AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security

Ahmed Taha*, Ruben Trapero*, Jesus Luna§* and Neeraj Suri*
*TU Darmstadt, Germany §CSA (Europe), United Kingdom
Email:{ataha, rtrapero, jluna, suri}@deeds.informatik.tu-darmstadt.de, jluna@cloudsecurityalliance.org

***Abstract*—While Cloud usage increasingly involves security considerations, there is still a conspicuous lack of techniques for users to assess/ensure that the security level advertised by the Cloud Service Provider (CSP) is actually delivered. Recent efforts have proposed extending existing Cloud Service Level Agreements (SLAs) to the security domain, by creating Security SLAs (SecLAs) along with attempts to quantify and reason about the security assurance provided by CSPs. However, both technical and usability issues limit their adoption in practice.**

In this paper we introduce a new technique for conducting quantitative and qualitative analysis of the security level provided by CSPs. Our methodology significantly improves upon contemporary security assessment approaches by creating a novel decision making technique based on the Analytic Hierarchy Process (AHP) that allows the comparison and benchmarking of the security provided by a CSP based on its SecLA. Furthermore, our technique improves security requirements specifications by introducing a flexible and simple methodology that allows users to identify their specific security needs. The proposed technique is demonstrated with real-world CSP data obtained from the Cloud Security Alliance's Security, Trust and Assurance Registry.

I. Introduction

The paucity of comprehensive approaches to specify, assess and quantitatively reason about security in Cloud systems is a major impediment that customers encounter when they decide to migrate their key applications to the Cloud. On one hand, the Cloud Service Providers (CSPs) are trying to convince users to trust the security of their provided services. On the other hand, users should themselves be able to assess and validate the security claims from the CSPs and then select the best provider that suits their security requirements.

In order to meaningfully model and assess CSP security, the European Network and Information Security Agency (ENISA) and the Cloud Security Alliance (CSA) have targeted the specification of security in Cloud services in the form of Service Level Agreements (termed as Security Level Agreements or SecLA [1]). Subsequently, CSA has designed a self-assessment questionnaire framework to define the security information contained in a SecLA: the Consensus Assessments Initiative Questionnaire (CAIQ) [2] where CAIQ currently contains more than 200 security relevant questions. Multiple CSPs have filled their answers to the CAIQ and published them in the STAR repository (Security, Trust and Assurance Registry) [3]. With the published CAIQ, users are able to browse the claimed information that represents capabilities of the Cloud providers regarding their security controls and policies. However, this is still mostly free-text level qualitative information that is hard to be quantitatively parsed by the user.

While the state of the art predominantly focuses on the methodologies to build and represent Cloud SecLAs [4]–[6], the techniques to quantitatively reason about Cloud SecLA are conspicuous by their paucity. Having user friendly approaches (including automation) to specify desired security attributes and flexible comparison techniques are needed to effectively rank the level of security provided by several CSPs and especially to compare them for matching with respect to the users' security requirements.

A. Contributions

This paper aims to solve these aforementioned issues by developing quantitatively reasoning approaches about Cloud SecLAs. Thus, we propose a framework that allows to *(i)* automatically compare, benchmark and rank the security level provided by two or more CSPs, *(ii)* provide a composite quantitative and qualitative SecLA assessment technique based on Analytic Hierarchy process (AHP) depending on Cloud user security requirements and, *(iii)* allow users to specify their security requirements at varied levels of the security provisions, which would help to remove the need to specify every single security requirement (more than 200 in case of CAIQ). Finally, *(iv)* we introduce a system validation tool *(SecCloudcmp)* that implements the proposed framework. This tool is publicly available[1] and allows Cloud users to choose the most suitable CSPs by assessing the security of Cloud SecLAs.

In this paper we also perform the initial validation of the proposed framework by evaluating a real world case study based on the Cloud SecLAs found on the CSA's public STAR repository.

[1] http://cloud.quant-security.org

The paper is organized as follows. Section II introduces the basic concepts and Section III outlines related work. Section IV describes the proposed framework and Section V presents a case study to validate the proposed framework.

II. Basic Concepts

We introduce the concepts used in the paper covering Cloud SecLAs, security metrics and security quantification. A *Service Level Agreement (SLA)* represents a commitment between a service provider and a user which *(a)* describes the provided services, *(b)* documents the service level objectives to fulfill, and *(c)* includes the responsibilities/contractual-penalties of the service provider and user with respect to the unfulfillment of the provided services. Analogously, security requirements can be specified as dedicated SLAs, termed as *SecLAs*. The notion of SecLAs forces a stakeholder (CSP or user) to explicitly specify security attributes thus providing transparency across user requirements and the provisioning claimed by the CSPs. While SecLAs aim to provide service based assurance, it is clear that SecLAs are not intended to replace assurance mechanisms for security policy enforcement [4]. Cloud SecLAs usually models CSPs security at the service level which results in a collection of security statements that define the services the CSP agrees to provide, i.e., security *Service Level Objectives (SLOs)*.

