Trust-Aware Decision-Making Methodology for Cloud Sourcing*

Francisco Moyano[1], Kristian Beckers[2], and Carmen Fernandez-Gago[1]

[1] Department of Computer Science
University of Malaga, 29071 Malaga, Spain
{moyano,mcgago}@lcc.uma.es
[2] paluno - The Ruhr Institute for Software Technology -
University of Duisburg-Essen, Germany
firstname.lastname@paluno.uni-due.de

Abstract. Cloud sourcing consists of outsourcing data, services and infrastructure to cloud providers. Even when this outsourcing model brings advantages to cloud customers, new threats also arise as sensitive data and critical IT services are beyond customers' control. When an organization considers moving to the cloud, IT decision makers must select a cloud provider and must decide which parts of the organization will be outsourced and to which extent. This paper proposes a methodology that allows decision makers to evaluate their trust in cloud providers. The methodology provides a systematic way to elicit knowledge about cloud providers, quantify their trust factors and aggregate them into trust values that can assist the decision-making process. The trust model that we propose is based on trust intervals, which allow capturing uncertainty during the evaluation, and we define an operator for aggregating these trust intervals. The methodology is applied to an eHealth scenario.

Keywords: trust, cloud computing, decision making, security, domain knowledge elicitation.

1 Introduction

There is an increasing trend to outsource IT services and infrastructures to the cloud [1]. This model, also called cloud sourcing[1], is replacing traditional outsourcing engagements due to its advantages [2]. These include the provision of elastic IT resources and cost savings as a result of reduced operational costs for complex IT processes [3].

* This research was partially supported by the EU project Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS, ICT-2009.1.4 Trustworthy ICT, Grant No. 256980), and by the Spanish Ministry of Science and Innovation through the research project ARES (CSD2007-00004). The first author is funded by the Ministry of Education through the national F.P.U. program.

[1] Techopedia: http://www.techopedia.com/definition/26551/cloudsourcing

M. Jarke et al. (Eds.): CAiSE 2014, LNCS 8484, pp. 136–149, 2014.

Security and trust are significant barriers for the adoption of clouds in companies [4]. Lack of trust in cloud providers lies within the nature of clouds: storage and management of critical data, and execution of sensitive IT processes are performed beyond the customers control. As a consequence, new security threats arise[2,3], and IT decision makers must balance the advantages and these threats before making decisions. These decisions range from selecting a cloud provider to determining how much data or which part of the infrastructure moving to the cloud.

Trust includes the expectation that we hold on another party regarding the outcome of an interaction with that party. Even when there is not any agreed definition for trust, it is generally accepted that it can help in decision-making processes in the absence of complete information [5,6]. Given that information about cloud providers, due to internal policy or strategic reasons, may be uncertain and incomplete, trust can enhance the cloud sourcing decision-making process.

We present a methodology that evaluates trust in cloud providers and that can help IT decision makers to make more informed decisions during the outsourcing process. The methodology provides a systematic way to gather knowledge about cloud providers and to exploit this knowledge in order to yield trust values that can be used as inputs to the decision-making process. The methodology pinpoints which aspects of the providers should be analysed, indicators that decision makers can use to quantify these aspects, and how these quantifications can be aggregated into trust values. We use trust intervals in order to quantify trust and we define a summation operator to aggregate trust intervals. The methodology constitutes a guide that decision makers can follow to evaluate their trust in cloud providers under several dimensions or viewpoints.

The paper is structured as follows. Related work is discussed in Section 2. We explain the methodology in Section 3, whereas in Section 4 we present its application to an eHealth scenario. We discuss some aspects of the methodology in Section 5 and we conclude the paper in Section 6, where we also outline some directions for future research.

We present an extended version of this paper in a technical report, which is available for the interested reader[4].

2 Related Work

Cloud provider evaluation is a necessary step for cloud sourcing decision-making, but clouds can be evaluated under different angles, including performance [7], scalability [8], accountability [9] and transparency [10].

The impact of trust for cloud adoption and some trust-related factors that influence users when selecting cloud providers have been identified in previous

[2] `http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853`

[3] Top Threats to Cloud Computing V1.0, `https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf`

[4] Technical report: `http://www.uml4pf.org/publications/trust.pdf`

works [11][12]. In this direction, Sarwar et al. [13] review several works that elicit relevant trust aspects in the cloud. Ahmad et al. [14] argue that trust in the cloud must be built upon a deep knowledge about the cloud computing paradigm and the provider.

