# A Consumer-Centric Conceptual Framework for Trust Assessment in Cloud Computing 14

Amândio Balcão Filho, Ferrucio de Franco Rosa, Rodrigo Ruiz, Rodrigo Bonacin, and Mario Jino

**Abstract**

Consumers are heavily dependent on secure and reliable cloud computing services. However, there are various shortcomings in cloud services, such as those concerning performance, security, trust and privacy, among others. Cloud services consumers do not have enough information on these critical issues neither on compliance with laws and regulations. We present a conceptual framework for trust assessment of cloud computing environments. Our proposal is based on a consumer-centric approach, since it deals with cloud trust aspects from the perspective of end users. For this purpose, metrics and indicators are proposed to allow consumers to assess the trust of cloud services providers. Our contributions are: (1) a conceptual framework with indicators and processes for trust assessment; (2) a lightweight ontology of key concepts of trust assessment; and (3) an application scenario to illustrate the practical adequacy of the conceptual framework.

A. B. Filho (✉)
Renato Archer Information Technology Center (CTI), Campinas, Brazil

School of Electrical and Computer Engineering at University of Campinas (UNICAMP), Campinas, Brazil
e-mail: amandio.balcao@cti.gov.br

F. de Franco Rosa · R. Bonacin
Renato Archer Information Technology Center (CTI), Campinas, Brazil

University of Campo Limpo Paulista (UNIFACCAMP), Campo Limpo Paulista, Brazil

R. Ruiz
Renato Archer Information Technology Center (CTI), Campinas, Brazil

M. Jino
School of Electrical and Computer Engineering at University of Campinas (UNICAMP), Campinas, Brazil

**Keywords**

Cloud computing · Trust assessment · Metrics · Consumer-centric · Security · MCDM

## 14.1 Introduction

An effective trust management system should support cloud service providers (CSP) and consumers. Trust assessment mechanisms, distrusted feedbacks, poor identification of feedbacks, privacy of participants, and lack of feedbacks integration are examples of open issues, which still need to be investigated [1].

In this sense, models that are more comprehensive are necessary, based on a set of representative criteria such as those inspired by Saaty and Ergu [2]. These models should consider various aspects, including: reputation, performance, recommendation, policies, regulations, compliance with legislation and standards, accreditation by third party auditors, and mandatory disclosure of information security incidents. Thus, investigation is necessary of new forms of communication and efficient disclosure of information, considering its relevance and meaningfulness for end users. Indicators can be defined to include these aspects, pointing to trends considering quantitative and qualitative parameters. These indicators can serve as metrics of results of CSP actions and processes [3].

In [4], the authors point out that "Trust is a mental state comprising: (1) *expectancy*—the consumer expects (hopes for) a specific behavior from the provider (such as providing valid information or effectively performing cooperative actions); (2) *belief*—the consumer believes that the expected behavior occurs, based on the evidence of the provider's competence and goodwill; and (3) *willingness to take risk*—the consumer is willing to take risk for that belief." Trust is a matter of calculating advantage and risk under given

S. Latifi (ed.), *17th International Conference on Information Technology–New Generations (ITNG 2020)*, Advances in Intelligent Systems and Computing 1134,
https://doi.org/10.1007/978-3-030-43020-7_14

circumstances, which presupposes that experts will account for security incidents. It is understood that there is a balance between trust and acceptable risk, guaranteed by credibility of specialist systems, expertise, and contingent systems designed to mitigate the impacts of possible accidents [5].

Privacy is another emerging concern that is not fully addressed by the models. Privacy has a significant influence on the willingness of users to use cloud services [6]. Web services that violate user's privacy expectations are penalized by decline of confidence levels [7].

Contracts with CSP should be transparent and make clear security issues, as well as define relevant responsibilities in the business relationship with their customers [8]. Transparency relies on information and data provided by cloud providers. Monitoring is another key aspect on trust. Monitoring is often performed using metrics imposed by service providers. Decision-making relies on systems that continuously collect and process such data. From the users' perspective, decision-making is a combination of security transparency, confidence and interpretation of the collected data. A comprehensive, relevant and meaningful trust model should consider all these aspects [9].

We present a consumer-centric framework for trust assessment in cloud computing environments. Proposed indicators provide consumers of cloud services a means to assess trust of CSP. The improvement of consumers' confidence in cloud environments is a hard task; new criteria and indicators related to sensitive data, supported by proper metrics, are demanded.

The remainder of the paper is organized as follows: in Sect. 14.2 literature review and related work are presented; in Sect. 14.3 the conceptual framework for trust assessment is described; in Sect. 14.4 an application scenario is presented; in Sect. 14.5 our proposal is discussed; and finally, in Sect. 14.6 we present our final remarks and future work.

## 14.2 Literature Review and Related Work

This section contains a summary of a review; related work is described and compared. The review is based on guidelines for systematic mappings [10, 11]. Questions and keywords were chosen to collect relevant papers in scientific databases, such as: IEEE Xplore, ACM Digital Library, SpringerLink, among other databases. The following search string was used to select an initial set of papers from these databases: *((trust OR confidence) AND ("cloud computing") AND ("security information" OR privacy)).* The search was carried out on titles, considering the search period of 2015 to 2019. Firstly the selection of articles was based on their relevance according to the abstracts and conclusions.

