information

MDPI

Article

Selecting a Secure Cloud Provider—An Empirical Study and Multi Criteria Approach

Sebastian Pape [1,*], Federica Paci [2], Jan Jürjens [3] and Fabio Massacci [4]

1 Faculty of Economics and Business, Goethe University Frankfurt, 60323 Frankfurt, Germany
2 Department of Computer Science, University of Verona, 37134 Verona, Italy; federicamariafrancesca.paci@univr.it
3 Faculty of Computer Science, University of Koblenz, 56070 Koblenz, Germany & Fraunhofer ISST, 44227 Dortmund, Germany; juerjens@uni-koblenz.de
4 Department of Information Sciences and Engineering, University of Trento, 38123 Trento, Italy; fabio.massacci@unitn.it
* Correspondence: sebastian.pape@m-chair.de; Tel.: +49-69-798-34668

Received: 1 April 2020; Accepted: 6 May 2020; Published: 11 May 2020

Abstract: Security has become one of the primary factors that cloud customers consider when they select a cloud provider for migrating their data and applications into the Cloud. To this end, the Cloud Security Alliance (CSA) has provided the Consensus Assessment Questionnaire (CAIQ), which consists of a set of questions that providers should answer to document which security controls their cloud offerings support. In this paper, we adopted an empirical approach to investigate whether the CAIQ facilitates the comparison and ranking of the security offered by competitive cloud providers. We conducted an empirical study to investigate if comparing and ranking the security posture of a cloud provider based on CAIQ's answers is feasible in practice. Since the study revealed that manually comparing and ranking cloud providers based on the CAIQ is too time-consuming, we designed an approach that semi-automates the selection of cloud providers based on CAIQ. The approach uses the providers' answers to the CAIQ to assign a value to the different security capabilities of cloud providers. Tenants have to prioritize their security requirements. With that input, our approach uses an Analytical Hierarchy Process (AHP) to rank the providers' security based on their capabilities and the tenants' requirements. Our implementation shows that this approach is computationally feasible and once the providers' answers to the CAIQ are assessed, they can be used for multiple CSP selections. To the best of our knowledge this is the first approach for cloud provider selection that provides a way to assess the security posture of a cloud provider in practice.

Keywords: cloud service provider; security self-assessment; security assessment; risk assessment

1. Introduction

Cloud computing has become an attractive paradigm for organisations because it enables "*convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort* [1]". However, security concerns related to the outsourcing of data and applications to the cloud have slowed down cloud adoption. In fact, cloud customers are afraid of loosing control over their data and applications and of being exposed to data loss, data compliance and privacy risks. Therefore, when it comes to select a cloud service provider (CSP), cloud customers evaluate CSPs first on security (82%), and data privacy (81%) and then on cost (78%) [2]. This means that a cloud customer will more likely engage with a CSP that shows the best capabilities to fully protect information assets in its cloud service offerings. To identify the "ideal" CSP, a customer has first to assess and compare

the security posture of the CSPs offering similar services. Then, the customer has to select among the candidate CSPs, the one that best meets his security requirements.

Selecting the most secure CSP is not straightforward. When the tenant outsources his services to a CSP, he also delegates to the CSP the implementation of security controls to protect his services. However, since the CSP's main objective is to make profit, it can be assumed that he does not want to invest more than necessary in security. Thus, there is a tension between tenant and CSP on the provision of security. In addition, for security compared to other providers' attributes like cost or performance there are no measurable and precise metrics to quantify it [3]. The consequences are twofold. It is not only hard for the tenant to assess the security of outsourced services, it is also hard for the CSP to demonstrate his security capabilities and thus to negotiate a contract. Thus, even if a CSP puts a lot of effort in security, it will be hard for him to demonstrate it, since malicious CSPs will pretend to do the same. This imbalance of knowledge is known as information asymmetry [4] and together with the cost of cognition to identify a good provider and negotiate a contract [5] has been widely studied in economics.

Furthermore, information gathering on the security of a provider is not easy because there is no standard framework to assess which security controls are supported by a CSP. The usual strategy for the cloud customer is to ask the CSP to answer a set of questions from a proprietary questionnaire and then try to fix the most relevant issues in the service level agreements. But this makes the evaluation process inefficient and costly for the customers and the CSPs.

In this context, the Cloud Security Alliance (CSA) has provided a solution to the assessment of the security posture of CSPs. The CSA published the Consensus Assessments Initiative Questionnaire (CAIQ), which consists of questions that providers should answer to document which security controls exist in their cloud offerings. The answers of CSPs to CAIQ could be used by tenants for selecting the provider the best suit their security needs.

However, there are many CSPs offering the same service—Spamina Inc. lists around 850 CSPs worldwide. While it can be considered acceptable to manually assess and compare the security posture of an handful of providers, this task becomes unfeasible when the number of providers grows up to hundreds. As a consequence, many tenants do not have an elaborated process to select a secure CSP based on security requirement elicitation. Instead, often CSPs are chosen by chance or the tenant just sticks to big CSPs [6]. Therefore, there is the need for an approach that helps cloud customers in comparing and ranking CSPs based on the level of security they offer.

The existing approaches to CSP ranking and selection either do not consider security as a relevant criteria for selection or they do but do not provide a way to assess security in practice. To the best of our knowledge there are no approaches that have used CAIQs to assess and compare the security capabilities of CSPs.

Hence, we investigate in this paper whether manually comparing and ranking CSPs based on CAIQ's answers is feasible in practice. For this aim we have conducted an empirical study that has shown that manually comparing CSPs based on CAIQ is too time consuming. To facilitate the use of CAIQ to compare and ranking CSPs, we have proposed an approach that automates the processing of CAIQ's answers. The approach uses CAIQ's answers to assign a value to the different security capabilities of CSPs and then uses an Analytic Hierarchy Process (AHP) to compare and rank the providers based on those capabilities.

The contribution of this paper is threefold. First, we discuss the issues related to processing CAIQ for provider selection that could hinder its adoption in practice. Second, we refined the security categories used to classify the questions in the CAIQ into a set of categories that can be directly mapped to low-level security requirements. Then, we propose an approach to CSP comparing and ranking that assigns a weight to the security categories based on CAIQ's answers.

To the best of our knowledge, our approach is the only one which provides an effective way to measure the level of security of a provider.

The rest of the paper is structured as follows. Section 2 presents related work and Section 3 discusses the issues related to processing CAIQs. Then, Section 4 presents the design and the results of the experiment and discusses the implications that our results have for security-aware provider selection. Section 5 introduces our approach to comparing and ranking CSPs' security. We evaluate it in Section 6 and Section 7 concludes the paper and outlines future works.

In the in Appendix A we give an illustrative example for the application of our approach.

2. Related Work

The problem of service selection has been widely investigated both in the context of web services and cloud computing. Most of the works based the selection on Quality of Service (QoS) but adopt different techniques to comparing and ranking CSPs such as genetic algorithms [7], ontology mapping [8,9], game theory [10] and multi-criteria decision making [11]. In contrast, only few works considered security as a relevant criteria for the comparison and ranking of CSPs [12–18] but none of them provided a way to assess and measure the security of a CSP in practice.

