scenario depicted in Figure 1. Alice possesses a digital document that is supposedly signed by Bob using his private key, K′b. To verify the document's signature, Alice requires Bob's public key, Kb. However, Alice only trusts her designated certification authority, CA1, and is aware of only K1, which is her trust anchor's public key. In order to validate the signature and confirm that it belongs to Bob, Alice needs to establish a certification path (a sequence of certificates) from CA1 to CA3, who issued Bob's public key certificate. As illustrated in the figure, Alice utilizes K1, the public key of CA1, to validate K2, the public key of CA2. Since Alice places trust in CA1 for public key certification, and CA2's public key is certified by CA1, Alice can reasonably believe that CA2's public key is indeed K2. Subsequently, Alice employs K2 to validate K3, the public key of CA3, and ultimately utilizes K3 to validate Bob's public key, Kb. The main question here is why Alice should have confidence in K3 being CA3's public key and Kb being Bob's public key.

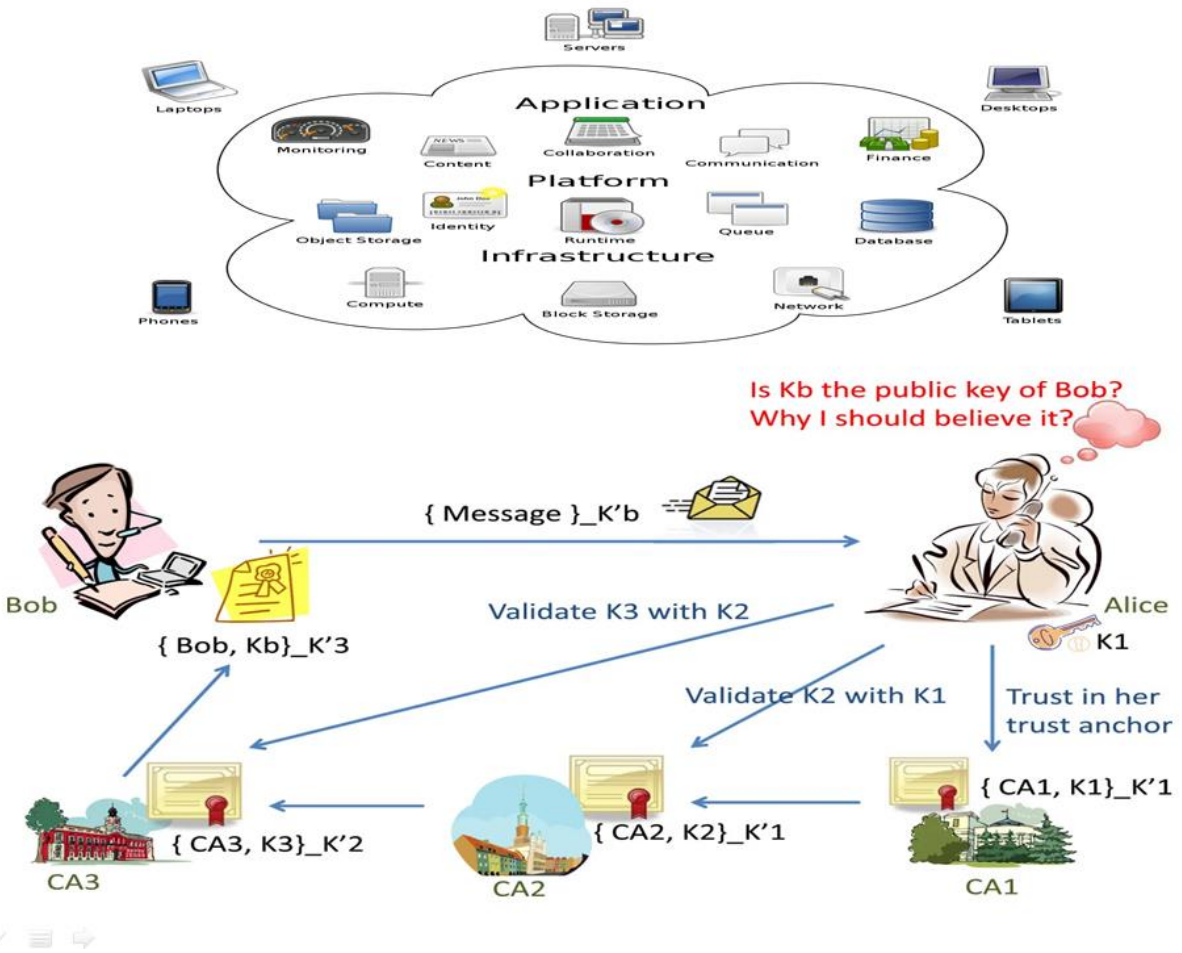


Figure 1. Example of trust in PKI. This illustrative scenario demonstrates the trust relationships involved in public key certification and validation.

In essence, for Alice to believe in the statement "Bob's key is Kb," she must trust CA3, the entity responsible for making that assertion. However, this raises questions about the foundation of that trust and how it is determined or calculated. Some research suggests that trust stems from recommendations received along the chain of certificates by the certificate issuers [22]. On the other hand, real-world practices of digital certification and validation in PKI systems indicate that trust is established through compliance with specific certificate policies.