Our literature review points out that there are few studies focusing on trust and transparency of security from the cloud consumers' point of view. There are also few articles that deal with communication of users with CSP such as how to give visibility to information security practices and how to enable consumers to understand these practices. Besides, reviewed papers do not discuss how to provide meaningful and relevant information to cloud shareholders, cloud service providers, or decision makers. The articles indicate the need of a unified approach for the following problems: (1) Difficulty to access security data of cloud systems; (2) Many models and metrics to measure cloud confidence; (3) Lack of information on management, resources and infrastructure aspects; (4) Lack of disclosure of information security incidents; and (5) Consumers' difficulty in identifying objective forms of relationship with providers. Table 14.1 summarizes our findings.

SOFIC (Security Ontology For InterCloud) [12] is standards-based and has been adapted to address the security requirements of different inter-cloud scenarios. A model named "Trust Model for Cloud Computing Environment", which includes mutual audit management agreements, is

**Table 14.1** Summary of the Related Work

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bernabe et al. [12] | X | | X | | | | X | X | X | | SI | Ontology, metrics |
| Branco and Santos [13, 14] | X | | X | | | X | | | | | SI | Metric, model |
| Chrysikos and Mcguire [15] | | X | X | X | X | | | X | | | SI | Taxonomy, framework |
| Dasgupta and Rahman [16] | | | X | | X | X | | | | | GV | Framework |
| Kai et al. [17] | X | | X | | | | | X | X | | GV, SI | Metrics |
| Noor et al. [18, 19] | X | X | | | | | | | | | GV | Framework |
| Rizvi et al. [20] | | | X | | X | | X | | X | | GV | Framework |
| Rizvi et al. [21] | | | X | | | | X | | X | | GV | Framework |
| Singh and Sidhu [22] | X | | | | X | | | | X | | GV | Framework |
| Our paper | | | | X | | | X | | X | | GV, TP, SI | Framework, metrics |

A = Paper reference; B = Performance; C = Reputation; D = Security design; E = Recommendation; F = User context aware; G = Contractual guarantees; H = Certification; I = Resources involved; J = Transparency; K=Information disclosure (security incidents); L = Domain (GV-Governance; SI-Security Information; TP-Transparency); M = Contribution type proposed in [13]. The model establishes a formal relationship involving relevant legal responsibilities. To establish and control the appropriate contractual requirements, technologies must be adopted to collect data needed to inform risk decisions, such as access usage, security controls, location and other data related to the use of the service. Contracts with CSP should be more transparent as well as more specific to make clear security issues and to define relevant responsibilities [14].

A taxonomy of trust models and classification of information sources for trust assessment is presented in [15], suggesting a new qualitative solution. A method for calculating security coverage for cloud services is proposed in [16]; it is based on the number and types of installed products and security tools. In [17] the authors propose a method to qualify the security status for cloud computing systems based on an approach with practical elements, techniques and attack graphs.

CloudArmor [18, 19] is a reputation-based trust management framework providing a set of capabilities to deliver Trust as a Service (TaaS); it includes: (1) a protocol to prove credibility of trusted feedbacks and preserve users' privacy; (2) a credibility model to measure the credibility of trusted feedbacks to protect the cloud services from malicious users and to compare the reliability of cloud services; and (3) a model to manage the availability of decentralized implementation of the trust management service. Specifically, CloudArmor is an adaptive conceptual model proposal to measure the credibility of user feedback to protect cloud services from malicious users.

In [20] a framework is proposed to ease the cloud service users (CSU) in choosing a CSP by: (a) allowing CSU to provide their security preferences with the desired cloud services; (b) providing a conceptual mechanism to validate the security controls and internal security policies of CSPs published in the CSA's (Cloud Security Alliance) Security Trust and Assurance Registry (STAR) database; and (c) maintaining a database of CSP along with their responses to the Consensus Assessments Initiative Questionnaire (CAIQ) as well as certificates issued by the certificate authorities. In [21] the authors extend the work to incorporate a third party auditing (TPA) for performing CAIQ analysis and to inform users.

A compliance-based multidimensional reliability assessment system (CMTES) is presented in [22]. It uses a variety of mathematical techniques to provide reliability assessment results from the perspective of various stakeholders, such as Cloud Auditors, Peers, and Cloud Brokers. The framework considers the customer's perspective from the point of view of performance and reliability (SLA) of cloud services; thus, issues related to information security and privacy are not part of their assessment framework.

## 14.3 Conceptual Framework for Trust Assessment

A decision is a 4-tuple: (1) Understanding of the problem to minimize doubts and uncertainties; (2) A complete structure to represent factors involving criteria and alternatives; (3) Measurement scales to represent judgments; and (4) A priority rank derived from numerical judgments.

Next, we present our conceptual proposal—a framework for trust assessment in cloud computing environments. The framework is consumer-centric and deals with trust aspects from the consumer or end user perspective.