Despite the advantages of Cloud SecLAs, usually these documents are typically informally specified in text form hence limiting either quantitative or automated reasoning about them. It would be helpful to have a user centric mechanism to quantitatively evaluate and objectively rank SecLAs with respect to a predefined user requirement. In order to enforce a SecLA, the definition and usage of appropriate metrics and their underlying measures form an essential aspect of the Cloud SecLA. In general a *metric* is a measure for quantitatively assessing, controlling or selecting a process or a service. Metrics help in the measurement of Cloud security service objectives by defining security parameters, formulas and measurement rules which facilitate assessment and decision making. To this end, the process of *quantifying* textual based security requirements to machine friendly values is essential for metrics to provide a meaningful *quantitative* assessment of security.

III. Related Work

Multiple approaches are emerging to assess CSP functionality and security. In [7], the authors proposed a framework to compare different Cloud providers accross performance indicators. In [8], an AHP based ranking technique that utilizes performance data to measure various QoS attributes and evaluates the relative ranking of Cloud providers was proposed. In [9], a framework of critical characteristics and measures that enable comparison of Cloud services is presented.

While multiple Cloud security approaches have focused on specifying security aspects in SecLAs, fewer efforts exist for specifying and quantifying security attributes in SecLAs exists. Security requirements have been treated by Casola et al. [10], who proposed a methodology to evaluate security SLAs for web services. Chaves et al. [5] explore security in SLAs applied on a monitoring and controlling architecture. In [11] and [12], the authors propose a technique to aggregate security metrics from a web services SecLAs. However, differing from our research, the authors did not propose any techniques to assess SecLAs or empirically validate the proposed metrics.

In [6] the authors presented a method for managing the SecLA lifecycle in the context of federated Cloud services. However, they did not further elaborate the techniques needed to conduct benchmarking. In [13] the authors propose the notion of evaluating Cloud SecLAs, by introducing a metric to benchmark the security of a CSP based on categories. However, the resulting security categorization is purely qualitative. In [14], Luna et al. presented a security metrics framework for Cloud provider's security assessment and in [1] a methodology to quantitatively benchmark CSPs SecLAs with respect to user defined requirements. Both works are based on the Reference Evaluation Methodology (REM) [15], which formally allows to compose security levels of different Cloud providers but only in the low level nodes in contrast to our multi-level methodology. Overall our approach allows users to (a) specify their priorities at different levels of SecLA granularity, (b) perform a bottom-up aggregation of SLOs to result in an overall assessment across all the security levels and (c) allowing both basic and expert users to manifest their security requirements according to their expertise and specific needs.

Research efforts also include security management systems, such as policy-based security management [16]. Martinelli et al. [17] presented the problem of enforcing a security policy through its qualitative aspect. Most of these approaches focus on the security capturing and enforcement phases rather than the feedback and improvement phases.

To the best of our knowledge this broadly reflects the state of the art for security assessment of CSPs. In particular we refer to related works that utilize the notion of SecLAs and aim to empirically validate their security metrics with real CSP data.

IV. Security Assessment Methodology

The quantitative security level assessment of Cloud providers (for their match to the user requirements) is the primary objective of the proposed framework

developed in this section. Using this assessment the CSPs are ranked (as per their SecLAs) for the best match to the user requirements. Our proposed methodology computes quantitative values for various CSPs based on their security levels measured according to user defined security requirements and priorities. As discussed before, SecLAs contains multiple SLOs each with multiple attributes which make the assessment process (of Multiple Criteria Decision Making (MCDM) [18]) a highly complex task necessitating the use of hierarchically structured approaches. The challenge is not only how to quantify different SLOs in SecLAs, but also how to aggregate them in a meaningful metric. To solve these issues, we propose a ranking mechanism based on Analytic Hierarchy Process (AHP) [19] which is one of the most widely used mechanism for solving MCDM problems.

The advantages of AHP over contemporary multi-criteria methods are its ability to handle composite qualitative and quantitative attributes, along with its flexibility and ability to identify inconsistencies across requirements [20]. AHP allows the use of qualitative as well as quantitative criteria when evaluating alternatives by using a pairwise comparisons of decision criteria. The pairwise results are organized into a hierarchical structure with relative weights assigned to each criterion. These comparisons and weightings of the factor are the crucial elements that are utilized over SecLA's to drive our CSP evaluations.