According to IETF RFC 5280 [23], a public key certificate contains not only the fundamental statement that binds a public key with a subject but also a certificate

policy (CP) extension. When a public key certificate is issued to a certification authority (CA), it signifies that the issuing CA adheres to the specified CP and asserts that the subject CA possesses the certified public key while also conforming to the specified CP. Consequently, for Alice to infer her belief in CA3's key and Bob's key, she must trust the CP in a way that any CA conforming to that CP will generate valid public key certificates. PKI trust involves more complex and intriguing aspects [24], but for the purposes of this discussion, we will not delve further into them.

In summary, in the current practice of PKI, trust in a certification authority (CA) regarding the issuance and maintenance of valid public key certificates relies on the CA's adherence to specific certificate policies. Certificate policies play a central role in establishing trust within PKI. We refer to this trust mechanism as policy-based trust.

Now we will discuss the utilization of attributes as evidence in making trust decisions.

Based on the definition of trust provided in the section 'Semantics of trust,' a trustor's belief in the expected behavior of a trustee is established upon the evidence regarding the trustee's attributes of competency, goodwill, and integrity in relation to that expectation. Formally, we can express a general form of evidence-based trust as follows:

If an individual, u, believes that a subject, s, possesses attribute attr1 with value v1, and believes that s has attribute attrn with value vn, then u trusts (either through trust in belief or trust in performance) s in regards to x, which represents s's performance, information generated by s, or believed by s, in a specific context, c.