In many works, trust depends on the verification of Service Level Agreements (SLAs) [15] or the measurement of Quality of Service (QoS) attributes [16]. However, these works are usually focused on cloud services evaluation and selection rather than on the cloud providers themselves.

Pavlidis et al. [17] propose a process for trustworthy selection of cloud providers. This selection is based on how well the cloud provider fulfils the customer's security and privacy requirements. It also aims to reduce uncertainty by justifying trust relationships and by making trust assumptions explicit. Compared to our approach, we consider other aspects of the cloud providers and we use trust intervals instead of probabilities and weights.

Supriya et al. [18] propose a fuzzy trust model to evaluate cloud service providers that uses the attributes defined by the Service Measurement index (SMI) [19]. Examples of these attributes are assurance, performance and security. Even though uncertainty is embedded in the fuzzy engine, the authors do not provide guidelines on quantifying the attributes or on eliciting cloud knowledge. Qu et al. [20] introduce customers' feedback in the evaluation, although this evaluation is focused on cloud service selection, rather than on cloud provider selection.

As a conclusion from our literature review, trust has already been incorporated in the evaluation of clouds. However, in most cases, the purpose of this evaluation is service selection, rather than cloud provider selection. Most contributions are also focused on the metrics rather than on a concrete methodology to gather and quantify all the information. Uncertainty or subjectivity, which are intrinsic to the notion of trust, are usually laid aside. This paper aims to fill these gaps. The existing literature provides valuable information about the aspects of cloud providers that are usually considered by cloud customers before moving to the cloud, and our approach builds upon this knowledge.

3 Trust-Aware Methodology for Decision Making

In this section, we present a methodology to evaluate trust in cloud providers. A high-level overview of the methodology is depicted in Figure 1. The first step consists of gathering knowledge about the cloud provider. Next, we elicit and quantify a set of trust factors about the provider's stakeholders and about the cloud provider as a whole. In parallel, we specify trust thresholds that are based on the scenario requirements. These thresholds are minimum trust values that we expect for a given scenario. In the following step, the factors are aggregated into three dimensions or viewpoints: a stakeholder dimension, a threat dimension, and a general dimension. In order to perform the aggregation, we define a summation operator. Finally, the information is graphically visualized.

Next sections discuss each step in detail.

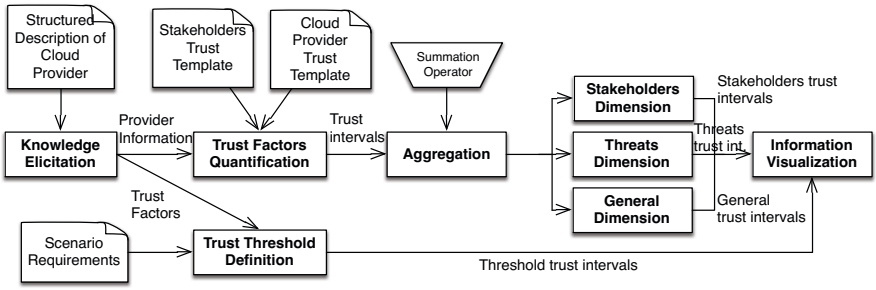

Fig. 1. Overview of the Methodology

3.1 Domain Knowledge Elicitation

The goal of this step is to gather knowledge about the cloud provider and the cloud domain. We propose context-pattern for a structured domain knowledge elicitation [21]. These patterns contain a graphical pattern and templates with elements that require consideration for a specific context. In addition, our context-pattern contains a method for eliciting domain knowledge using the graphical pattern and templates. For this work we use a specific context pattern, the so-called *cloud system analysis pattern* [22,23]. It describes stakeholders and other systems that interact with the *Cloud*, i.e. they are connected to the cloud by associations. For example, the *cloud provider* offers its resources to *cloud customers* as *Services*, i.e., *IaaS*, *PaaS*, or *SaaS*. However, it is also possible to use other methods for structured domain knowledge elicitation during this step of our method such as the one proposed in [24]. Once we have gathered general knowledge about the provider, we focus on the trust factors in the next step.