As an overview of our approach, the SecLA assessment and the ranking of CSPs is performed in progressive stages as shown in Figure 1. In Stage (A), we define the CSP SecLA as well as the user SecLA requirements. In (B) we address the security level quantification that is associated with each SecLA. This is done by defining a measurement model for the different types of attributes, and then specifying metrics for each attribute. Finally, in Stage (C), the data from the preceding stage serves as input to the ranking algorithm based on AHP. We detail each of these framework stages in the subsequent sections.

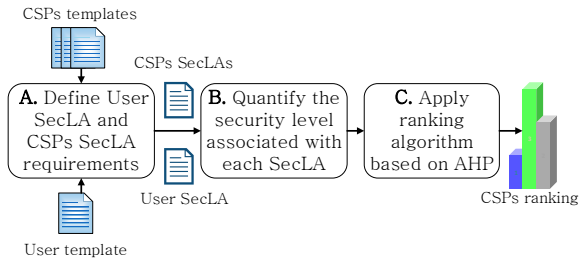

Fig. 1: Stages of the proposed framework.

Stage A. Define user and CSPs SecLAs requirements

Over this stage, the users create their set of security requirements based on the same SecLA template as used by the CSPs to specify their security provisions. In practice, these SecLA templates are created by multi-disciplinary working groups [21]. In these groups, usually industry and academia design the SecLAs contents (i.e., the security and privacy requirements along with their associated metrics) and discuss their technical, operational and legal issues [1]. The user defined requirements are distinctive elements of Cloud SecLA, where all the security SLOs are weighted in order to represent their relative importance from the user's perspective. The output of this stage will be one user SecLA and, one or more CSP SecLAs.

Stage B. Security quantification

In order to compare Cloud providers with the proposed technique, the measurement model for different security SLOs should be defined. In this section, we propose different comparison metrics for different types of requirements. For the rest of the paper the terms shown in Table I are used. The security SLOs can be

TABLE I: Used terms definitions

Term	Definition
k	security SLO.
C_i	Cloud provider i, such that $i \in \{1, \ldots, n\}$, where n is the number of Cloud providers.
$V_{i,k}$	service level objective value of k provided by C_i.
$C_{i,k}$	C_i provides k with value $V_{i,k}$.
U	Cloud user.
$V_{u,k}$	user required value of k.
W	relative rank ratio.
C_1/C_2	indicates the relative rank W of C_1 over C_2, regarding k. Or relative rank $1/W$ of C_2 over C_1, regarding k.
C_2/C_1	indicates the relative rank W of C_2 over C_1, regarding k. Or relative rank $1/W$ of C_1 over C_2, regarding k.
$C_{i,k}/U$	indicates the relative rank of C_i over U, which specifies if C_i satisfies U requirements, with respect to k.

boolean or numerical as described:

1) Boolean: As in CAIQ, CSPs have to answer to the security SLOs related questions with yes or no, representing whether each CSP will offer the required services or not. yes and no are defined as boolean $true$ and $false$ or 1 and 0, respectively. The relationships across the CSPs (C) with respect to security SLO value (V) can be represented as a ratio:

$$\frac{C_1}{C_2} = \frac{V_1}{V_2} \tag{1}$$

Thus,

$$\begin{aligned} \frac{C_1}{C_2} &= 1 \quad if \quad (V_1 = 1 \wedge V_2 = 1) \vee (V_1 = 1 \wedge V_2 = 0) \\ &= 0 \quad if \quad (V_1 = 0 \wedge V_2 = 0) \vee (V_1 = 0 \wedge V_2 = 1) \end{aligned}$$

i.e. Assume two CSPs, C_1 and C_2, with values V_1 and V_2 for security SLO k respectively, such that: $V_1 = 1 \equiv yes$, $V_2 = 0 \equiv no$ and assume k is required by the user U, thus $V_u = 1 \equiv yes$. The pairwise comparison relation between C_1, U is defined as: $C_1/U = 1$. Therefore, C_1 is satisfying the user requirement. On the other hand, $C_2/U = 0$. Thus, C_2 is not fulfilling the user requirement.

2) Numerical: Assume encryption key size defined as k and specified by {64, 128, 256, 512, 1024, 2048}, such that 64 < 128 < 256 < 512 < 1028 < 2048, which is defined as $level_1, level_2, level_3, level_4, level_5, level_6$. The security levels are modeled as {1,2,3,4,5,6} respectively, such that 1 < 2 < 3 < 4 < 5 < 6. The relationships across the CSPs (C) with respect to security SLO value (V) can be represented as a ratio:

$$\frac{C_1}{C_2} = \frac{V_1}{V_2} \tag{2}$$

Thus,

$$\begin{aligned} \frac{C_1}{C_2} &= 1 \qquad if \quad V_1 \equiv V_2 \\ &= W \qquad if \quad V_1 > V_2 \\ &= \frac{1}{W} \qquad if \quad V_1 < V_2 \end{aligned}$$

It can be of two types, higher is better (i.e., encryption key size) or lower is better (i.e., Backup periodicity). If higher is better then V_1/V_2 is the value of C_1/C_2 and if lower is better then V_2/V_1 is the value of C_1/C_2. We assume that if a provider is offering a specific level of security then we can consider that it is also able to provide all the lower levels.