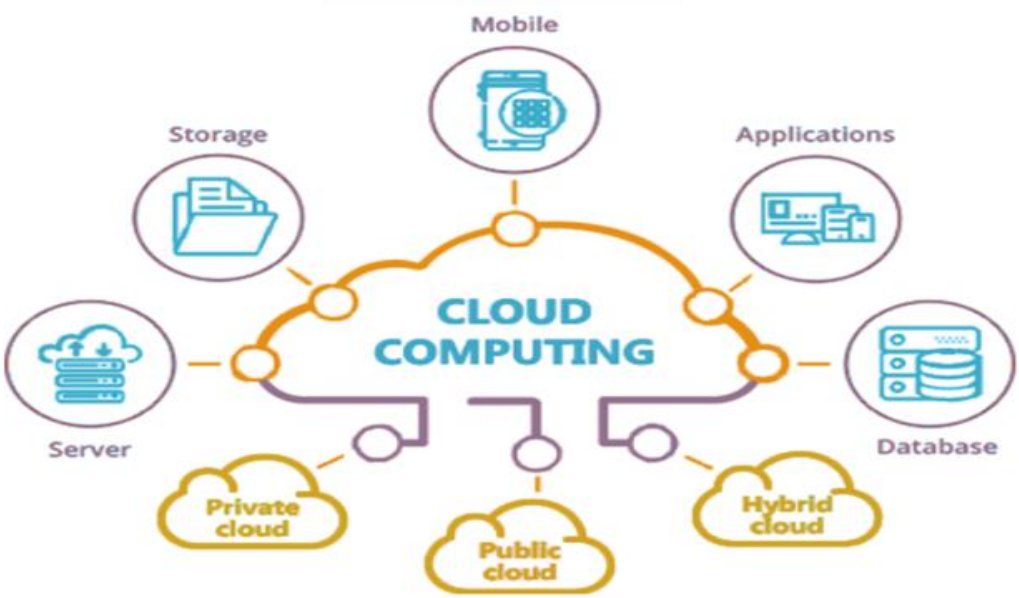
An entity's belief in an attribute assessment is contingent upon whether the entity trusts the source that provides that attribute assessment. Formally, referring to the definition of trust-in-performance discussed in formula (1) in the section 'Semantics of trust,' we can state the following:

If an individual, u, trusts an attribute authority, a, to make assertions about a subject, s, having attribute attr with value v, in a specific context, c, and a specific assertion attr(s,v) is made by a in context c, then u believes that assertion.

To represent the assertion attr(s,v), we use a reified proposition represented as a term. In the formula, we may employ attr(e,v) to indicate that a cloud entity, e, possesses attribute attr with value e. By doing so, a logic formula similar to the one described above can depict the relationship between trust in a cloud auditor and the belief in the certified attribute of a cloud entity, such as a service provider.

To incorporate attributes as evidence in trust evaluation, we organize the relevant attributes in a two-dimensional space. The first dimension aligns with the trustor's expectations of the trustee within the context of cloud computing, encompassing aspects of performance, security, and privacy. The second dimension aligns with the source of trust, exploring the factors that lead the trustor to place trust in the trustee, such as the trustee's competency, integrity, and goodwill.

Figure 2 illustrates a spectrum of attributes in cloud computing. While attributes related to competency are commonly considered, attributes reflecting integrity and goodwill are often neglected but should be included in trust evaluation. Overlooking these attributes implies either assuming that trust is independent of them or assuming that any dependence is adequately fulfilled. Characterizing and quantifying integrity and goodwill pose interesting research challenges. Historical behavior of a trustee can provide insights into their integrity, while goodwill can be measured through performance improvements and feedback from cloud users.



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. Organizing attributes for evidence-based trust assessment can be achieved by categorizing them along two dimensions: (1) sources of trust, which encompass competency, goodwill, and integrity; and (2) domain-specific expectations.

Various cloud users may possess distinct trust policies that encompass different trust attributes. A unified trust framework facilitates evidence-based trust evaluation across diverse users and policies. The relationship between evidence-based trust and policy-based trust lies in the understanding that the conviction in an entity adhering to a trusted policy implies the perception that the entity possesses a collection of attributes aligned with that policy.

Attribute certification refers to the process of certifying specific attributes in addition to X.509 identity certification commonly used for public key authentication. While X.509 identity certification serves the purpose of authentication, attribute certification serves both authentication and authorization. An attribute certificate (AC) is a digitally signed statement issued by an AC issuer, certifying that the AC holder possesses a defined set of attributes. These certified attributes can include access identity, authentication information (such as username/password pairs), group membership, role, and security clearance. The structure of an AC typically includes fields such as the AC identifier, AC holder, AC issuer, attribute-value pairs, validity period, signature verification algorithm identifier, and extensions encompassing AC targeting and Certificate Revocation List (CRL) distribution points.