3.2 Trust Factors Quantification

The goal of this step is to quantify the factors that are used to evaluate trust. Factors are aspects and non-functional requirements that may influence a trust decision.

The Stakeholder Trust Template (STT) in Table 1 is a modification over the original stakeholder template [21], and identifies the trust factors that we consider for each stakeholder. In Table 2 we present an excerpt of the Cloud Provider Trust Template (CPTT)[5], which identifies the trust factors that we consider for the cloud provider. In each table, the first two columns show the name of the factor and its meaning respectively, whereas the last column provides hints for quantifying the factors.

Quantification in our methodology entails providing two values for each factor: the factor value itself and a confidence value. The latter refers to the confidence

[5] The complete table is in the Technical Report:
`http://www.uml4pf.org/publications/trust.pdf`

that the factor value is accurate. The role of this value is to make explicit the uncertainty derived from having partial and subjective information.

For the quantification of each factor and confidence value, we decide to use only integer numbers from 0 to 3. More justification on this decision and on the trust engine[6] in general is provided in Section 5.

In our methodology, threats are sub-factors of two trust factors: *direct interaction* and *3rd party referrals*. The former refers to information about threats derived from previous direct experience with the cloud provider, whereas the latter requires asking external organizations for this information. We use the threats identified by the Cloud Security Alliance[7], which summarize the experience of a large industrial consortium in the field of cloud computing.

Once we have a factor value and its corresponding confidence value, we calculate a *trust interval* for each factor, as explained in the next definition.

Definition 1 (Trust Interval). *Let v and c be a factor value and its corresponding confidence value, respectively. These values are integer numbers between 0 and 3. We form the trust interval as:* $TI = [\frac{vc}{3}, \frac{vc}{3} + (3 - c)]$.

This interval is in the domain of the real numbers. 0 and 3 are lower and upper bounds of the interval, respectively. For the rationale of this definition we refer the reader to the contribution by Shakeri et al. [25]. Given that we use integer values, there is a finite set of possible intervals during quantification. For example, when the factor value is 2 and the confidence value is 1, the resulting trust interval is $[\frac{2}{3}, \frac{8}{3}]$. Note that when $c = 0$, we have the maximum uncertainty, that is, the interval is $[0, 3]$ and has the maximum width. When $c = 3$, uncertainty is minimum, that is, the interval width is zero because we know the trust value.

Table 1. Stakeholder Trust Template

Direct Interaction	Evaluation of previous direct interaction with the stakeholder.	Analyse the number of incidents and overall satisfaction with the stakeholder in the past.
3rd Parties referrals	Referrals from 3rd parties regarding interactions with the stakeholder.	Ask other organisations about their general satisfaction with the stakeholder.
Knowledge	Stakeholder knowledge on its task.	Check number of years of experience and whether the stakeholder has any certification.
Willingness	Willingness of the stakeholder to perform the task.	Take into account the aforementioned factors; research on the motivations of the stakeholder (e.g. bonuses); check how long it takes him to finish his task.

Before proceeding to the aggregation of the trust intervals, decision makers define trust thresholds as explained in the next section.

[6] A trust engine is a set of rules or mathematical functions that yield trust values.

[7] Threats are listed in the Technical Report: `http://www.uml4pf.org/publications/trust.pdf`

Table 2. Excerpt of the Cloud Provider Trust Template

SLA and Contracts	Quality of SLAs and signed contracts that express the conditions and liabilities regarding the service offered by the cloud provider.	Check if there was some abuse of the contract or SLAs.
Security	Provider's concern and actions on security.	Check whether the cloud provider participates in cloud standards bodies such as CloudAudit, Open Cloud Computing Interface, CSA and ENISA. Does the cloud provider perform security assessment?
Transparency	Transparency of the provider.	How difficult is to retrieve data from the cloud provider? Does it publish its privacy and security policies?
Direct interaction	Own experience in the interaction with the cloud provider.	Evaluate direct experience against threats.
3rd parties referrals	Referrals from 3rd parties regarding interactions with the cloud provider.	Evaluate 3rd parties referrals against threats.