The assessment result is presented as *Numeric Indicators* representing: the current evaluation, the history of previous evaluations, and the trend of consumer confidence in the cloud service. The indicators aim to allow a consumer-centric assessment of trust, and are adaptable and extensible to other contexts.

The foundations of the proposed framework come from three axioms representing increase of users' confidence in cloud services, namely:

1. *Information about the system, leads to trust.* Trust increases when there is meaningful and relevant communication, ease of interpretation, ease of access, and credibility of information.
2. *Meeting consumer expectations increases confidence.* Performance, protection of privacy and data security and responsiveness to questions foster trust.
3. *Positive opinions increase confidence.* Reputation, recommendation, certification and audits influence trust.

These axioms will serve as a basis for defining the domains that will make up the framework.

We consider three domains: *Transparency* (TP), *Security Information* (SI), and *Governance* (GV). These domains support the comprehension and contribute to the achievement of meaningful and relevant results for consumers. Each domain is divided into criteria and sub-criteria.

This section contains five subsections: (a) Conceptualization; (b) Engineering Process; (c) Framework Architecture; (d) Assessment Criteria; and (e) Indicators Calculation.

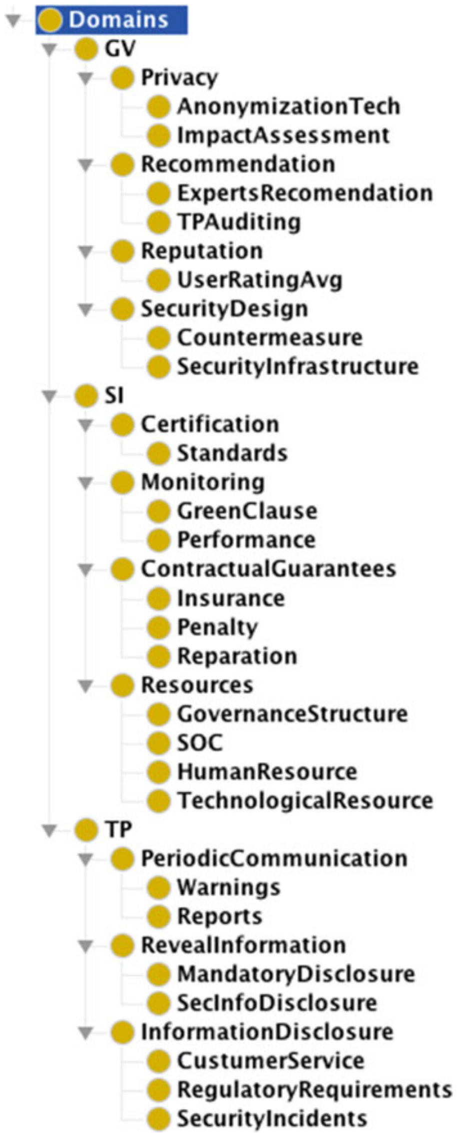
### 14.3.1 Conceptualization

Here, we present the main concepts necessary to understand our framework. A lightweight-ontology is presented to represent the relationships among the main concepts of the framework. In Fig. 14.1, we present the hierarchy of the proposed lightweight ontology.

*Governance* (GV) is the comprehensive set of requirements that support organizations to manage day-to-day processes, to assess security, privacy, regulatory, and business imperatives; it supports organizations to move forward, with some degree of control to obtain the customer's confidence.

*Security Information* (SI) is the aggregation of people effort, processes, and technology, to support organizations to provide confidentiality, integrity and availability in their information assets.

*Transparency* (TP) means "revealing sufficient information" to enable strategic decisions, providing mechanisms to ensure confidentiality needs of the CSP. Security transparency can be understood as appropriate dissemination of the governance aspects of security controls, policies and practices.



- Domains
  - GV
    - Privacy
      - AnonymizationTech
      - ImpactAssessment
    - Recommendation
      - ExpertsRecomendation
      - TPAuditing
    - Reputation
      - UserRatingAvg
    - SecurityDesign
      - Countermeasure
      - SecurityInfrastructure
  - SI
    - Certification
      - Standards
    - Monitoring
      - GreenClause
      - Performance
    - ContractualGuarantees
      - Insurance
      - Penalty
      - Reparation
    - Resources
      - GovernanceStructure
      - SOC
      - HumanResource
      - TechnologicalResource
  - TP
    - PeriodicCommunication
      - Warnings
      - Reports
    - RevealInformation
      - MandatoryDisclosure
      - SecInfoDisclosure
    - InformationDisclosure
      - CustumerService
      - RegulatoryRequirements
      - SecurityIncidents

**Fig. 14.1** Hierarchy lite-ontology

### 14.3.2 Engineering Process

We follow the six steps process proposed in [23] to develop our framework. Steps 1–4 are planning steps, Step 5 is an examination process, and step 6 is the decision-making process. We address Steps 1–5; we do not discuss the decision-making step. This final step is very complex and context dependent. We expect that the rigorous development of our evaluation model will deliver good *Indicators* for improving the decision-making process.