Sundareswaran et al. [12] proposed an approach to select an optimal CSP based on different features including price, QoS, operating systems and security. In order to select the best CSP they encode the property of the providers and the requirements of the tenant as bit array. Then to identify the candidate providers, they find the service providers whose properties encoding are the k-nearest neighbours of the encoding of the tenant's requirements. However, Sundareswaran et al., do not describe how an overall score for security is computed, while in our approach overall security level of a CSP is computed based on the security controls that the provider declares to support in the CAIQ.

More recently, Ghosh et al. [13] proposed SelCSP, a framework that supports cloud customers in selecting the provider that minimises the security risk related to the outsourcing of their data and application to the CSP. The approach consists in estimating the interaction risk the customer is exposed to if it decides to interact with a CSP. The interaction is computed based on the trustworthiness the customer places in the provider and the competence of the CSP. The trustworthiness is computed based on direct and indirect ratings obtained through either direct interaction or other customers' feedback. The competence of the CSP is estimated from the transparency of SLAs. The CSP with minimum interaction risk is the one ideal for the cloud customer. Similarly to us, to estimate confidence Ghosh et al., have identified a set of security categories and mapped those categories to low-level security controls supported by the CSPs. However, they do not mention how a value can be assigned to the security categories based on the security controls. Mouratidis et al. [19] describe a framework to select a CSP based on security and privacy requirements. They provide a modelling language and a structured process, but only give a vague description how a structured security elicitation at the CSP works. Akinrolabu [20] develops a framework for supply-chain risk assessment which can also be used to assess the security of different CSPs. For each CSP a score has to be determined for nine different dimensions. However, they do not mention how a value can be assigned to each security dimension. Habib et al. [18] also propose an approach to compute a trustworthiness score for CSPs in terms of different attributes, for example, compliance, data governance, information security. Similarly to us, Habib et al. use CAIQ as a source to assign a value to the attributes on the basis of which the trustworthiness is computed. However, in their approach the attributes match the security domains in the CAIQ and therefore a tenant has to specify its security requirements in terms of the CAIQ security domains. In our approach, we do not have such a limitation: the tenant specifies his security requirements that are then mapped to security categories, that can be mapped to specific security features offered by a CSP. Mahesh et al. [21] investigate audit practices, map the risk to technology that mitigates the risk and come up with a list of efficient security solutions. However, their approach is used to compare different security measures and not different CSPs. Bleikertz et al. [22] support cloud customers with the security assessments. Their approach is focused on a systematic analysis of attacks and parties in cloud computing to provide a better understanding of attacks and find new ones.

Other approaches [14–16] focus on identifying a hierarchy of relevant attributes to compare CSPs and then use multi-criteria decision making techniques to rank them based on those attributes.

Costa et al. [14] proposed a multi-criteria decision model to evaluate cloud services based on the MACBETH method. The services are compared with respect to 19 criteria including also some aspects of security like data confidentiality, data loss and data integrity. However, the MACBETH approach does not support the automatic selection of the CSP because it requires the tenant to give for each evaluation criteria a neutral reference level and a good reference level and to rate the attractiveness of each criteria. While in our approach the input provided by the tenant is minimised: the tenant only specifies the security requirements and their importance and then our approach automatically compares and ranks the candidate CSPs.

Garg et al. proposed a selection approach based on the Service Measurement Index (SMI) [23,24] developed by the Cloud Services Measurement Initiative Consortium (CSMIC) [25]. SMI aims to provide a standard method to measure cloud-based business services based on an organisation's specific business and technology requirements. It is a hierarchical framework consisting of seven categories which are refined into a set of measurable key performance indicators (KPI). Each KPI gets a score and each layer of the hierarchy gets weights assigned. The SMI is then calculated by multiplying the resulting scores by the assigned weights. Garg et al. have extended the SMI approach to derive the relative service importance values from KPIs, and then use the Analytic Hierarchy Process (AHP) [26,27] for ranking the services. Furthermore, they have distinguished between essential, where KPI values are required, and non-essential attributes. They have also explained how to handle the lack of KPI values for non-essential attributes. Built upon this approach, Patiniotakis et al. [16] discuss an alternative classification based on the fuzzy AHP method [28,29] to handle fuzzy KPIs' values and requirements. To assess security and privacy, Patiniotakis et al. assume that a subset of the controls of the cloud control matrix is referenced as KPIs and that the tenant should ask the provider (or get its responses from the CSA STAR registry) and assign each answer a score and a weight.

As the approaches to CSP selection proposed in References [15–17], our approach adopts a multi-criteria decision model based on AHP to rank the CSPs. However, there are significant differences. First, we refine the categories proposed to classify the questions in the CAIQ into sub-categories that represent well-defined security aspects like access control, encryption, identity management, and malware protection that have been defined by security experts. Second, a score and weight to these categories is automatically assigned based on the answers that providers give to corresponding questions in the CAIQ. This reduces the effort for the cloud customer who can rely on the data published in CSA STAR rather than interviewing the providers to assess their security posture.

Table 1 provides and overview of the mentioned related work. The columns "dimension" list if the approach considers security and/or other dimensions, the column "data security" lists if the approach proposes a specific method how to evaluate security and the column "security categories" lists how many different categories are considered for security.

In summary, to the best of our knowledge, our approach is the first approach to CSP selection that provides an effective way to measure the security of a provider. Our approach could be used as a building block for the existing approaches to CSP selection that consider also other providers' attributes like cost and performance.

Table 1. Comparison of Different cloud service provider (CSP) Comparison/Selection Approaches.

Reference	Method	Dimensions		Security	
		Other	Security	Data	Categories
Anastasi et al. [7]	genetic algorithms	✓	✗	✗	✗
Ngan and Kanagasabai [8]	ontology mapping	✓	✗	✗	✗
Sim [9]	ontology mapping	✓	✗	✗	✗
Wang and Du [10]	game theory	✓	✗	✗	✗
Karim et al. [11]	MCDM [1]	✓	✗	✗	✗
Sundareswaran et al. [12]	k-nearest neighbours	✓	✓	✗	✗
Ghosh et al. [13]	minimize interaction risk	✓	✓	✗	12
Costa et al. [14]	MCDM [1]	✓	✓	✗	3
Garg et al. [15]	MCDM [1]	✓	✓	✗	7
Patiniotakis et al. [16]	MCDM [1]	✓	✓	✗	1
Wittern et al. [17]	MCDM [1]	✓	✓	✗	unspec.
Habib et al. [18]	trust computation	✓	✓	(✓) [2]	11
Mouratidis et al. [19]	based on Secure Tropos	✗	✓	✗	unspec.
Akinrolabu et al. [20]	risk assessment	✗	✓	✗	9
Our Approach	MCDM [1]	✗	✓	✓	flexible

[1] multi-criteria decision making. [2] Data source (CAIQ) specified, but only yes/no considered and no specific algorithm specified.

3. Standards and Methods

In the first subsection we introduce the Cloud Security Alliance (CSA), the Cloud Controls Matrix (CCM) and the Consensus Assessments Initiative Questionnaire (CAIQ). In the second subsection, we discuss the issues related to the use of CAIQs to compare and ranking CSPs' security.