3.3 Trust Thresholds Definition

This step, which is performed in parallel with the quantification step, defines trust thresholds according to the scenario requirements. These thresholds represents the minimum trust that decision makers expect for each trust factor. The goal is to have a yardstick that can be used to check whether cloud providers meet our trust expectations.

For each trust factor, the decision maker assigns an expected factor value and a confidence value. In this case, the confidence value expresses how sure the decision maker is about the need to expect the corresponding factor value. As in the quantification step, for each factor, a trust interval is derived from these values by using Definition 1.

3.4 Trust Aggregation

During the previous steps we have calculated trust intervals for different factors of stakeholders and cloud providers. This step reduces the number of trust intervals by aggregating them.

Before defining the operator that performs the aggregations, we need another definition.

Definition 2 (Interval Accuracy). *Given a trust interval* $[a, b]$*, we define the interval accuracy as* $IA = 3 - w$*, where* $w = b - a$ *is the width of the interval.*

The maximum possible width of a trust interval is 3 (see Definition 1). When the width is maximum, the interval accuracy is 0 because uncertainty is maximum. On the other hand, when the width of a trust interval is 0, the interval accuracy is 3 because uncertainty is minimum.

Next we define a summation operator that aggregates trust intervals.

Definition 3 (Summation Operator). *Given two trust intervals* $[a, b]$ *and* $[c, d]$*, where* $a \neq c$ *or* $b \neq d$*, we define the summation operator* $\oplus$ *as* $[a, b] \oplus [c, d] = [e, f]$ *where* $[e, f]$ *is a new trust interval that can be obtained as:* $e = \frac{IA_1 a + IA_2 c}{IA_1 + IA_2}$ *and* $f = \frac{IA_1 b + IA_2 d}{IA_1 + IA_2}$*.* IA_1 *and* IA_2 *are the interval accuracy of* $[a, b]$ *and* $[c, d]$*, respectively. If* $a = c$ *and* $b = d$*, then* $[a, b] \oplus [c, d] = [a, b] = [c, d]$*.*

The resulting interval after a summation is somewhere in between the two source intervals. The uncertainty, represented by the interval accuracy, determines how close e is to a or c, and how close f is to b or d. This is why we weight a, b, c and d by the interval accuracy. The higher the interval accuracy, the more the values of the corresponding interval contributes. Note that the operator has an identity element: $[0, 3]$. This makes sense as this interval expresses the maximum uncertainty and does not add any knowledge to the trust value.

In order to present meaningful trust information, we suggest performing three aggregations that correspond to three dimensions or viewpoints: the stakeholders dimension, the threats dimension and the general dimension. Next subsections explain each of them.

Stakeholders Dimension. This dimension illustrates the level of trust in the cloud provider according to the stakeholders working in it. This aggregation is performed by summing all the intervals of all the factors for each stakeholder, and then summing the resulting intervals for all the stakeholders.

Threats Dimension. This dimension shows the amount of trust in the cloud provider according to the threats defined by the Cloud Security Alliance (CSA)[3]. For each threat, we aggregate the trust intervals of the *direct interaction* and *3rd party referrals* factors.

We believe that having independent trust intervals for each threat is convenient, instead of aggregating all the different threats together, because decision makers can make more fine-grained decisions. For example, if the trust interval is low for the threat *Data Loss & Leakage*, the decision maker can decide not to move the customers data of the organisation to the cloud provider. However, if trust intervals of the other threats for the same cloud provider are high, some services or infrastructures could be outsourced to that cloud provider. If we aggregated all the threats into a unique trust interval, we would lose this valuable information.

General Dimension. This dimension depicts trust in the cloud provider with regards to the rest of trust factors that are not threats, including *Security*, *Transparency* and *Accountability*.

After the trust aggregation step, there are ten trust intervals for a cloud provider: one for the stakeholders dimension, eight for the threats dimension (i.e. one for each threat) and one in the general dimension.

3.5 Trust Information Visualization

The last step consists of plotting the trust intervals for each dimension for comparison purposes and decision making.

In the Y-axis, we represent possible trust values, whereas in the X-axis we represent the three dimensions. For each dimension, we draw a line from the lower bound to the upper bound of its trust intervals. This arrangement allows fast comparison between providers in each dimension. Likewise, it allows comparing the trust intervals with the trust thresholds.