- *Step 1—Select the target of evaluation.* It refers to the object under evaluation. We have chosen to evaluate cloud computing services from the consumer perspective, regardless of being IaaS, PaaS or SaaS.
- *Step 2—Identify assessment criteria.* Literature often distinguishes between properties and attributes, but as argued in [24], we adopted them as interchangeable and refer to them as criteria. Our proposal considers that the evaluation of criteria is carried out through questions. Criteria are described in Subsection D—Assessment Criteria.
- *Step 3—Define evaluation yardstick.* A yardstick is a standard measure used to compare or to judge a certain target. Choosing the appropriate scale is a hard task and depends on the person and the decision problem [24]. The numerical values used in the scale affect the preferences of an individual; we cannot assure that a given method of preference disclosure is entirely independent of the measurement scale. The use of verbal responses is intuitive and may represent ambiguity in nontrivial comparisons.

Verbal statements can be represented by an ordered scale, because it is a feasible alternative when the evaluator does not have a comprehensive understanding of the problem [25].

We proposed the following scale, inspired in a "5 Likert ordinal scale" [26]: 0—Non-presence; 1—Strongly Disagree or Minimal Confidence; 2—Disagree or Acceptable Confidence; 3—Agree or Good Confidence; and 4—Strongly Agree or High Confidence. In our scale there is no neutral point, so that the evaluator is required to have either a positive or a negative opinion.

- *Step 4—Select and develop data gathering.* This step comprises the data gathering techniques required to obtain data to analyze each evaluation criterion. We have chosen: documents review, service monitoring tools, reputation or evaluation form (checklist), third party auditing, recommendation; primary data gathering techniques used to collect data from a specific resource.

- *Step 5—Select and develop synthesis techniques.* It refers to a set of well-defined steps and activities to synthesize all data and information (including the degree of importance for each criterion) to evaluate a target against the criteria. The synthesis techniques and equations are described in Subsection E—Indicators.
- *Step 6—Decision-making Process.* It refers to a series of specific activities and tasks to be executed to solve a specific decision problem.

### 14.3.3 Framework Architecture

Multi-Criteria Decision-Making (MCDM) methods, based on Cloud Service Evaluation Methods (CSEMs), were developed for different purposes, such as: classify, select, compose, adopt, improve and compare Cloud services. The results of the framework should be used for decision making in an MCDM. Our aim is to meet the recommendations of Saaty and Ergu [2]. We apply it first in the cloud context, due to it being a well-established service platform that allows us to test and validate the proposal. Once restrictions or gaps in the framework are known, it can be adapted and extended to other platforms and contexts.

In Fig. 14.2, we present a layered functional architecture of the framework. *Collecting* aims to collect data from the provider and external sources. *Processing* is intended for data processing (criteria and metrics). A database of metrics and indicators supports the framework. *Monitoring* is responsible for monitoring performance and revealed information. *Decision Making* is responsible for providing data for decision-making. Interface provides the visualization of indicators and allows the setting of parameters as well as score inputting by the consumer.

### 14.3.4 Assessment Criteria

When we evaluate trust in Cloud services, the information security facet is the first concern, but it is not enough. Other factors such as privacy, performance, transparency, and communication have a relevant weight in the trust assessment of Cloud providers [27]. All these factors must be evaluated through use of criteria. The choice of criteria and the composition of the model must follow requirements to make the model accomplish the objectives it proposes.

The evaluation criteria have the following principles [23]: (1) *Understandability*—evaluation criteria are well defined, meaningful for decision makers, easy to understand, clear and unambiguous; (2) *Decomposability*—evaluation criteria can be decomposed from the top of the hierarchy to its bottom to cover all important characteristics of decision making problem and to simplify evaluation processes; and (3) *Reliability*—evaluation criteria are formulated based

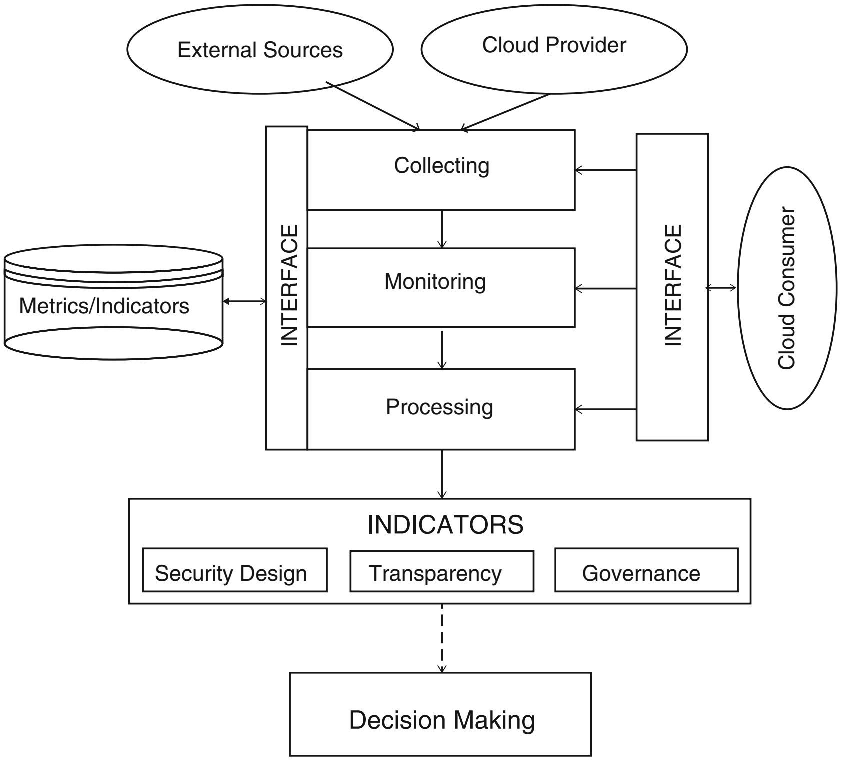


**Fig. 14.2** Layered functional architecture of the framework

on reliable sources and verified using formal verification approach.