Stage C. Ranking using AHP

The proposed AHP-based methodology for CSP rankings consists of four main phases: (1) hierarchy structure (2) weights assignment (3) pairwise comparison and (4) attributes aggregation to give the overall rank calculation. In the following subsections, we describe the four steps used in modeling the ranking problem.

1) Hierarchy structure: The SecLAs are constructed as a hierarchical structure which also defines the structure of Cloud SecLAs from the highest to the lowest level as shown in the Figure 2. The data used in the figure is based on specifications defined in CAIQ. The current CAIQ contains the following domains: Compliance (CO), Data governance (DG), Information Security (IS) and others. Each domain consists of one or more control groups that are composed of one or more attributes. Given these CAIQ properties, it is possible to create SecLAs with the features required by the evaluation and ranking methodology presented.

The first layer of the hierarchy structure, as shown in Figure 2, is the *Root level* which defines the main goal and aims to find the overall rank. The second layer is the *Domain level* or *High level* which presents the hierarchies of security SLOs. The third layer defines the *Control groups*, which are decomposition's of the main domains specified in the Domain level. The last layer is the Consensus Assessment Questions contained in the Control groups, which are specified as values of security attributes. This level is termed as the *Attributes level* or *Low level*.

2) Weights Assignment: In order to compare two CSPs security SLOs, the user priorities of each security SLO should be assigned as weights, to take into account their relative importance as shown in Figure 2. To address this issue we consider two types of weights:

- *User assign qualitative labels*. Users can assign desired weights to each SLO to indicate their priorities (Extremely-Important (EI), Medium-Important (MI), Not-Required (NR)). These labels are transformed to a quantitative metrics and assigned as normalized numbers to satisfy the AHP requirements.
  Extremely-Important (EI) denotes that all security SLOs are necessary requirements for the user. Not-Required (NR) indicates that the security SLOs are not required by the user. Medium-Important (MI) specifies users non-mandatory requirements where users can accept varied values specifying several degrees of importance that will depend on the considered scale.
- *Using AHP's standard method.* The user can assign weights to each of the security SLOs using values in some scale as defined in the AHP method from 1 to 9 to indicate the importance of one attribute over another (such that 9 indicates extremely more important and 1 equal importance). Users express their preferences for each attribute relative to other attributes.

The proposed framework allows the users to assign qualitative or quantitative or both weights at varied levels of the hierarchical specification.

3) Pairwise comparison: The process of modeling values to a quantitative meaningful metric denoting the specified security level is not straightforward as attributes can have various types of values. Therefore, we propose a relative ranking model defining the most important requirements used and their quantitative metrics specified in Table I. The ranking model is based on pairwise comparison matrix of security attributes provided by different CSPs and required by users. Using a Comparison Matrix (CM) for each CSP, we obtain a one to one comparison of each CSP for a particular attribute where $C_{1,k}/C_{2,k}$ indicates the relative rank of C_1 over C_2 as indicated in Table I. This will result in a one to one comparison matrix of size n x n if there

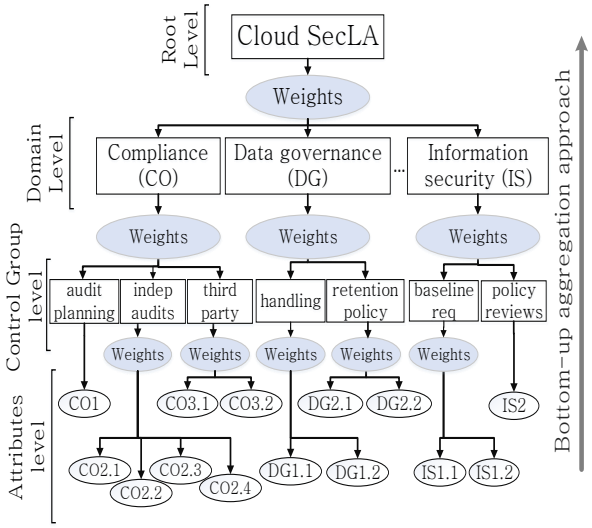

Fig. 2: Cloud SecLA AHP hierarchy based on STAR repository.

are a total of n CSPs such that:

$$CM = \begin{array}{c} \\ C_1 \\ C_2 \\ \vdots \\ C_n \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \dots & C_n \end{array} \\ \begin{pmatrix} C_1/C_1 & C_1/C_2 & \dots & C_1/C_n \\ C_2/C_1 & C_2/C_2 & \dots & C_2/C_n \\ \vdots & \vdots & \ddots & \vdots \\ C_n/C_1 & C_n/C_2 & \dots & C_n/C_n \end{pmatrix} \end{array} \quad (3)$$

The relative ranking of all the Cloud providers for a particular SLO is given by the eigenvector of the comparison matrix. This eigenvector is called Priority Vector (PV) which indicates a numerical ranking of the providers that specifies an order of preference among them as indicated by the ratios of the numerical values.