This is better illustrated in the next section, where we apply the methodology to an eHealth scenario.

4 Evaluation in an eHealth Case Study

In this section we present an application of our methodology to a case study provided by the EU project NESSoS[8]. The scenario concerns managing *Electronic Health Records* (EHRs) in clouds. EHRs contain any information created by health care professionals in the context of the care of a patient. Examples are laboratory reports, X-ray images, and data from monitoring equipment.

Security concerns in this scenario include the confidentiality and integrity of EHRs during communication and storage; data separation of EHRs and other data of the eHealth applications; availability of EHRs; availability of network connection; and data origin authentication. Some of these concerns, like confidentiality and integrity, require authentication mechanisms.

Given these security concerns, the CSA threats that become more relevant are the following: *Insecure Interfaces and APIs (Threat 2)*, because these are essential for security functionalities like authentication; *Malicious Insiders (Threat 3)*, because they could steal EHRs and use them for blackmailing or similar criminal activities. *Shared Technology (Threat 4)* and, specially, *Data Loss & Leakage (Threat 5)*, can lead to a loss of confidentiality of EHRs or data separation. *Account or Service Hijacking (Threat 6)* leads to bypass authentication controls, including those for data origin authentication; *Unknown Risk Profile (Threat 7)* and *Unknown Causes (Threat 8)*[9] can also have a negative effect on all the security concerns.

For this scenario, we consider the following cloud vendors: Amazon, Apple, Microsoft and Google. For space limitations, we lay stakeholders evaluation aside and we focus on evaluating trust in the threat and general dimensions. Next subsections include each step in our methodology.

[8] The NESSoS project: `http://www.nessos-project.eu`

[9] Note that the original CSA Top Threats are just 7, but the CSA documented cloud security incident referenced numerous incidents that cannot be categorized because of a lack of information. This lead us to adding an additional threat.

Trust Factor Quantification and Thresholds Definition Threats quantification is based on a data set from CSA, which mapped 11 491 cloud security incidents to these threats[10].

As explained before, for each trust factor (including the threats), we assign a factor value and a confidence value. For example, in the case of *Threat 1* for Amazon, we assigned factor value 0 and confidence value 2. The rationale, which must also be included as part of the analysis, is that we found three incidents on record and one that had a significant amount of user accounts affected. As another example, for *Security* trust factor in Microsoft, we assigned factor value 3 and confidence value 2. The rationale is that Microsoft considers some certifications (e.g. ISO 27001) and complies with the CSA control matrix and FedRAMP. Applying Definition 1, we obtain the trust interval $[0, 1]$ for the first example, and $[2, 3]$ for the second example[11].

In parallel and based on the security requirements of the scenario, we define minimum trust values for each trust factor. These thresholds, already aggregated in the threat and general dimensions, are presented in Table 4.

Trust Aggregation We aggregate the trust intervals of every factor for a given cloud provider. As an example, consider the following: Apple has trust interval $[0, 2]$ for *Security* and $[0.33, 2.33]$ for transparency. We use the operator in Definition 3 to aggregate these intervals. The resulting interval is $[0.17, 2.17]$. We would now aggregate this trust interval with the one corresponding to *Accountability and Auditing*, and so forth, until we reach a final trust interval in the general dimension. The resulting trust interval in the general dimension for each cloud provider is shown in Table 3.

Table 3. Trust Intervals for Cloud Providers

	Threat 1	**Threat 2**	**Threat 3**	**Threat 4**	**Threat 5**	**Threat 6**	**Threat 7**	**Threat 8**	**General**
Amazon	[0,1]	[0.67,1.67]	[0,3]	[0.33,2.33]	[1.33,2.33]	[0,3]	[0.33,2.33]	[0,1]	[0.34,1.86]
Apple	[0.67,1.67]	[0,1]	[0,0]	[0.33,2.33]	[1.33,2.33]	[0.33,2.33]	[0.67,1.67]	[0.67,2.67]	[0.02, 2.02]
Microsoft	[2,3]	[0.33,2.33]	[1.33,2.33]	[0.67,2.67]	[0.67,1.67]	[0.67,1.67]	[1.33,2.33]	[0,1]	[0.8, 2.25]
Google	[1.33,2.33]	[0,1]	[0.33,2.33]	[1.33,2.33]	[0,1]	[0.33,2.33]	[0.33,2.33]	[0,1]	[0.53, 2.39]