The criteria and sub-criteria have been defined by a group of five experts in information security and cloud computing. Criteria and sub-criteria were grouped into three domains:

- *Governance* (GV)—*Security Design:* Security infrastructure (CGV1); Countermeasures (CGV2). *Recommendation:* Third Party Auditing (CGV3); Experts Recommendation (CGV4). *Reputation:* Users Rating Average (CGV5). *Privacy:* Privacy Impact Assessment (CGV6); Anonymization Techniques (CGV7).
- *Transparency* (TP)—*Reveal Information:* Security Information Disclosure (CTP1); Mandatory Disclosure (CTP2). *Information Disclosure:* Regulatory Requirements (CTP3); Security Incidents (CTP4); Customer Service (CTP5). *Periodic Communication:* Reports (CTP6); Warnings (CTP7).
- *Security Information* (SI)—*Resources:* Human Resources (CSI1); Security Operations Center (CSI2); Governance Structure (CSI3); Technological Resources (CSI4). *Certifications:* Standards (CSI5). *Contractual Guarantees:* Insurance (CSI6); Penalty (CSI7); Reparation (CSI8). *Monitoring:* Performance (CSI9); Green Clause (CSI10).

### 14.3.5 Indicators Calculation

A framework for evaluation should provide a complete mathematical and logical solution with its justifications. Therefore, there is a formal mathematical representation of logic and reasoning behind the theory underlying the evaluation model. Metrics and indicators are proposed, in addition to a sequence of steps called stages.

Indicators are calculated for each domain (GV, TP, SI). If there is more than one evaluator per criterion, the geometric mean for each sub-criterion should be calculated, so that only one value enters the calculations by sub-criterion. It has been proven that the geometric mean, not the arithmetic mean, is the correct way to do this [28].

Thus, for each domain, the Indicators are calculated through 8 steps:

1. Evaluate all sub-criteria, Cxxi;
2. Calculate, Eq. (14.1), the arithmetic mean, per domain, based on the values of Step 1, GVj, TPj, SIj, (1);
3. Calculate the difference between the average of the current month and the average of the immediately previous month—values obtained in step 2; e.g. (GVj − GVj$_{-1}$) the result represents the tendency for the future;
4. Calculate the average of the last 12 means obtained in Step 2, the result represents the history;
5. Add the plots obtained with the following calculation: *k1* times the value of Step 2; *k2* times the value of Step 3 and *k3* times the value of Step 4. This weighted sum summarizes the current assessment, the trend for the future and the history of the evaluations;
6. Divide the result from Step 5 by 2 power *m*, where *m* is the number of catastrophic or extremely shocking security incidents that occurred in the month, such as data breaches, leakage of customer information, disaster recovery;
7. Calculate the Indicator for the domain by multiplying the result of Step 6 by a bonus *RB*, related to the relationship time, which will vary from 1 to 10%, to be assigned by the consumer based on the experience in the last evaluation period (2);
8. Present the Indicators, which reflect the trust placed by the consumer in that Cloud service under evaluation.

Equation (14.2) incorporates three plots, the first represents the proportional term, the second the trending, and the third the history; weighted by parameter *k1*, *k2*, and *k3* which varies from 0.00 to 1.00; and the $k_i$ sum must be equal to 1.00. The relationship bonus *RB* and *m* reflect the dynamism of the Cloud service. *RB* can increase trust by up to 10%; while serious security incidents (m) split trust by $2^{\mathrm{m}}$.

The example shown applies to the GV domain. The same formulas should be applied to the other two domains (TP and SI). CGV represents the score (0–4) of the criteria under evaluation, defined by the evaluator. IGV represents the GV Indicator. The assessment should be performed monthly, so that we have a follow-up on the behavior of the CSP.

$$GV_j = \frac{\sum_{i=1}^{n} CGV_i}{n} \tag{14.1}$$

$$IGV_j = \frac{\left(\left(k1 \times GV_j\right) + \left(k2 \times \left(GV_j - GV_{j-1}\right)\right) + \left(k3 \times \sum_{j-12}^{j} GV_j/12\right)\right) \times RB}{2^m} \tag{14.2}$$

## 14.4 An Application Scenario

Consider an application scenario in which a DevOps team (software house) needs to evaluate a cloud service (IaaS and PaaS) for choosing a CSP by considering features, costs, etc. DevOps is a term designed to describe a set of practices for integration between the software development, operations (infrastructure), support teams (e.g. Quality control) and the adoption of automated processes for fast and secure deployment of applications and services. It is a process that makes possible the CI/CD (continuous integration/continuous deployment), i.e., the agile application development.