4) Attributes Aggregation: In the final phase, we follow up a bottom-up aggregation to give the security levels overall assessment and final ranking of CSPs. To achieve that, the priority vector of each attribute is aggregated with their relative weights assigned in Phase 2. This aggregation process is repeated for all the attributes in the hierarchy with their relative weights.

$$PV_{aggregated} = (PV_1 \quad \dots \quad PV_n)\,(w_i) \quad (4)$$

where w_i is user assigned weights of criteria i.
At this stage we have been able to map the user's and CSPs' SecLAs as a data structure where the user's priorities and CSPs' SLOs are represented as (a) weighed nodes and (b) with hierarchical relationships across the security SLOs. This framework now forms the basis of conducting quantitative comparisons/rankings across the user and CSP requirements as detailed over actual CSP case studies in Section V.

V. Case Study: Ranking CSPs based on STAR repository values

As an initial effort to validate the proposed framework, we applied it to the CSP data stored in the STAR repository. Currently, STAR contains Cloud SecLAs in the form of questionnaire (CAIQ [2]) reports, which provide industry accepted guidelines to document what security controls exist in Cloud provisions. We applied the proposed framework to three different Cloud SecLAs, that were chosen to cover all possible conditions for each attribute -over/under provisioning or satisfying- user requirements. Three CSPs' data stored in the STAR repository Microsoft365 (C_1), Mimecast (C_2) and Solutionary (C_3) [3] were evaluated. These providers have published their profiles by answering yes or no questions, consisting of CAIQ properties as shown in Table II. In this case study, we only considered qualitative weights to indicate user's relative priorities such that, *EI* and *NR* indicate a relative value 1 and 0 respectively. *MI* can be considered any intermediate values between 1 and 0. In this analysis *MI* indicate a relative rank value 0.5.
For the analysis shown in this section, three use case studies were evaluated to present different combinations representing three different user's requirements as shown in Table II.
Case I. User gives a detailed specification, by specifying Low level (Attribute level) requirements.
Case II. User denotes qualitative weights for Control group level SLOs and for other SLOs in the Domain level. Simultaneously, users specify requirements at the Attribute level.
Case III. Qualitative weights are only assigned at the Domain level.
To the best of our knowledge, this is the first study that assesses security objectives at different levels of SecLA granularity.

A. Analytical results

Prior to the calculation of relative ranking matrix using (3), the following steps should be considered. (i) As specified earlier, user assigned weights are normalized as to comply with AHP requirements. (ii) User undefined weights are by default specified as *Medium-Important*. (iii) All SLOs and attributes specified by the user as *Not-Required* and as boolean no, are assigned weight 0. (iv) All SLOs and attributes specified by the user as *Extremely-Important* and as boolean yes, are assigned weight 1. The ranking computation process for Cloud security SLOs defined in Table II is explained step by step in the following subsection.

1) Case I: For the Compliance domain of Cloud SecLA, there are three security SLOs which are further divided to attributes. Equation (1) is used to define *CO1*

TABLE II: Case Study

STAR Repository UseCases			CSP_1	CSP_2	CSP_3	$User$		
Domain level	Control group level	Attributes	C_1	C_2	C_3	Case I	Case II	Case III
Compliance CO	audit planing CO1	CO1	no	yes	yes	yes	EI	EI
	independent audits CO2	CO2.1	yes	yes	yes	yes	EI	
		CO2.2	yes	yes	yes	yes		
		CO2.3	yes	yes	yes	yes		
		CO2.4	yes	yes	yes	yes		
	third party audits CO3	CO3.1	no	no	yes	no	NR	
		CO3.2	yes	yes	yes	yes		
Data governance DG	handling/security DG1	DG1.1	yes	yes	yes	yes	EI	EI
		DG1.2	yes	yes	yes	yes		
	retention policy DG2	DG2.1	yes	yes	yes	yes		
		DG2.2	yes	yes	yes	yes		
Information security IS	baseline requirement IS1	IS1.1	yes	yes	yes	yes	no	MI
		IS1.2	yes	yes	yes	yes	no	
	policy reviews IS2	IS2	yes	no	yes	no	yes	

attribute pairwise relation as for example:

$$C_1/C_2 = 0 \quad C_2/C_3 = 1 \quad C_3/C_1 = 1 \quad U/C_2 = 1$$

Thus, the CM of *CO1* attribute as specified in (3) is:

$$CM_{CO1} = \begin{array}{c} \\ C_1 \\ C_2 \\ C_3 \\ U \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & C_3 & U \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