[10] Documented Cloud Security Incidents: `https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/`

[11] The Technical Report shows the whole quantification for one of the considered cloud providers: `http://www.uml4pf.org/publications/trust.pdf`

Table 4. Trust Thresholds

Threat 1	Threat 2	Threat 3	Threat 4	Threat 5	Threat 6	Threat 7	Threat 8	General
[1.0,1.0]	[0.67,2.67]	[0.33,2.33]	[2.0,2.0]	[2.0,2.0]	[0.67,2.67]	[0.33,2.33]	[0.33,2.33]	[0.67,2.67]

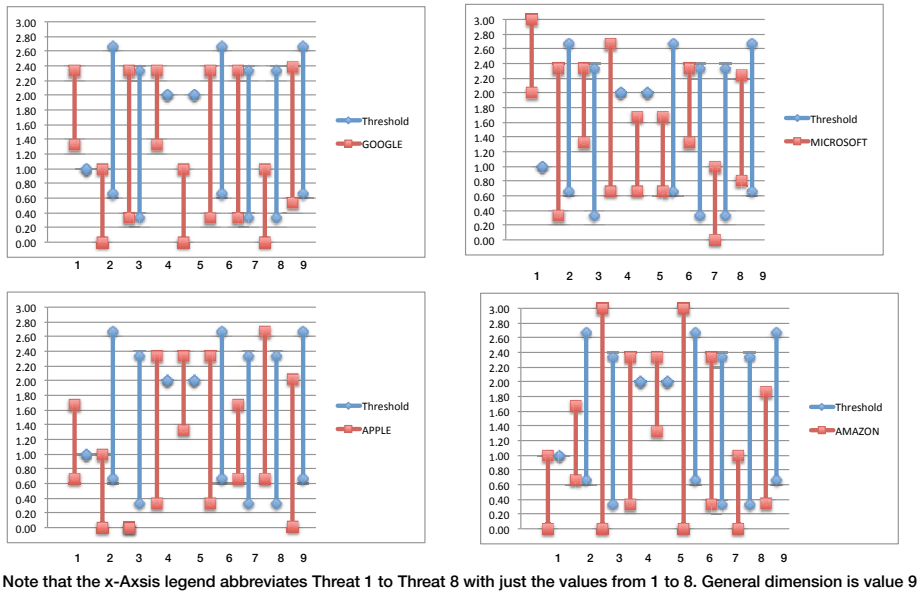

Fig. 2. Contrasting Trust Thresholds and Trust Intervals

We assume that we have no direct previous experience with the providers. Therefore, there is no need to aggregate trust intervals in the threat dimension, which this time only considers information from *3rd party referrals*, in this case, from CSA. Trust intervals for each threat and cloud provider are presented in Table 3. Note that due to space limitations, we laid the stakeholder dimension aside.

Trust Visualization. Figure 2 allows comparing the trust intervals with the trust thresholds[12].

As a conclusion, we see in Figure 2 that no cloud provider upholds all trust thresholds. However, at this point, we can say that Amazon violated "only" the trust thresholds for threats 2 and 8. Google violates the trusts thresholds for threat 5 significantly and threats 2, 4, and 6 just slightly. Microsoft has significant trust threshold violations for threats 4 and 5, while threats 2, 4 and 5 are just violated. Apple has significant misses for threats 2 and 3, while threats 6, 7 and 8 have just minor violations of the threshold. The cloud provider that

[12] Other interesting figures, including a comparison of cloud providers, are depicted in the Technical Report: `http://www.uml4pf.org/publications/trust.pdf`.

best meets the trust expectations in the general dimension is Microsoft, followed by Google. To sum up, our analysis would lead us to either not pursue any cloud provider for our scenario at this time and repeat the analysis later, or to confront the cloud providers with the results and ask for a detailed justifications for their security mechanisms, especially regarding threats 2 and 8. Once the decision maker has more information, he may improve the trust and confidence values.