Members of the team answer structured questions by means of an online form. Four security experts previously prepared the questions as part of the proposed framework. These experts set the framework based on the expectations and needs of the DevOps team. The form is part of a system that collects all answers and makes the necessary calculations to provide the trust Indicators in the cloud service assessment. This way, an average consumer can easily use the framework and perform the assessment. The team should periodically repeat this assessment to get an overview of how the confidence in the contracted service is evolving. With these results it is possible to make decisions about changes that prove necessary.

The DevOps team is completely dependent on the CSP and its services to operate their business. Hence the importance of the trust placed in the CSP.

The team is distributed around the world, with a central office where the policies and most of the management tasks are performed. This team has as priorities the reliability and confidentiality of the service. They apply the proposed framework to evaluate the trust in the chosen service. An evaluation was carried out and the outcomes of the initial assessment are presented in Appendix.

## 14.5 Discussion

We proposed the framework taking into account the coherence with the definition of Trust adopted in Sect. 14.1, with the given axioms presented in Sect. 14.3, and the end user's decision-making perspective. The consumer relies on cooperation, goodwill, competence, explicit contractual guarantees, expert and consumer recommendations, as well as contingent systems that could mitigate negative impacts.

The proposed Indicators (IGV, ITP, ISI—Sect. 14.3.5) represent the consumers' evaluation in relation to the provider. These Indicators have internal validity because the bases employed in their construction are theoretically and contextually grounded, and have shared meanings between the participants—consumer and provider. The intended external validity refers to the possibility of generating knowledge that contributes to the improvement of services and interaction among participants. These indicators are used as outcome metrics for processes and actions of the CSP.

The proposed architecture has operational characteristics, which were adapted from [29]: (1) Appropriateness—It refers to the quality of being suitable or proper to the problem at hand; (2) Ease to use—no expert is needed to supervise the usage process; (3) Reliability—evaluation criteria are being formulated based on reliable and verified sources; and (4) Validity—justifications are used to validate its procedures and prove its effectiveness with real world examples.

The measurement scale, introduced to evaluate the performance of each alternative with respect to each criterion, is able to handle the classification of tangible and intangible criteria. The values assigned to each criterion are synthesized by a merge function to obtain the outcomes (Sect. 14.3.5).

The framework is adaptable to different contexts, via parameterization and formulation of evaluation questions; for example, it can be extended to other contexts as IoT or Edge Computing. The comparison month-to-month shows the evolution of trust.

The GV Indicator represents how the CSP is structured, based on technological resources, third party evaluations, as well as opinions and audits. The TP Indicator represents security transparency and relationship with the consumer. The SI Indicator represents the contractual guarantees, performance monitoring and the socio-technical resources.

The framework is simple to use and provides the capability to build a comprehensive decision structure, with breadth, depth and merit. This is particularly relevant when the decision is complex and, in addition, involves Benefits, Opportunities, Costs and Risks (BOCR).

Therefore, the framework provides valid outcomes useful for different types of decisions.

### 14.5.1 Obstacles of Cloud Assessment Models

Assessments are made by considering data from the CSPs that are not always available; as well as it is impossible to know which protocols that was used for collecting these data. There is a lack of information to provide security transparency. This circumstance is changing, as users demand their rights as consumers of services, which should be protected by consumer protection laws. There is also a need for more regulation of these services to overcome obstacles in communicating with providers, as well as mandatory notification of significant events for the security and trust of the services. There is still much uncertainty as to the representativeness of the criteria and parameterization adopted. By using the proposed framework, could be possible to adjust these criteria and parameters.

## 14.6 Conclusion

Customer's confidence and trust on cloud services are impacted by cost, responsibilities, quality and assurance provided by Cloud Service Providers (CSP). Cloud computing has been receiving a lot of attention in the last years.

A consumer-centric framework for trust assessment in cloud computing environments is proposed; it aims to provide metrics and indicators that allow consumers of cloud services to measure Trust on a CSP. We consider in the calculus, for example: security events or incidents with great impact on trust; a relationship bonus; history of evaluations; and trends. The framework is extensible and can be applied to other complex contexts, such as IoT, Edge, and Fog Computing.

A conceptual formalization, expressed by means of a lightweight ontology, is proposed and described. It models the hierarchy of the main concepts of trust assessment in the cloud-computing context.

Our main contributions are: (1) a conceptual framework, composed of indicators and processes for trust assessment; (2) a lightweight ontology that includes the hierarchy of the main concepts on trust assessment; and (3) an application scenario that simulates the usage of the conceptual framework in a trust assessment of a CSP.

The contribution of the article is significant because it proposes a framework that meets the needs of assessing the consumer confidence. Consumers do not need to have extensive knowledge of the operational aspects of cloud services, so they can carry out the evaluation. Also, the ease of evaluating and monitoring the evolution of trust about the relationship between the CSP and the contractor, are aspects that contribute to the cloud computing research area. As far as we can see it is the only framework that uses Indicators to present the results, making the trust assessment from the consumers' point of view.