The existing IETF X.509 AC standard [25] could potentially be employed for cloud attribute certification, but it has certain limitations. Firstly, the standard does not encompass important attributes specifically required in the cloud context. Although extensions can be utilized to address this issue, there are no standardized provisions for attributes related to service performance, security, and privacy. Secondly, in terms of attribute certification, the true authority behind attribute assertions is the entity that possesses accurate knowledge about the certified entity. For instance, when it comes to the role or membership of an entity within a particular organization, that organization naturally holds the authority to declare such attributes. Hence, it is crucial to differentiate between the "attribute assertion authority" (AAA) and the attribute certification authority (ACA), also known as the AC issuer. The term "Attribute Authority" (AA) is used to refer to an entity that serves as both AAA and ACA. In the context of cloud computing, the most reliable sources for attribute assertion and assessment are independent third-party professional organizations like cloud auditors, accreditors, and even cloud brokers.

Lastly, the current IETF X.509 AC standard [25, 26] adopts a simple trust structure where "one authority issues all of the ACs for a particular set of attributes." However, in cloud applications, especially in hybrid cloud and public cloud scenarios, the AC issuer may often lie outside the trust boundary of an AC user. As a result, mechanisms for cross-domain attribute certification and validation become necessary to address the requirements of these environments.

Figure 3 depict the interdependence between trust placed in various cloud entities and the sources of evidence utilized for making trust judgments. These figures are divided into two sections: the left part represents the trust vested in different types of cloud entities, while the right part illustrates the corresponding trust mechanisms employed as sources of evidence to support trust judgments. The arrows symbolize the dependency relationships between these entities and mechanisms, forming the chains of trust within the cloud. It is important to note that the six mechanisms depicted in these illustrations serve as abstractions of typical mechanisms, and an actual trust judgment system may incorporate multiple mechanisms in practice. For instance, a cloud reputation system might calculate reputation scores and provide evaluated attributes based on feedback from brokers and user reviews. It is worth mentioning that the three mechanisms outlined in the lower-right section, indicated by dotted border-lines, are proposed suggestions and do not currently exist. While most mechanisms can support trust judgments for different types of cloud entities, it is crucial to recognize that the specific contents examined by a particular mechanism may vary depending on the type of entity involved. For example, when applied to a cloud service provider, the "policy compliance audit" mechanism refers to evaluating the provider's adherence to its cloud service policy. However, when applied to a cloud auditor, it pertains to evaluating the auditor's compliance with a cloud audit policy.