The relative ranking of the Cloud providers for *CO1* is given by the priority vector for CM_{CO1} (PV_{CO1}). That reflects which of the CSPs provide the *CO1* security SLO relative to other CSPs and to the user requirements.

$$PV_{CO1} = \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & C_3 & U \end{array} \\ \begin{pmatrix} 0 & 0.3333 & 0.3333 & 0.3333 \end{pmatrix} \end{array}$$

Which means that C_2 and C_3 equally satisfy U's requirement. However, C_1 does not fulfill that requirement.

Independent audits priority vector (PV_{CO_2}) is calculated the same way, such that *CO2.1, CO2.2, CO2.3* and *CO2.4* priority vectors are aggregated. Similarly, we premeditate PV_{CO3} where CO3.1 and CO3.2 are specified by the user as no and yes respectively. Therefore, $PV_{CO3.1}$ and $PV_{CO3.2}$ are aggregated with user defined normalized weights (w_{CO3}) such that:

$$w_{CO3} = \begin{array}{c} \begin{array}{cc} CO3.1 & CO3.2 \end{array} \\ \begin{pmatrix} 0 & 1 \end{pmatrix} \end{array}$$

Therefore, PV_{CO3} is:

$$PV_{CO3} = \begin{array}{c} \\ C_1 \\ C_2 \\ C_3 \\ U \end{array} \begin{array}{c} \begin{array}{cc} PV_{CO3.1} & PV_{CO3.2} \end{array} \\ \begin{pmatrix} 0 & 0.25 \\ 0 & 0.25 \\ 1 & 0.25 \\ 0 & 0.25 \end{pmatrix} \end{array} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The three Compliance provisions *CO1, CO2, CO3* priority vectors are aggregated to have the overall compliance priority vector PV_{CO}. In a similar way the information security and data governance priority vectors are considered.

Finally, the priority vectors of Compliance, Data governance and Information security are aggregated to obtain the total SecLA priority vector:

$$PV_{total} = \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & C_3 & U \end{array} \\ \begin{pmatrix} 0.22 & 0.2593 & 0.2593 & 0.2593 \end{pmatrix} \end{array}$$

Consequently, C_2 and C_3 fulfill the user's requirements, as shown in Figure 3.

The proposed framework allows users to visualize the differences between various Cloud providers' security SLOs with respect to user requirements. C_1 under-provisions *CO1* and over-provisions IS2. Although, both C_2 and C_3 fulfill user's requirements, C_3 over-provisions *CO3* and *IS2*. As a result, C_2 is the best matching provider according to user's requirements followed by C_3. Due to space limitations we present in Figure 3 the overall rank of CSPs and not each security SLO, for different user requirements cases.

2) Case II: We assume the user denoted audit planning and independent audits as *Extremely-Important* and *Not-Required* for third party. *Extremely-Important* for Data governance, and specified low level requirements for Information security as shown Table II.

Since audit planning and independent audits are assigned *EI*, the respective weight is set to 1. On the other hand, third party is denoted *NR* by the user where the respective weight is set to 0. Therefore, PV_{CO1}, PV_{CO2} and PV_{CO3} are aggregated with user defined normalized weights (w_{CO}) such that:

$$w_{CO} = \begin{array}{c} \begin{array}{ccc} CO1 & CO2 & CO3 \end{array} \\ \begin{pmatrix} 0.5 & 0.5 & 0 \end{pmatrix} \end{array}$$

$$PV_{CO} = (0.125 \quad 0.2917 \quad 0.2917 \quad 0.2917)$$

This implies that C_1 does not fulfill U Compliance SLO and both C_2 and C_3 equally satisfy that requirement.

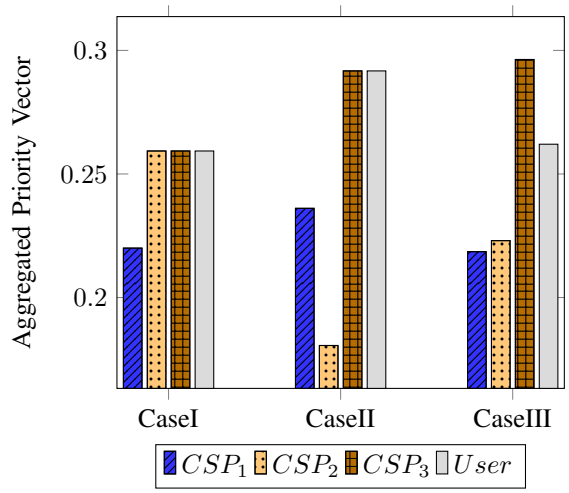

Fig. 3: Different CSPs comparison with respect to the user requirements.