3.1. Cloud Security Alliance's Consensus Assessments Initiative Questionnaire

The Cloud Security Alliance is a non-profit organisation with the aim to promote best practices for providing security assurance within Cloud Computing [30]. To this end, the Cloud Security Alliance has provided the Cloud Controls Matrix [31] and the Consensus Assessments Initiative Questionnaire [32]. The CCM is designed to guide cloud vendors in improving and documenting the security of their services and to assist potential customers in assessing the security risks of a CSP.

Each control consists of a control specification which describes a best practice to improve the security of the offered service. The controls are mapped to other industry-accepted security standards, regulations, and controls frameworks, for example, ISO/IEC 27001/27002/27017/27018, NIST SP 800-53, PCI DSS, and ISACA COBIT.

Controls covered by the CCM are preventive, to avoid the occurrence of an incident, detective, to notice an incident and corrective, to limit the damage caused by the incident. Controls are in the ranges of legal controls (e.g., policies), physical controls (e.g., physical access controls), procedural controls (e.g., training of staff), and technical controls (e.g., use of encryption or firewalls).

For each control in the CCM the CAIQ contains an associated question which is in general a 'yes or no' question asking if the CSP has implemented the respective control. Figure 1 shows some examples of questions and answers. Tenants may use this information to assess the security of CSPs whom they are considering contracting.

CID	Consensus Assessment Questions	Response	Comments and Notes
CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Yes	Independent internal and external audits are scheduled and conducted with audit assertions produced following ISACA's Cloud Computing Management Audit/Assurance Program and ISO 27001.
CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	Yes	Independent audit reports produced by external security consultant and certification body are available for viewing by tenants upon request.
CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	Yes	Penetration Testing and Vulnerability Assessment on the cloud service infrastructure at network, operating systems and application levels are conducted half-yearly by independent security consultant.
CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?	Yes	Web Application Penetration Testing and Vulnerability Assessment on the cloud service infrastructure is conducted on a half-year basis by independent security consultant.
CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	Yes	Internal audits are conducted at least annually using the ISACA Cloud Computing Management Audit / Assurance Program and ISO 27001 as the basis of evaluation.
CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?	Yes	External audits are conducted at least annually using ISO 27001 as the basis of evaluation.
CO-02.6	Are the results of the network penetration tests available to tenants at their request?	Yes	Penetration Testing and Vulnerability Assessment Reports are available for viewing by tenants upon request.
CO-02.7	Are the results of internal and external audits available to tenants at their request?	Yes	Internal and external audit reports are available for viewing by tenants upon request.
CO-03.1	Do you permit tenants to perform independent vulnerability assessments?	Yes	Tenants can perform independent vulnerability assessments of their own virtual infrastructure or equipment.
CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?	Yes	Penetration testing and vulnerability assessment on the applications and networks of the cloud computing infrastructure are conducted by external third party security consultant at least annually.
CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes	Contact list of local authorities is maintained and updated regularly.

(**a**) Snapshot of a CAIQ version 1.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers		
					Yes	No	Not Applicable
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?			
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?			
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?			
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?			
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?			
Application & Interface Security	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?			
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?			
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Does your data management policies and procedures require audits to verify data input and output integrity routines?			
		AIS-03.2		Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?			
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?			
Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?			
		AAC-01.2		Does your audit program take into account effectiveness of implementation of security operations?			
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?			
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure at least annually?			
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?			
		AAC-02.4		Do you conduct internal audits at least annually?			
		AAC-02.5		Do you conduct independent audits at least annually?			
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?			
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?			

(**b**) Snapshot of a CAIQ version 3.1

Figure 1. Consensus Assessments Initiative Questionnaire (CAIQ) questionnaires.

As of today, there are two relevant versions of the CAIQ: version 1.1 from December 2010 and version 3.0.1 from July 2014. CAIQ version 1.1 consists of 197 questions in 11 domains (see Table 2), while CAIQ version 3.0.1 instead consists of 295 questions grouped in 16 domains (see Table 3). In November 2019 version 3.1 of the CAIQ was published and it was stated that 49 new questions were added, and 25 existing ones were revised. Furthermore, with CAIQ-Lite, there exists a smaller version consisting of 73 Questions covering the same 16 Control Domains.

Table 2. Cloud Controls Matrix (CCM)-Item and CAIQ-Question Numbers per Domain (version 1.1).

ID	Domain	CCM-Items	CAIQ-Questions
CO	Compliance	6	16
DG	Data Governance	8	16
FS	Facility Security	8	9
HR	Human Resources	3	4
IS	Information Security	34	75
LG	Legal	2	4
OP	Operations Management	4	9
RI	Risk Management	5	14
RM	Release Management	5	6
RS	Resiliency	8	12
SA	Security Architecture	15	32
	Total	98	197

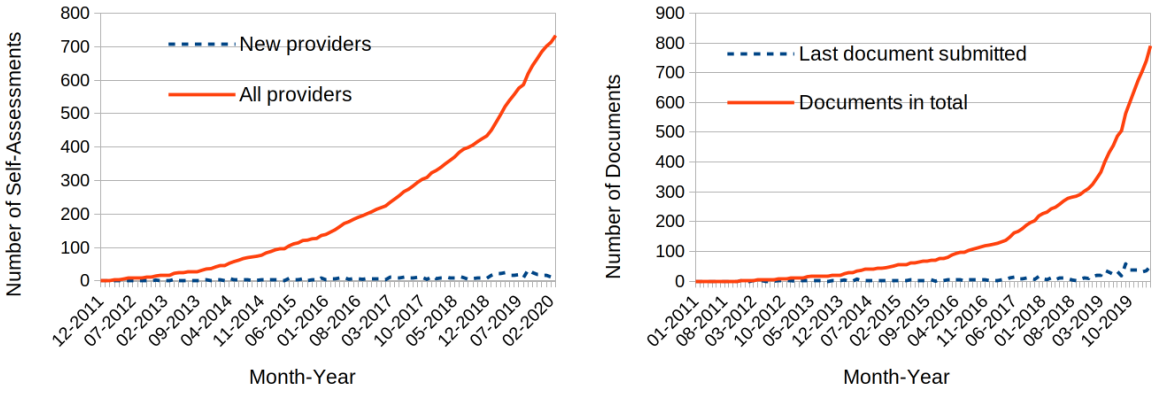
Table 3. Cloud Controls Matrix (CCM)-Item and CAIQ-Question Numbers per Domain (version 3.1).

ID	Domain	CCM	CAIQ
AIS	Application & Interface Security	4	9
AAC	Audit Assurance & Compliance	3	13
BCR	Business Continuity Management & Operational Resilience	11	22
CCC	Change Control & Configuration Management	5	10
DSI	Change Control & Configuration Management	7	17
DCS	Datacenter Security	9	11
EKM	Encryption & Key Management	4	14
GRM	Governance and Risk Management	11	22
HRS	Human Resources	11	24
IAM	Identity & Access Management	13	40
IVS	Infrastructure & Virtualization Security	13	33
IPY	Interoperability & Portability	5	8
MOS	Mobile Security	20	29
SEF	Security Incident Management, E-Discovery & Cloud Forensics	5	13
STA	Supply Chain Management, Transparency and Accountability	9	20
TVM	Threat and Vulnerability Management	3	10
	Total	133	295

CAIQ version 3.0.1 contains a high level mapping to CAIQ version 1.1, but there is no direct mapping of the questions. Therefore, we mapped the questions. In order to determine the differences, we computed the Levenshtein distance (The Levenshtein distance is a string metric which measures the difference between two strings by the minimum number of single-character edits (insertions, deletions or substitutions) required to change one string into the other) [33] between each question from version 3.0.1 and version 1.1. The analysis shows that out of the 197 questions of CAIQ version 1.1 one question was a duplicate, 15 were removed, 12 were reformulated, 79 have undergone editorial changes (mostly Levenshtein distance less than 25), and 90 were taken over unchanged. Additionally 114 new questions were introduced to CAIQ version 3.0.1.