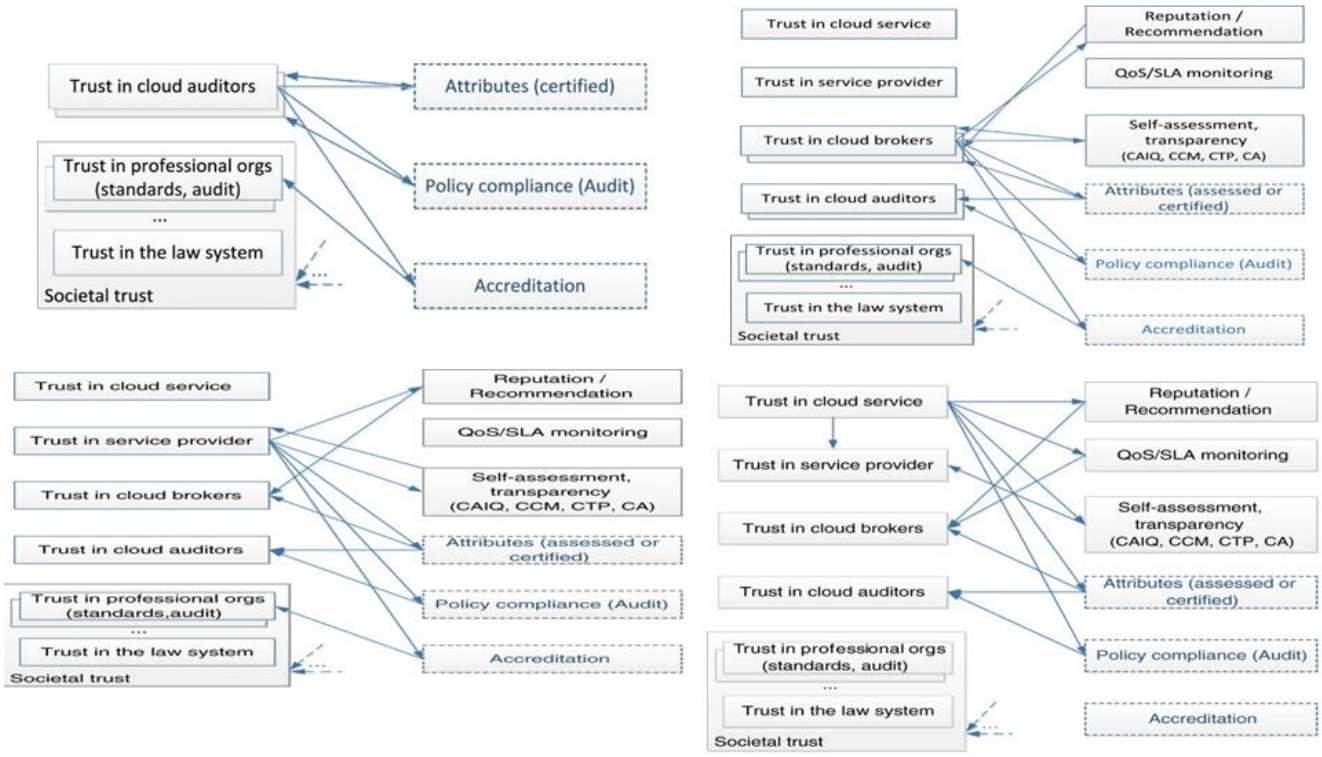


Figure 3. Assessing trust in a cloud service relies on evidence and interconnected chains of trust

Conclusion

Trust is a fundamental element in the context of cloud computing, and extensive research and practices have been conducted to explore different trust mechanisms. These mechanisms can be broadly categorized into five groups: reputation-based, SLA verification-based, transparency mechanisms (such as self-assessment and information disclosure), trust as a service, and formal accreditation, audit, and standards. However, the current focus on specific aspects of trust is limited, and a more comprehensive understanding of trust mechanisms is required. Trust is a multifaceted social phenomenon, necessitating a systemic approach to analyzing trust mechanisms in cloud computing.

In this paper, we adopt a broad perspective on analyzing trust mechanisms in the cloud and present an abstract framework as a guide for such analysis. Specifically, we propose two approaches to trust judgment:

A policy-based approach, where trust in a cloud service or entity is derived from a formal audit that verifies its adherence to trusted policies.

A formal attribute-based approach, where specific attributes of a cloud service or service provider serve as evidence for trust judgment. The belief in these attributes is based on formal certification and chains of trust for validation.

To support these mechanisms, we introduce a general structure for evidence-based trust judgment. This structure allows for the inference of trust in a cloud entity based on the belief in its associated attributes. In this structure, the attributes to be examined are defined within a two-dimensional space, encompassing the domain of expectancy and the source of trust, including competency, integrity, and goodwill.

Future research will focus on developing mathematically formal frameworks for reasoning about trust. This includes the creation of models, languages, and algorithms that facilitate the computation of trust.

References

[1]. Mehraj, S., & Banday, M. T. (2020, January). Establishing a zero trust strategy in cloud computing environment. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

[2]. Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2, 1-14.

[3]. Sarwar, A., & Khan, M. N. (2013). A review of trust aspects in cloud computing security. International Journal of Cloud Computing and Services Science, 2(2), 116.

[4]. Chiregi, M., & Navimipour, N. J. (2017). A comprehensive study of the trust evaluation mechanisms in the cloud computing. Journal of Service Science Research, 9, 1-30.

[5]. Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.