However, C_3 over-provisions *CO3.2*. For data governance, the user specified *EI* which is assigned as 1 for all security SLOs. Similarly, as Case I Information security is evaluated such that:

$$PV_{IS} = (0.3333 \quad 0 \quad 0.3333 \quad 0.3333)$$

Subsequently, PV_{CO}, PV_{DG} and PV_{IS} are aggregated to obtain the total SecLA priority vector:

$$PV_{total} = (0.2361 \quad 0.1806 \quad 0.2917 \quad 0.2917)$$

Therefore, only C_3 satisfies the user needs while both C_1 and C_2 does not fulfill user requirements, as shown in Figure 3. That was expected, as *IS2* and *CO1* were not provided by C_2 and C_1 respectively, and were required by the user. The presented framework can give accurate CSPs ranking even if the low level is not defined. Thus the user can define weights at the higher levels instead of answering multiple low-level questions.

3) Case III: The user allocates *Extremely-Important* for both Compliance and Data governance SLOs in the control group level and *Medium-Important* for Information security. Similarly, as shown in previous cases, the priority vectors of *CO*, *DG*, and *IS* are:

$$PV_{CO} = (0.125 \quad 0.2361 \quad 0.3194 \quad 0.3194)$$

$$PV_{DG} = (0.25 \quad 0.25 \quad 0.25 \quad 0.25)$$

$$PV_{IS} = (0.3428 \quad 0.1429 \quad 0.3428 \quad 0.1714)$$

This means that C_1 and C_3 are satisfying user requirements for *IS*. Therefore, the total priority vector is:

$$PV_{total} = (0.2186 \quad 0.223 \quad 0.2963 \quad 0.2621)$$

Consequently, the ranking has been different from the previous cases, as in this case C_3 has higher rank than the user which is expected as the user assigns weights only at the High (Domain) level and *IS* is assigned *MI*. However, C_2 is not providing *CO3.1* and *IS2*. C_1 is not providing *CO1* and *CO3.1*, which means both C_1 and C_2 do not satisfy user requirements as shown in Figure 3. Therefore, only C_3 fulfill the user needs.

B. Proof-of-concept

Despite the pervasive nature of Cloud technologies and their advocated economic/technological advantages, the migration of applications has been limited, in part, due to the lack of security assurance by the CSP. This lack of assurance, along with the current paucity of techniques to quantify security, often result in users being unable to assess the security of the CSP they are paying for. In order to provide users with a tool to assess the security offered by a CSP, our research contributes to the state of the art with the Cloud security ranking system or simply SecCloudcmp). The first version of SecCloudcmp implements the proposed methodology, taking into consideration CAIQ SLOs used in our analysis. The core of SecCloudcmp consists of the following building blocks:
Provider Input GUI. Step (1): Users are allowed to specify their requirements and assign their priorities at varied levels of hierarchical representation, in order to obtain the required SecLAs. Step (2): After CSPs has uploaded their CAIQ reports to STAR repository the user retrieves it via a load manager.
Comparison GUI. Step (3): Both the user's SecLA (specified in Step 1) and CSPs' SecLAs are manually entered and stored into the SecCloudcmp repository via the *SecLA Management* module. This module is also used to update, delete and modify stored Cloud SecLAs.
Analyzer GUI. Step (4): This module retrieves from the repository the CSPs SecLAs chosen by the user to be assessed with respect to user defined SecLA requirement. Step (5): Two graphs are shown that visualize the differences between various CSPs SecLAs with respect to user's SecLA. One graph shows each security SLO and the other shows the overall rank (aggregation of all SLOs).
Interested parties are encouraged to contact the authors of this paper for requesting access to the SecCloudcmp system as their feedback will be used to provide further empirical validation to the methodology presented in this paper.

VI. Conclusions and Future Work

As different CSPs offer varied security features, it is a challenging task to quantitatively compare the security offered by different CSPs for their match to the security requirements specified by a user. Our AHP-based framework presented in the prior sections was specifically developed to address this need.

Using our framework, we evaluated different CSPs based on various security specifications with respect to user's security requirements. We addressed user different security levels assessment and weights assignment for allowing users to compare security levels offered by CSPs (quantitative and qualitative evaluation). Additionally, we modeled priorities in the form of weights at different levels of SecLA granularity. (e.g., defining requirements just at the higher level of the hierarchy, on every individual security SLO of all the categories or a mix of both approaches). In this context, this work presents the first framework, which allows users to define their requirements and priorities at different SecLAs levels.