Our framework contributes to the improvement of confidence assessment models for complex environments(e.g. Systems-of-systems), by using a unified approach that considers tangible and intangible criteria and socio-technical aspects. It also contributes to overcoming the shortcomings presented in Sect. 14.2.

### 14.6.1 Future Research and Recommendations

Important aspects to be considered in future research are related to the transparency of security, the measurement metrics of service levels and also the interpretation of the data used in decision-making. Also, ease to use, ease of interpretation and ease of access must be considered. These aspects need to be considered in a relevant, meaningful and comprehensive framework. There is a world of underutilized data on the back-end of the providers that could be used to improve the service quality for both providers and consumers. When evaluating complex systems, users must evaluate the security aspects of these environments. The complexity of making this assessment is so high that a team of experts is needed; also, the evaluation will be outdated in a short time.

The best approach is to assess the trust placed in this complex environment rather than the cyber security of the environment. The responsibility of the cyber security rests with the provider. The consumers are responsible for their own environment. By using Indicators it is possible to communicate, in a simply and meaningfully manner, how well the security, reliability, and other aspects of a cloud service are going.

Further studies are also needed on which Indicators best represent the qualities and characteristics of the CSPs under evaluation. Therefore, approaches that use Indicators seem to be more promising, as it reveals trends, incorporates several evaluation actors, and communicates in simpler manners.

## A.1 Appendix: Applying the Framework (Criteria and Sub-Criteria) in a Cloud Service

| | | | | | | A | B | C | D | E | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Domain | Criteria | ID $Cxx_i$ | Sub-criteria | Criteria Score (0–4) | Score Average $GV_J$, $TP_J$, $SI_J$ | *k1 0.50* | *k2 0.25* | *k3 0.25* | *RB 1* | *m 0* | F |
| Governance | Security design | CGV1 | Security infrastructure | 1 | 2.14 | 1.07 | 0.00 | 0.53 | 1.62 | 1.60 | $IGV_j$ 1.60 |
| | | CGV2 | Counter measures installed | 2 | | | | | | | |
| | Recommendation | CGV3 | Third party auditing | 3 | | | | | | | |
| | | CGV4 | Experts recommendation | 1 | | | | | | | |
| | Reputation | CGV5 | Average users assessment | 3 | | | | | | | |
| | Privacy | CGV6 | Privacy impact assessment | 4 | | | | | | | |

(continued)

| | | | | | | A | B | C | D | E | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Domain | Criteria | ID $Cxx_i$ | Sub-criteria | Criteria Score (0–4) | Score Average $GV_J$, $TP_J$, $SI_J$ | *k1 0.50* | *k2 0.25* | *k3 0.25* | *RB 1* | *m 0* | F |
| | | CGV7 | Anonymization techniques | 1 | | | | | | | |
| Transparency | Review information | CTP1 | Security information disclosure | 2 | 2.42 | 1.21 | 0.00 | 0.60 | 1.83 | 1.81 | $ITP_j$ 1.81 |
| | | CTP2 | Mandatory disclosure | 4 | | | | | | | |
| | Information disclosure | CTP3 | Regulatory requirements | 4 | | | | | | | |
| | | CTP4 | Security incidents | 3 | | | | | | | |
| | | CTP5 | Customer service | 1 | | | | | | | |
| | Periodic communication | CTP6 | Reports | 1 | | | | | | | |
| Security | Resources | CTP7 | Warnings | 2 | 2.10 | 1.05 | 0.00 | 0.52 | 1.59 | 1.57 | $ISI_j$ 1.57 |
| information | | CSI1 | Human resources | 1 | | | | | | | |
| | | CSI2 | Security operation center | 1 | | | | | | | |
| | | CSI3 | Governance structure | 3 | | | | | | | |
| | | CSI4 | Technological resources | 4 | | | | | | | |
| | Certifications | CSI5 | ISO27001, GDPR, STAR CSA, ISO27018, ITIL | 1 | | | | | | | |
| | Contractual Garantees | CSI6 | Insurance | 2 | | | | | | | |
| | | CSI7 | Penalty | 3 | | | | | | | |
| | | CSI8 | Reparation | 2 | | | | | | | |
| | Monitoring | CSI9 | Performance (QoS, SLA) | 3 | | | | | | | |
| | | CSI10 | Green clause | 1 | | | | | | | |

(A) Current month; (B) Previous month difference; (C) Last 12 months average; (D) Relationship bonus—RB; (E) Catastrophic events—m; and (F) Indicator. The values of sensibilities are: k1 = 0.50; k2 = 0.25; k3 = 0.25