The CSA provides a registry, the Cloud Security Alliance Security, Trust and Assurance Registry (STAR), where the answers to the CAIQ of each participating provider are listed. As shown in Figure 2, the STAR is continuously updated. The overview of answers to CAIQ submitted to STAR in Figure 2 shows that from the beginning in 2011 each year there are more providers contributing to it. At the beginning of October 2014 there were 85 documents in STAR: 65 answers to CAIQ, 10 statements to the CCM, and 10 STAR certifications, where the companies did not publish corresponding self-assessments. In March 2020, there were 733 providers listed with 690 CAIQs (53 versions 1.* or 2515 version 3.0.1,

122 version 3.1), and 106 certifications/attestations. Some companies list the self-assessment along with their certification, some do not provide their self-assessment when they got a certification.



(**a**) Providers (**b**) Documents

Figure 2. Submissions to Security, Trust and Assurance Registry (STAR).

3.2. Processing the CAIQ

Each CAIQ is stored in a separate file with a unique URL. Thus, there is no way to get all CAIQs in a bunch and no single file containing all the answers. Therefore, we had to manually download the CAIQs with some tool support. After downloading, we extracted the answers to the questions and stored them in an SQL database. A small number of answers was not in English and we disregarded them when evaluating the answers.

One challenge was, that there was no standardization of the document format. In October 2014, the 65 answers to CAIQ were in various document formats (52 XLS, 7 PDF, 5 XLS+PDF, 1 DOC). In March 2020, the majority of the document formats was based on Microsoft Excel (615), but there were also others (41 PDFs, 33 Libre Office documents (33), 1 DOC). Besides the different versions, that is, version 1.1 and version 3.0.1, another issue was that many CSP do not comply with the standard format for the answers proposed by the CSA. This makes it not trivial to determine whether a CSP implements a given security control.

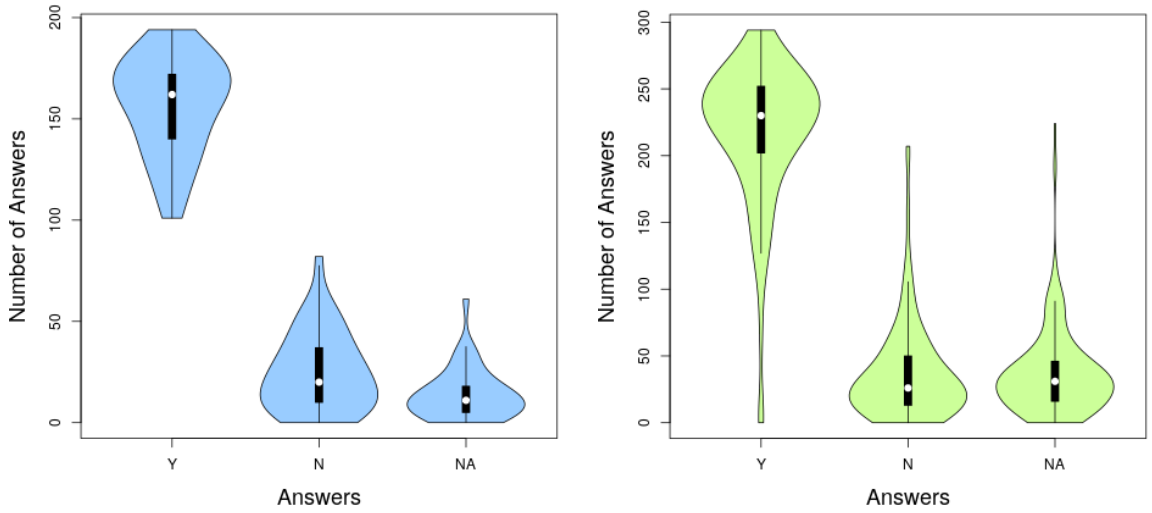
For CAIQ version 1.1 the CSA intended the CSPs to use one column for yes/no/not applicable (Y/N/NA) answers and one column for additional, optional comments (C) when answering the CAIQ. But only a minority (17 providers) used it that way. The majority (44 providers) used only a single column which mostly (22 providers), partly (11 providers) or not at all (11 providers) included an explicit Y/N/NA answer. For CAIQ version 3.0.1 the CSA has introduced a new style: three columns where the provider should indicate whether yes, no or not applicable holds, followed by a column for optional comments. So far, this format for answers seems to work better, since most providers answering CAIQ version 3.0.1 followed it, however, since some providers merged cells, added or deleted columns or put their answer in other places, the answers to the CAIQ can not be gather automatically.

To make it even harder for a customer to determine whether a CSP supports a given security control, the providers did not follow a unique scheme for answers. For example to questions of the kind "Do you provide [some kind of documentation] to the tenant?" some provider answered "Yes, upon request" when others answered "No, only on request". Similarly, some questions asking if controls are in place were answered by some providers with "Yes, starting from [Date in the future]" while others answered "No, not yet". However, these are basically the same answers, but expressed differently. Similar issues could be found for various other questions, too.

Additionally, some providers did not provide a clear answer. For example, some providers claim that they have to clarify some questions with a third party or did not provide answers for questions at all. Some providers also make use of Amazon AWS (e.g., Acquia, Clari, Okta, Red Hat, Shibumi)

but gave different answers when referring to controls implemented by Amazon as IaaS-Provider or did not give an answer and just referred to Amazon.

In order to facilitate the CSPs' answers for comparison and ranking, we give a brief overview of the processed data. Figure 3 (cf. Section 5.4 for information how we processed the data) shows the distribution of the CSPs' answers to the CAIQ. Neglecting the number of questions, there is no huge difference between the distribution in the different versions of the questionnaires. The majority of controls seem to be in place, since "yes" is the most common answer. It can also be seen that the deviation of all answers is quite large which suits to the observation that they are not equally distributed. Regarding the comments on average every second answer had a comment. However, we noticed that comments are a double edge sword: sometimes they help to clarify an answer because they provide the rationale for the answer while at other times they make the answer unclear because they provide information that is conflicting with the yes/no-answer.