We proposed different dimensional metrics specifying various security attributes and designed metrics for each quantifiable security attribute for measuring precisely the security level of each Cloud provider. As a final contribution, our research is validated with a working prototype that implements the proposed methodology. Our research has already considered making SecCloudcmp publicly available in the short term, both to provide further empirical validation of our methodology and empower end users through providing choices of service providers via the use of Cloud SecLAs.

Our proposed framework represents a significant step towards enabling security measurement and the selection of Cloud providers according to user's requirements. By using the techniques presented in this work, users can easily select the best CSP matching their needs. Furthermore, Cloud providers can identify how well they perform with respect to their competitors and therefore improve their services and adapt them to the actual users' security requirements.

In the future, we plan to extend our security assessment methodology to cope with new formats of security controls by adopting fuzzy techniques, which will allow us to also consider not-easy-to-quantify security SLOs. Finally, we also believe that our framework is a valuable starting point to deal with the composition of Cloud services, especially with the creation of Cloud provider rankings.

ACKNOWLEDGMENT

The research was supported by EC FP7 SPECS ♯ 610795, TUD-CASED and TUD EC-SPRIDE.

REFERENCES

[1] J. Luna, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," *Proc. of CCSW*, pp. 103–112, 2012.

[2] "Cloud Security Alliance (CSA), Consensus Assessments Initiative (CAI) Questionnaire," 2012. [Online]. Available: https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/

[3] "Cloud Security Alliance. Security, Trust & Assurance Registry (STAR)," 2011. [Online]. Available: https://cloudsecurityalliance.org/star/

[4] R. Henning, "Security service level agreements: quantifiable security for the enterprise?" *Proc. of New Security Paradigms Workshop*, pp. 54–60, 1999.

[5] S. Chaves, C. Westphall, and F. Lamin, "SLA perspective in security management for cloud computing," *Proc. of Networking and Services (ICNS)*, pp. 212–217, 2010.

[6] K. Bernsmed, M. Jaatun, P. Meland, and A. Undheim, "Security SLAs for federated cloud services," *Proc. of Availability, Reliability and Security*, pp. 202–209, 2011.

[7] A. Li, X. Yang, S. Kandula, and M. Zhang, "Cloudcmp: comparing public cloud providers," *Proc. of SIGCOMM*, pp. 1–14, 2010.

[8] K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Journal of Future Generation Computer Systems*, pp. 1012–1023, 2013.

[9] J. Siegel and J. Perdue, "Cloud services measures for global use: the service measurement index (smi)," *Proc. of SRII Global Conference*, pp. 411–415, 2012.

[10] V. Casola, A. Mazzeo, N. Mazzocca, and M. Rak, "A sla evaluation methodology in service oriented architectures," *In Quality of Protection*, pp. 119–130, 2006.

[11] G. Frankova and A. Yautsiukhin, "Service and protection level agreements for business processes," *Proc. of European Young Researchers Workshop on Service Oriented Computing*, pp. 38–43, 2007.

[12] L. Krautsevich, F. Martinelli, and A. Yautsiukhin, "A general method for assessment of security in complex services," *Towards a Service-Based Internet*, pp. 153–164, 2011.

[13] M. Almorsy, J. Grundy, and A. Ibrahim, "Collaboration-based cloud computing security management framework," *Proc. of CLOUD*, pp. 364–371, 2011.

[14] J. Luna, H. Ghani, D. Germanus, and N. Suri, "A security metrics framework for the cloud," *Proc. of Security and Cryptography*, pp. 245–250, 2011.

[15] V. Casola, R. Preziosi, M. Rak, and L. Troiano, "A reference model for security level evaluation: Policy and fuzzy techniques," *Journal of Universal Computer Science*, pp. 150–174, 2005.

[16] C. Basile, A. Lioy, G. Perez, F. Clemente, and A. Skarmeta, "POSITIF: A policy-based security management system," *Proc. of Policies for Distributed Systems and Networks*, p. 280, 2007.

[17] F. Martinelli, I. Matteucci, and C. Morisset, "From qualitative to quantitative enforcement of security policy," *In Computer Network Security*, pp. 22–35, 2012.

[18] M. Zeleny, *Multiple Criteria Decision Making*. McGraw Hill, 1982.

[19] T. Saaty, "How to make a decision: the analytic hierarchy process," *European Journal of Operational Research*, pp. 9–26, 1990.

[20] R. Ramanathan, "A note on the use of the analytic hierarchy process for environmental impact assessment," *Journal of Environmental Management*, pp. 27–35, 2001.

[21] "Security and Privacy Level Agreements working groups," 2012. [Online]. Available: https://cloudsecurityalliance.org/research/pla/