5 Discussion

There are many trust and reputation engines in the literature [26]. Given that this methodology is aimed at decision makers, who do not necessarily have much technical background, a requirement for our trust engine was its simplicity. As explained in Section 3, the engine that we present in this work uses trust intervals to represent trust information. There are other engines that are easier to use, such as summation or average engines. However, they present two main problems. First, they usually require weighting the attributes, and selecting weights is difficult. Second, they lack the capability to represent uncertainty, which is a concept highly coupled to the notion of trust. We believe that trust intervals present a good trade-off between simplicity and expressiveness.

Best practices in risk assessment indicate that practitioners should set an even number of choices since users tend to choose the middle value in odd numbered scales [27]. This is why we quantify each trust factor with 4 possible values (i.e. from 0 to 3). We think that 2 would give too few flexibility, whereas more than 4 would be confusing.

A disadvantage of our methodology is that it relies on data that in many cases may not be accessible or available. Cloud providers may be reluctant to provide certain information and it might not be straightforward to gather knowledge about the stakeholders of a cloud provider.

Another source of imprecision is subjectivity. By definition, trust is subjective and therefore some of the information that the methodology requires may have a subjectivity bias. The results of the trust evaluation may not be completely accurate, but we advocate that even minimal or partially subjective information is better than blind decision-making. In order to avoid strong subjectivity bias, it is important to state the rationale for each factor quantification.

Subjectivity draws a line between trust and trustworthiness. Having a trustworthiness value would help in determining trust. Whereas trust usually depends on subjective information and may change among trustors, trustworthiness is an objective measure of many different qualities. The ideal situation occurs when trust in a trustee matches the trustworthiness of that trustee [28]. This is the reason why we claim that we are evaluating trust and not trustworthiness.

6 Conclusion and Future Work

We have proposed a methodology that allows IT decision makers to evaluate their trust in cloud providers. We have applied this methodology to an eHealth

scenario, where an organization (e.g. a hospital) is planning to outsource the management and storage of EHRs to the Cloud.

In order to perform the evaluation, we have chosen four real cloud providers: Amazon, Apple, Microsoft and Google. We have retrieved information from two main sources: the Cloud Security Alliance and the providers' web pages. The former is a valuable source of information about security incidents, which is indispensable for evaluating trust in the threat dimension. The latter allowed us to determine more general information about the providers, such as their compliance to security or privacy standards. However, we noticed that in general it is hard to find information about cloud providers. Often we had to browse through several sub-sites in order to find meaningful information. Due to these issues, our analysis is most likely done on incomplete information. It is also important to point out that some factors are susceptible to subjective evaluation and that we have not considered the stakeholders dimension or direct experience information.

As future work, we plan to study how to evaluate a cloud provider's reputation, which can provide a valuable input for trust evaluation. We also intend to retrieve information about cloud stakeholders in order to perform a comprehensive empirical study. We would like to study the impact of small changes to different trust factors in the final results. Finally, we plan to provide tool support for the proposed methodology.

References

1. Neovise Research Report: Use of Public, Private and Hybrid Cloud Computing (2013)
2. Martorelli, W., Andrews, C., Mauro, S.P.: Cloud Computing's Impact on Outsourcing Contracts (January 2012)
3. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. Working Paper of the National Institute of Standards and Technology (NIST) (2009)
4. Ponemon Institute Research Report: Security of Cloud Computing Users Study. Technical report, Ponemon Institute, sponsored by CA Technologies (March 2013)
5. Yan, Z., Holtmanns, S.: Trust Modeling and Management: from Social Trust to Digital Trust. Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions (January 2008)
6. Griffiths, N.: A Fuzzy Approach to Reasoning with Trust, Distrust and Insufficient Trust. In: Klusch, M., Rovatsos, M., Payne, T.R. (eds.) CIA 2006. LNCS (LNAI), vol. 4149, pp. 360–374. Springer, Heidelberg (2006)
7. Bubak, M., Kasztelnik, M., Malawski, M., Meizner, J., Nowakowski, P., Varma, S.: Evaluation of Cloud Providers for VPH Applications. In: CCGrid2013 - 13th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (May 2013)
8. Gao, J., Pattabhiraman, P., Bai, X., Tsai, W.T.: SaaS performance and scalability evaluation in clouds. In: 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, pp. 61–71 (2011)