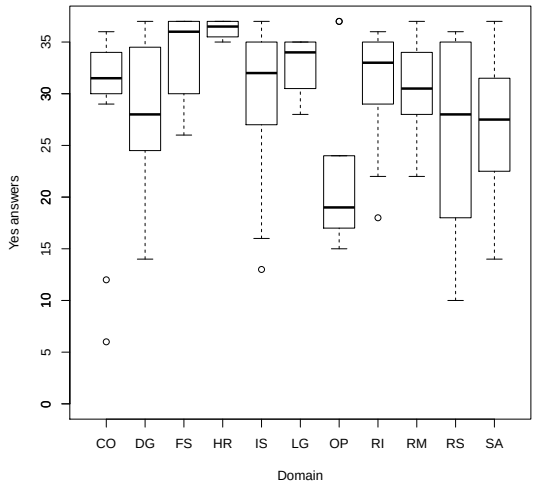


(**a**) CAIQ 1.1, n = 37 (**b**) CAIQ 3.0.1, n = 189

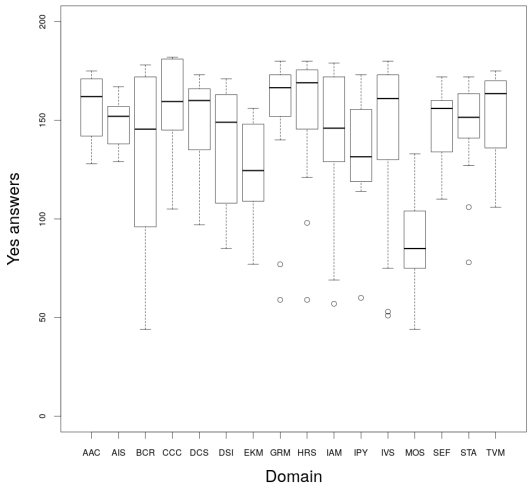
Figure 3. Distribution of Answers per Provider of the CAIQ as Violin-/Boxplot.

We also grouped questions by their domain (x-axis) and for each question within that domain determined the number of providers (y-axis) who answered with yes, no or not applicable. The number of questions per domain can be seen in Table 2 and Table 3. Figure 4 shows that for most domains, questions with mostly yes answers dominate (e.g., the domain "human resources" (HR) contains questions with 35 to 37 yes answers from a total of 37 providers (cf. Figure 4a). The domain of "operation management" (OP) holds questions with a significant lower count of yes answers due to questions with many NA answers (cf. Figure 4e), similarly to the domain of "mobile security" (MOS) in version 3.0.1 (cf. Figure 4f). The domains "data governance" (DG), "information security" (IS), "resilience" (RS) and "security architecture" (SA) share a larger variance that means that they contain questions with mostly yes answers as well as questions with only some yes answers.

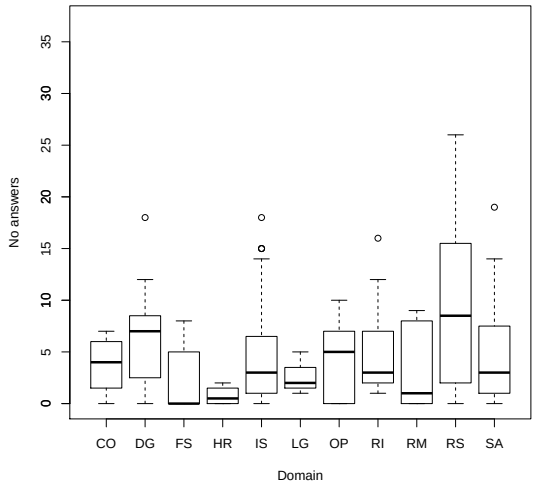
The above issues indicate that gathering information on the CSPs' controls and especially comparing and ranking the security of CSPs using the answers to CAIQ is not straight forward. For this reason, we have conducted a controlled experiment to assess whether it is feasible in practice to select a CSP using CAIQ. We also tested if comments help to determine if a security control is supported or not by CPSs.



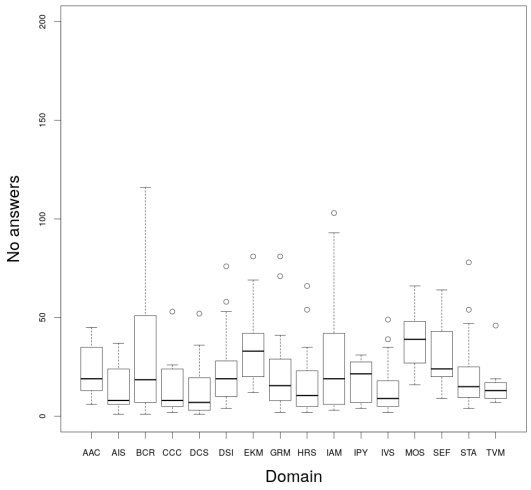
(**a**) Yes Answers, CAIQ v1.1, n = 37



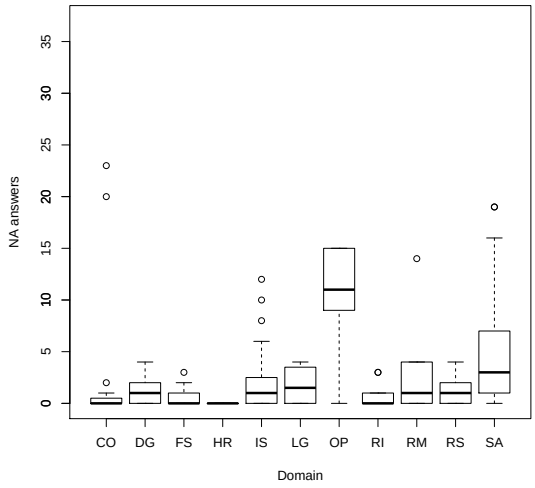
(**b**) Yes Answers, CAIQ v3.0.1, n = 189



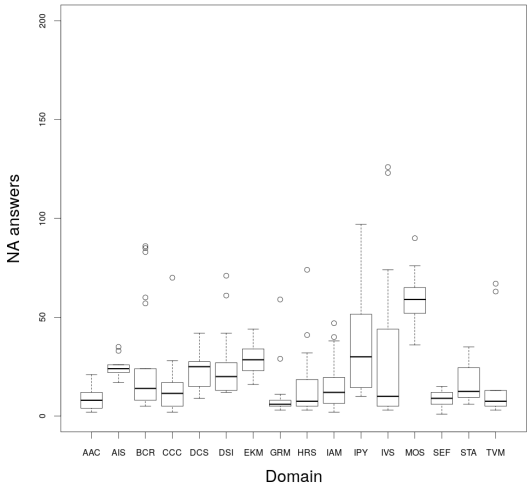
(**c**) No Answers, CAIQ v1.1, n = 37



(**d**) No Answers, CAIQ v3.0.1, n = 189



(**e**) NA Answers, CAIQ v1.1, n = 37



(**f**) NA Answers, CAIQ v3.0.1, n = 189

Figure 4. Distribution of Answers per Question grouped by Domain of CAIQ v1.1 and v3.0.1.

4. Empirical Study on Cloud Service Provider Selection

In this section we report on an empirical study conducted to evaluate the actual and perceived effectiveness of the CSP selection process based on the CAIQ. The perceived effectiveness of the selection process is assessed in terms of perceived ease of use and perceived usefulness.

4.1. Research Questions

The main research questions that we want to address in our study are:

- RQ_1—*Are CAIQs effective to compare and rank the security of CSPs?*
- RQ_2— *Are CAIQs perceived as ease to use (PEOU) to compare and rank the security of CSPs?*
- RQ_3— *Are CAIQs perceived as useful (PU) to compare and rank the security of CSPs?*

4.2. Measurements

To measure the *effectiveness* of using CAIQ, we assessed the correctness of the selection made by the participants. We asked two security experts (among the authors of this paper) to perform the same task of the participants. Then, we used the results produced by the experts as baseline to evaluate the correctness of the provider selected by the participants.