[6]. Li, W., Ping, L., & Pan, X. (2010, August). Use trust management module to achieve effective security mechanisms in cloud environment. In 2010 International Conference on Electronics and Information Engineering (Vol. 1, pp. V1-14). IEEE.

[7]. Ali, M., Wood-Harper, T., & Ramlogan, R. (2020). A framework strategy to overcome trust issues on cloud computing adoption in higher education. In Modern Principles, Practices, and Algorithms for Cloud Security (pp. 162-183). IGI Global.

[8]. Krautheim, F. J. (2010). Building trust into utility cloud computing. University of Maryland, Baltimore County.

[9]. Pearson, S. (2013). Privacy, security and trust in cloud computing (pp. 3-42). Springer London.

[10]. Saleem, M., Warsi, M. R., & Islam, S. (2023). Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. Journal of Information Security and Applications, 72, 103389.

[11]. Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami, N. (2023). Cloud security threats and solutions: A survey. Wireless Personal Communications, 128(1), 387-413.

[12]. Krumm, N. (2023). Organizational and Technical Security Considerations for Laboratory Cloud Computing. The Journal of Applied Laboratory Medicine, 8(1), 180-193.

[13]. Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C. W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1), 38.

[14]. George, A. S., & Sagayarajan, S. (2023). Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments. Partners Universal International Research Journal, 2(1), 24-34.

[15]. Sheik, S. A., & Muniyandi, A. P. (2023). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. Cyber Security and Applications, 1, 100002.

[16]. Khan, A. R., & Alnwihel, L. K. (2023). A Brief Review on Cloud Computing Authentication Frameworks. Engineering, Technology & Applied Science Research, 13(1), 9997-10004.

[17]. El-Kassabi, H. T., Serhani, M. A., Masud, M. M., Shuaib, K., & Khalil, K. (2023). Deep learning approach to security enforcement in cloud workflow orchestration. Journal of Cloud Computing, 12(1), 1-22.

[18]. Mangalagowri, R., & Venkataraman, R. (2023). Ensure secured data transmission during virtual machine migration over cloud computing environment. International Journal of System Assurance Engineering and Management, 1-12.

[19]. Chen, G., Qi, J., Sun, Y., Hu, X., Dong, Z., & Sun, Y. (2023). A collaborative scheduling method for cloud computing heterogeneous workflows based on deep reinforcement learning. Future Generation Computer Systems, 141, 284-297.

[20]. Hema, P., Paul, N. R., Čepová, L., Khan, B., Kumar, K., & Schindlerova, V. (2023). Complexity and Monitoring of Economic Operations Using a Game-Theoretic Model for Cloud Computing. Systems, 11(2), 50.

[21]. Lv, Y., Shi, W., Zhang, W., Lu, H., & Tian, Z. (2023). Don't trust the Clouds easily: The Insecurity of Content Security Policy based on Object Storage. IEEE Internet of Things Journal.

[22]. Das, R., & Inuwa, M. M. (2023). A review on fog computing: issues, characteristics, challenges, and potential applications. Telematics and Informatics Reports, 100049.

[23]. Zhao, S., Miao, J., Zhao, J., & Naghshbandi, N. (2023). A comprehensive and systematic review of the banking systems based on pay-as-you-go payment fashion and cloud computing in the pandemic era. Information Systems and e-Business Management, 1-29.

[24]. Joshi, A., Sasumana, J., Ray, N. M., & Kaushik, V. (2021). Neural network analysis. Advances in Bioinformatics, 351-364.

[25]. Sarkar, P., Dewangan, O., & Joshi, A. (2023). A Review on Applications of Artificial Intelligence on Bionic Eye Designing and Functioning. Scandinavian Journal of Information Systems, 35(1), 1119-1127.

[26]. Amini, M., & Bozorgasl, Z. (2023). A Game Theory Method to Cyber-Threat Information Sharing in Cloud Computing Technology. International Journal of Computer Science and Engineering Research, 11(4-2023).