9. Nuñez, D., Fernandez-Gago, C., Pearson, S., Felici, M.: A metamodel for measuring accountability attributes in the cloud. In: 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), Bristol, UK. IEEE (2013) (in press)
10. Pauley, W.: Cloud provider transparency: An empirical evaluation. IEEE Security & Privacy 8(6), 32–39 (2010)
11. Rashidi, A., Movahhedinia, N.: A Model for User Trust in Cloud Computing. International Journal on Cloud Computing: Services and Architecture (IJCCSA) 2(2) (2012)
12. Ko, R., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., Lee, B.S.: TrustCloud: A Framework for Accountability and Trust in Cloud Computing. In: 2011 IEEE World Congress on Services (SERVICES), pp. 584–588 (July 2011)
13. Sarwar, A., Khan, M.: A Review of Trust Aspects in Cloud Computing Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER) 2(2), 116–122 (2013)
14. Ahmad, S., Bashir Ahmad, S.M.S., Khattak, R.M.: Trust Model: Cloud's Provider and Cloud's User. International Journal of Advanced Science and Technology 44 (2012)
15. Chakraborty, S., Roy, K.: An SLA-based Framework for Estimating Trustworthiness of a Cloud. In: International Joint Conference of IEEE TrustCom/IEEE ICESS/FCST, pp. 937–942 (2012)
16. Manuel, P.: A trust model of cloud computing based on Quality of Service. Annals of Operations Research, 1–12 (2013)
17. Pavlidis, M., Mouratidis, H., Kalloniatis, C., Islam, S., Gritzalis, S.: Trustworthy selection of cloud providers based on security and privacy requirements: Justifying trust assumptions. In: Furnell, S., Lambrinoudakis, C., Lopez, J. (eds.) TrustBus 2013. LNCS, vol. 8058, pp. 185–198. Springer, Heidelberg (2013)
18. M, S., L.j, V., Sangeeta, K., Patra, G.K.: Estimating Trust Value for Cloud Service Providers using Fuzzy Logic. International Journal of Computer Applications 48(19), 28–34 (2012)
19. Garg, S.K., Versteeg, S., Buyya, R.: SMICloud: A Framework for Comparing and Ranking Cloud Services. In: Proceedings of the, Fourth IEEE International Conference on Utility and Cloud Computing, UCC 2011, pp. 210–218. IEEE Computer Society, Washington, DC (2011)
20. Qu, L., Wang, Y., Orgun, M.A.: Cloud Service Selection Based on the Aggregation of User Feedback and Quantitative Performance Assessment. In: Proceedings of the IEEE International Conference on Services Computing, SCC 2013, pp. 152–159. IEEE Computer Society, Washington, DC (2013)
21. Beckers, K., Faßbender, S., Heisel, M.: A meta-model approach to the fundamentals for a pattern language for context elicitation. In: Proceedings of the 18th European Conference on Pattern Languages of Programs (Europlop). ACM (2013) (accepted for publication)
22. Beckers, K., Küster, J.-C., Faßbender, S., Schmidt, H.: Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), pp. 327–333. IEEE Computer Society (2011)

23. Beckers, K., Côté, I., Faßbender, S., Heisel, M., Hofbauer, S.: A pattern-based method for establishing a cloud-specific information security management system. Requirements Engineering, 1–53 (2013)
24. Greenspan, S.J., Mylopoulos, J., Borgida, A.: Capturing more world knowledge in the requirements specification. In: Proceedings of the 6th International Conference on Software Engineering, ICSE 1982, pp. 225–234. IEEE Computer Society Press, Los Alamitos (1982)
25. Shakeri, H., Bafghi, G., A, S, Yazdi, H.: Computing Trust Resultant using Intervals. In: IEEE (ed.): 8th International ISC Conference on Information Security and Cryptology (ISCISC) 15–20 (2011)
26. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision Support Systems 43(2), 618–644 (2007)
27. Ontario: Standards of Sound Business and Financial Practices. Enterprise Risk Management: Application Guide. Technical report, Deposit Insurance Corporation of Ontario (2011)
28. Pavlidis, M.: Designing for trust. In: Proceedings of the CAiSE Doctoral Consortium 2011. CEUR-WS, vol. 731 (June 2011)