Instead, to measure the participants' *perception* of using CAIQs to select CSPs, we administered them a post-task questionnaire inspired to the Technology Acceptance Model (TAM) [34]. The questionnaire consisted of seven questions: five closed questions and two open questions: Q_1: The questions and answer in the CAIQ are clear and ease to understand (PEOU); Q_2: CAIQs make easier to assess and compare the security posture of two cloud providers (PEOU); Q_3: The use of CAIQs would reduce the effort required to compare the security posture of two cloud providers (PEOU); Q_4: The use fo CAIQs to assess and compare the security posture of two cloud provider was useful (PU); and Q_5: CAIQs do not provide an effective and complete solution to the problem of assessing and comparing the security posture of two cloud providers (PU). The closed questions were with answers on a 5 Likert scale: Strongly Agree (1) to Strongly Disagree (5).

The two open questions were included to collect insights into the rationale for selecting a CSP over another: (a) which of the two cloud providers better addresses BankGemini data protection and compliance requirements and (b) why the second provider worse addresses BankGemini security and compliance concerns.

4.3. Procedure

In order to measure the *actual effectiveness* and *perception* of using CAIQs to compare and select a cloud provider, the participants of our study were asked to impersonate BankGemini, a fictitious bank who would like to move their online banking services to the the cloud. BankGemini has very stringent requirements on data protection and legal compliance and has to select a cloud provider that meets its requirements. Due to the limited time available to run the study, we had to simplify the task for the participants. First, the participants only had to select the more secure cloud provider among only two cloud providers rather than several ones like it happens in practice. The participants were requested to choose among to real cloud providers Acquia and Capriza the one which better fulfills its data protection and compliance requirements. Second, the participants did not specify the security requirements against which comparing the two cloud providers but the requirements were given to them as part of the scenario introducing BankGemini.

4.4. Study Execution

The study consisted of three controlled experiments that took place at different locations. The first experiment took place at the University of Trento. The second one was organized at the Goethe University Frankfurt. The last experiment was conducted at University of Southampton. The same settings were applied for the execution of the three experiments. First, the participants attended one

hour lecture on cloud computing, the security and privacy issues related to cloud computing and the problem of selecting a cloud provider that meets the security needs of a tenant.

Then, 10 min were spent to introduce the participants to the high level goal of the study. The participants were explained that they had to play the role of the tenant—BankGemini—which has specific data protection and compliance requirements and that they had to select a CSP between Acquia and Capriza that better fulfils these requirements. To perform the selection, the participants were provided with:

- a brief description of BankGemini including the security requirements (for an example, refer to Appendix A)
- the CAIQ for Acquia and Capriza (see Supplementary Materials).

They were given 40 min to read the material and select the best CSP given the security requirements. After the task, they had 15 min to complete the post-task questionnaire.

4.5. Participants' Demographics

In our study we involved a total of 44 students with a different background. The first experiment conducted at the University of Trento involved 26 MSc students in Computer Science. The second one organized at the Goethe University Frankfurt involved 4 students in Business and IT. The last experiment conducted at University of Southampton had 14 MSc students in Cyber Security as participants. Table 4 highlights the background of the participants. Most of the participants (70%) had at least 2 years of working experience. Most of the participants have some knowledge in security and privacy but were not familiar with the online banking scenario that they analyzed.

Table 4. Overall Participants' Demographic Statistics

Variable	Scale	Mean/ Median	Distribution
Education Length	Years	4.7	56.8% had less than 4 years; 36.4% had 4–7 years; 6.8% had more than 7 years
Work Experience	Years	2.1	29.5% had no experience; 47.7% had 1–3 years; 18.2% had 4–7 years; 4.5% had more than 7 years
Level of Expertise in Security	0 [1]–4 [2]	1 [3]	20.5% novices; 40.9% beginners; 22.7% competent users; 13.6% proficient users; 2.3% experts
Level of Expertise in Privacy	0 [1]–4 [2]	1 [3]	22.7% novices; 38.6% beginners; 31.8% competent users; 6.8 % proficient users
Level of Expertise in Online Banking	0 [1]–4 [2]	1 [3]	47.7% novices; 34.1% beginners; 15.9% competent users; 2.3% proficient users

[1] Novice. [2] Expert. [3] Median.

4.6. Results

In this section we report the results on the actual and perceived effectiveness of using CAIQs to compare and rank CSPs.

4.6.1. Actual Effectiveness

To evaluate the correctness of the selection made by the participants we have asked two security experts to perform the same task of the participants. The experts agreed that the provider that best meets BankGemini's security requirements is Aquia. Indeed, Aquia allows tenants to decide the location for data storage, enforces access control for tenants, cloud provider's employees and subcontractors, monitors and logs all data accesses, classify data based on their sensitivity, and clearly defines the responsibilities of tenants, cloud providers and third parties with respect to data processing, while Capriza does not.

As shown in Figure 5, the results are not consistent across the three experiments. In the first experiment, the number of participants who selected Aquia is basically the same of the one who selected Capriza. However, in the second and the third experiment almost all the participants correctly identified Aquia as the cloud provider that best satisfies the given security requirements. If look the overall results, most of the participants (68%) were able to identify the correct cloud service provider based on the CAIQ, which indicates that CAIQ could be an effective tool to comparing and ranking the security posture of CSPs.

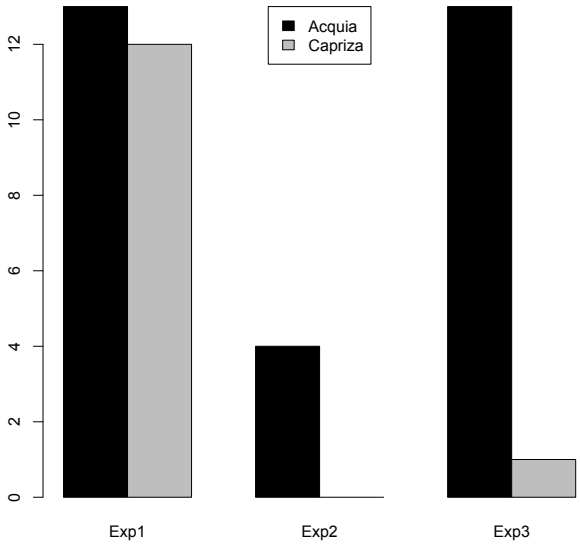


Figure 5. Actual Effectiveness—Cloud Provider Selected in the Experiments).

4.6.2. Perceived Effectiveness

Table 5 reports the mean for the answers related to PEOU and PU. The mean of the answers for all the three experiments is close to 3, which means that the participants are not confident that CAIQs make easier to compare and rank the security of CSPs and that are useful to perform the comparison and ranking of cloud service providers. These results are consistent among the three experiments. To test whether there is a statistically significant difference among the answers given by the participants in the three experiments, we run the Kruskal-Wallis statical test, the non-parametric alternative to one-way ANOVA for each question on PEOU and PU and on overall PEOU and PU. We assumed a significance level $\alpha = 0.05$. The p-values returned by Kruskal-Wallis test are reported in Table 5. The p-values are all greater than α, and therefore we have to accept the null hypotheses that there is no difference in the mean of the answers given by the participants in the three experiments. This means that all the participants believe that CAIQs are not ease to use and not useful to compare and select a cloud service provider.