## References

1. Noor, T.H., Sheng, Q.Z., Zeadally, S., Yu, J.: Trust management of services in cloud environments: obstacles and solutions. ACM Comput. Surv. **46**(1), 1–30 (2013)
2. Saaty, T.L., Ergu, D.: When is a decision-making method trustworthy? Criteria for evaluating multi-criteria decision-making methods. Int. J. Inf. Technol. Decis. Mak. **14**(06), 1171–1187 (2015)
3. Minayo, M.C.S.: Construção de indicadores qualitativos para avaliação de mudanças. Rev. Bras. Educ. Med. **33**(1 Supl), 83–91 (2009)
4. Nicol, D.M., Huang, J.: A formal-semantics-based calculus of trust. IEEE Internet Comput. **14**(5), 38–46 (2010)
5. Giddens, A.: The Consequences of Modernity. Stanford University Press, London (1991)
6. Asadullah, A., Oyefolahan, I.O., Bawazir, M.A., Hosseini, S.E.: Factors Influencing users' willingness to use cloud computing services: an empirical Study. In: Recent Advances in Information and Communication Technology, vol 361, pp. 227–236. IC2IT (2015)
7. Martin, K.: The penalty for privacy violations: how privacy violations impact trust online. J. Bus. Res. **82**, 103–116 (2017)
8. Branco, T., Santos, H.: What is missing for trust in the cloud computing? In: Proceedings of the 2016 ACM SIGMIS Conference on Computers and People Research, pp. 27–28. ACM, New York (2016)
9. Ardagna, C.A., Asal, R., Damiani, E., Vu, Q.H.: From security to assurance in the cloud: a survey. ACM Comput. Surv. **48**(1), 2 (2015)
10. Biolchini, J., Mian, P.G., Candida, A., Natali, C.: Systematic review in software engineering. Engineering. **679**, 165–176 (2005)
11. Kitchenham, B.: Procedures for performing systematic reviews. Keele UK Keele Univ. **33**(TR/SE-0401), 28 (2004)
12. Bernabe, J.B., Perez, G.M., Skarmeta Gomez, A.F.: Intercloud trust and security decision support system: an ontology-based approach. J. Grid Comput. **13**(3), 425–456 (2015)
13. Branco, T.T., Santos, H.: A trust model for cloud computing environment. In: 3rd International Conference on Cloud Security Management Security (ICCSM 2015), pp. 1–15. IEEE (2015)
14. Branco, T., Santos, H.: What is missing for trust in the cloud computing? In: Proceedings of the 2016 ACM SIGMIS Conference on Computers and People Research, pp. 27–28. ACM (2016)

15. Chrysikos, A., Mcguire, S.: A Predictive Model for Risk and Trust Assessment in Cloud Computing: Taxonomy and Analysis for Attack Pattern Detection. Springer, Berlin (2018)
16. Dasgupta, D., Rahman, M.: A framework for estimating security coverage for cloud service insurance. In: CSIIRW '11: Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research. ACM (2011)
17. Kai, S., Shigemoto, T., Kito, T., Takemoto, S., Kaji, T.: Development of qualification of security status suitable for cloud computing system. In: Proceedings of the 4th International Workshop on Security Measurements and Metrics - MetriSec'12, pp. 17–24. ACM (2012)
18. Noor, T.H., Sheng, Q.Z., Ngu, A.H.H., Alfazi, A., Law, J.: Cloud armor : a platform for credibility-based trust management of cloud services. In: Proceedings of the 22nd ACM International Conference on Conference on Information & Knowledge Management, pp. 2509–2511. ACM (2013)
19. Noor, T.H., Sheng, Q.Z., Yao, L., Dustdar, S., Ngu, A.H.H.: CloudArmor: supporting reputation-based trust management for cloud services. IEEE Trans. Parallel Distrib. Syst. **27**(2), 367–380 (2016)
20. Rizvi, S., Ryoo, J., Kissell, J., Aiken, B.: A stakeholder-oriented assessment index for cloud security auditing. In: Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication - IMCOM '15, pp. 1–7. ACM (2015)
21. Rizvi, S., Karpinski, K., Kelly, B., Walker, T.: Utilizing third party auditing to manage trust in the cloud. Procedia Comput. Sci. **61**, 191–197 (2015)
22. Singh, S., Sidhu, J.: Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers. Futur. Gener. Comput. Syst. **67**, 109–132 (2017)
23. Alabool, H., Kamil, A., Arshad, N., Alarabiat, D.: Cloud service evaluation method-based multi-criteria decision-making: a systematic literature review. J. Syst. Softw. **139**, 161–188 (2018)
24. Harker, P.T., Vargas, L.G.: The theory of ratio scale estimation: Saaty's analytic hierarchy process. Manag. Sci. **33**(11), 1383–1403 (2008)
25. Franek, J., Kresta, A.: Judgment scales and consistency measure in AHP. Procedia Econ. Financ. **12**, 164–173 (2014)
26. Joshi, A., Kale, S., Chandel, S., Pal, D.: Likert scale: explored and explained. Br. J. Appl. Sci. Technol. **7**(4), 396–403 (2015)
27. Eftekhar, S.M., Suryn, W., Roy, J., Roy, H.: Towards the development of a widely accepted cloud trust model. In: Computing and Quality: SQM XXVI, pp. 73–94. Solent University, Southampton (2018)
28. Saaty, T.L.: Decision making with the analytic hierarchy process. Int. J. Serv. Sci. **1**(1), 83–98 (2008)
29. Hobbs, B.F.: What can we learn from experiments in multiobjective decision analysis? IEEE Trans. Syst. Man Cybernet. **16**(3), 384–394 (1986)