Table 5. Questionnaire Analysis Results—Descriptive Statistics.

Q	Type	Mean				*p*-Value
		Exp1	Exp2	Exp3	All	
Q1	PEOU	3	3.7	2.9	3.0	0.3436
Q2	PEOU	2.9	2.7	2.7	2.8	0.8262
Q3	PEOU	2.4	2.2	2.4	2.4	0.9312
Q4	PU	2.4	2.5	2.2	2.3	0.9187
Q5	PU	3.1	3.2	3.0	3.1	0.8643
PEOU		2.8	2.9	2.7	2.7	0.7617
PU		2.7	3.0	2.6	2.7	0.9927

4.7. Threats to Validity

The main threats that characterize our study are related to conclusion and external validity.

Conclusion validity is concerned with issues that affect the ability to draw the correct conclusion about the relations between the treatment and the outcome of the experiment. One possible threat to conclusion validity is related to how to evaluate the effectiveness of CAIQs in comparing and ranking the security posture of CSPS. Actual effectiveness should be assessed based on the correctness of the results produced by the participants. Therefore, in our study we asked two of the authors of this paper to perform the same selection task performed by the participants and use their results as baseline to evaluate the correctness of the best CSP identified by the participants.

External validity concerns the ability to generalize experiment results beyond the experiment settings. The main threat is related to the *use of the students instead of practitioners*. However, some studies have argued that students perform as well as professionals [35,36]. Another threat to external validity is the *realism of experimental settings*. The experiments in our study were organised as a laboratory session and therefore the participants had limited time to by the participants in comparing and ranking the security posture of CSPs. For this reason we had to simplify the task by providing to the participants Bank Gemini's security requirements, rather then letting them identify the requirements. However, this is the only simplification that we introduced. For the rest, the task is the same that a tenant would perform when selecting and comparing the security of CSPs.

4.8. Implications for Practice

The CAIQ provides a standard framework that should help tenants to assess the security posture of a CSP. The last version of the CAIQ includes 295 security controls grouped in 16 domains. Each of this control has one or more "yes, no or not applicable" control assertion questions which should allow a tenant to determine whether a provider implements security controls that suit the tenant's security requirements.

The results of our study show that the selection of a cloud provider based on the CAIQ's questions and answers could be effective because most of the participants were able to correctly select Aquia as the CSP that best meet the requirements of the tenant. However, the participants of our study are not confident that the approach is ease to use and useful to select and compare the security posture of CSPs.

The main reason why CAIQ is not perceive as ease to use and useful, is that for each CSP to be compared, a tenant has to go through 295 questions in the CAIQ, identify those questions that match the tenant security requirements, and evaluate the answers provided by the CSP to decide if the corresponding security control is supported or not. This is quite a cumbersome task for the tenant.

Therefore, there is the need for an approach that extracts from the CAIQs the information to determine if a CSP meets a tenant's security requirements and based on this information assesses the overall security posture of the provider.

5. Ranking Cloud Providers' Security

In this section we present an approach that facilitates the comparison of the security posture of CSPs based on CAIQ's answers. The approach is illustrated in Figure 6. There are three main actors involved: the tenant, the alternative CSPs, and the cloud broker. A cloud broker is an intermediary between the CSPs and the tenant, that helps the tenant to choose a provider tailored to his security needs (cf. NIST Cloud Computing Security Reference Architecture [37]). (For example Deutsche Telekom is offering this service [38]). In the setup, the broker has to assess the answers of the CSPs (classification and scoring) and define the security categories which are mapped to the CAIQ's questions. The list of security categories is then provided to the tenant. For the ranking, the broker first selects the candidate CSPs among the ones that deliver the services requested by the tenant. Then, it ranks the candidate providers based on the weighted security categories specified by the tenant and the answers that the providers gave to the CAIQ. The list of ranked CSPs is returned to the tenant, who uses the list as part of his selection process.

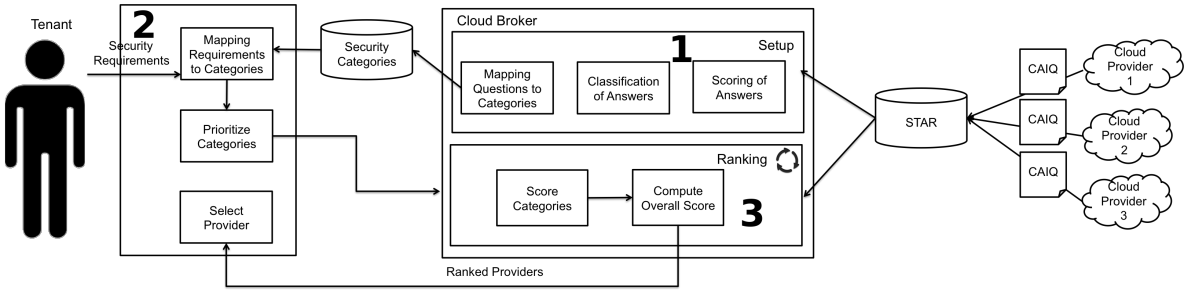


Figure 6. Security-Aware Cloud Provider Selection Approach.

The approach to rank CSPs adopts the Analytic Hierarchy Process (AHP) [26]. The first step is to decompose the selection process into a hierarchy. The top layer reflects the goal of selecting a secure CSP. The second layer denotes the security categories with respect to which the CSPs are compared while the third layer consists of the CAIQ's questions corresponding to the security categories. The bottom most layer contains the answers to the CAIQ's questions given by the different CSPs. The hierarchy is shown in Figure 7: weights and calculator symbols near each layer denote that a weight and a score for that layer is computed while the number on the symbols refer to the section in the paper were the computation is described. Similarly, the pad symbol denotes that the scores are aggregated.

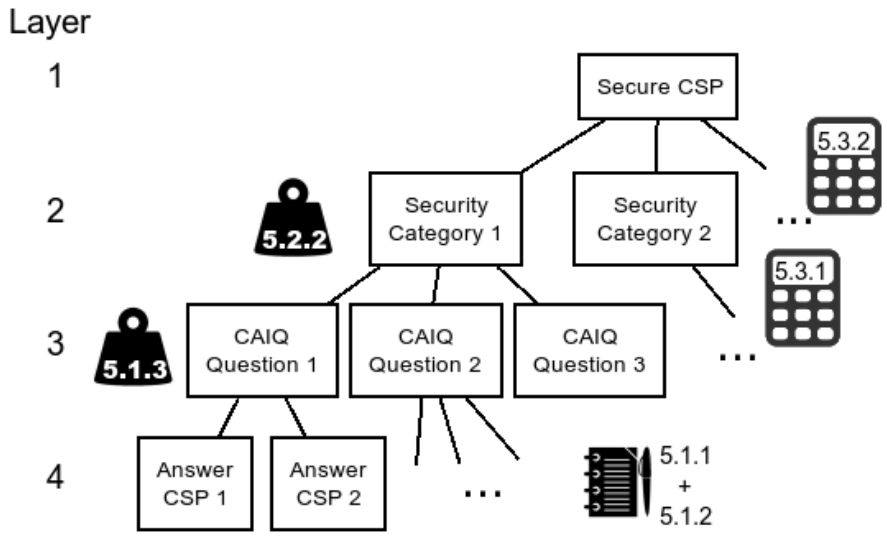


Figure 7. Hierarchies of Analytic Hierarchy Process (AHP) based Approach.

The result at the end of the decision making process is a hierarchy where each CSP gets a overall score and a score for each category. This allows the tenant not only to use the overall result in CSP selection processes with other criteria, but also to reproduce the CSPs' strengths and weaknesses regarding each category. For this reason, we chose to base our approach on AHP because it not only comes up with a result, but also provides some information on how the score was calculated (the scores of each category). This allows further reasoning or an adaptation of the requirements/scoring should the tenant not be confident with the result. In what follows we present in details each step of the CSP selection process.

5.1. Setup

Before the cloud broker can identify the optimal CSP based on the tenant's security needs there are three main steps he has to perform: classification of answers, scoring of answers and mapping questions from the CAIQ to security categories. Note that these steps have to be done only once for each provider present in the STAR.

5.1.1. Classification of Answers

The original AHP approach would require a pairwise comparison of all answers to each question. However, given the 37 (65) providers and 197 questions this would require 131202 (409760) comparisons and therefore is not feasible. Thus, the answers have to be manually classified which is extremely time consuming. The classification is reported in Table 6. Other classifications are also possible, depending on the new classification it may be sufficient to only re-rate a part of the answers.

Table 6. Possible Classes for Answers in CAIQ.

Answer	Comment Class	Description
Yes	Conflicting	The comment conflicts the answer.
Yes	Depending	The control depends on someone else.
Yes	Explanation	Further explanation on the answer is given.
Yes	Irrelevant	Comment is irrelevant to the answer.
Yes	Limitation	The answer 'yes' is limited or related due to the comment.
Yes	No comment	No comment was given.
No	Conflicting	The comment conflicts the answer.
No	Depending	The control depends on someone else.
No	Explanation	Further explanation on the answer is given.
No	Irrelevant	Comment is irrelevant to the answer.
No	No comment	No comment was given.
NA	Explanation	Further explanation on the answer is given.
NA	Irrelevant	Comment is irrelevant to the answer.
NA	No Comment	No comment was given.
Empty	No comment	No answer at all
Unclear	Irrelevant	Only comment was given and thereupon it was not possible to classify the answer as one of Y/N/NA.

The comments are used to further rate the answers of CSPs in more detailed classes. "Yes", "No" and "Not applicable" answers are assigned to the class "*No comment*" if the CSP did not give a comment. If the given answer is further described, for example, if additional information of the control in place, why the control is not in place or why this question is not applicable is given, the answers are assigned to the class "*Explanation*". If there is a comment, but it does not explain the answer of the provider, the answer is classified as "*Irrelevant*". An example for this class is the repeating of the question as a full sentence. Also comments about Non disclosure agreements which may have to be signed before were put in this class. For "yes" and "no" answers, two additional classes are considered: "*Depending*" if the provider claims that the control depends on a third party, and "*Conflicting*" if the

answer conflicts with the statement of the comment. For example "Yes, not yet started" means that either the control is not in place or the comment is wrong. For "yes" answers also the class "*Limitation*" is used when the comment limits the statement that the control is in place. Examples for this are comments which restrict the control to specified systems, which means that the control is not in place for all systems or when it is asked if the provider makes documentation available to the tenant and the comment restricts that to summaries of the specified documents. For empty answers only the class "*No comment*" is considered and for unclear answers only the class "*Irrelevant*" is used.

5.1.2. Scoring of Answers

Once the answers are classified, for each of the answers a score as to be computed to determine how the CSPs performs for each question (3rd AHP layer, sub criteria). The scoring depends on the aim the tenant wants to achieve, thus other scores are possible. For our approach we distinguish between two kind of tenants: tenants who really want to invest in security and tenants who are primarily interested in compliance (cf. Reference [39]). The tenant who wants to invest in security tries to reduce the risk of data loss. Therefore, he wants to compare the CSPs based on the risk level that incidents (e.g., loss of data, security breaches) happen. Thus, the best answer is a "Yes" with an "Explanation", followed by "Yes" answers with "No comment" or when the provider claims that the control is handled by a third party. "Irrelevant" comments, "Limitation", or even "Conflicting" comments may indicate that the control is not properly in place or not in place at all. If the provider claims that the control is not in place, the best the tenant can expect is an explanation why it is not in place, while conflicting answers may offer a chance that this control is in spite of the provider's answer in place. If the provider answered "Non Applicable", the tenant may have chosen a provider offering an unsuitable service or the provider may not have recognised that this control is relevant for him. Thus, "Non Applicable" answers were rated slightly lower than "No" answers. "Empty" and "Unclear" comments score lowest.

Instead, the tenants who are interested in compliance try to reduce the risk that if an incident occurs, there is no claim for damages or lost lawsuit. Thus, the tenant's interest is to compare the CSPs based on the risk level that he is sued after an incident has happened. Thus, basically most of the"yes" answers allow the tenant to blame his provider, should an incident have happened. However, "Limitation" and 'Conflicting" comments are scored lower, since a judge might conclude that the tenant should have noticed that. "No" answers score 0 as the latter would imply being surely not compliant. "Not applicable,""Empty" or "Unclear" answers leave at least a basis for discussions, and thus have a low score.

The scoring schemes for these two types of tenants discussed above were independently approved by three experts and are shown in Table 7.

Compared to the classification of the answers, the mapping of answer classes to scorings is less effort, but still a very decisive step which should be done by experts from the cloud broker based on the tenants' desired aims.

Table 7. Possible Scoring for Tenants Interested in Security or Compliance.

Answer	Comment Class	Security	Compliance
Yes	Explanation	9	9
Yes	No comment	8	9
Yes	Depending	8	9
Yes	Irrelevant	7	9
Yes	Limitation	6	7
Yes	Conflicting	5	5
No	Explanation	4	1
No	Conflicting	4	1
No	No comment	3	1
No	Depending	3	1
No	Irrelevant	2	1
NA	Explanation	3	3
NA	No comment	2	3
NA	Irrelevant	2	3
Empty	No comment	1	2
Unclear	Irrelevant	1	2

5.1.3. Mapping of Questions to Security Categories

The questions from CAIQ need to be mapped to security categories and assigned scores reflecting their importance to the corresponding category. This is basically the decision which sub criteria (3rd AHP layer) belong to which criteria (2nd AHP layer). Examples for security categories are: access control, data protection at rest/transport, patching policy, and penetration testing. The weight can be either given by comparing the security categories pairwise or as an absolute score.

The used score is shown in Table 8. Its range is from one to nine. If an absolute score is given (also in the range from one to nine), the relative weight for two categories (questions) may be derived by subtracting the lower score from the higher score and adding one. We give an example in the next section.

Table 8. Weights for Comparing Importance of Categories and Questions.

Weight	Explanation
1	Two categories (questions) describe an equal importance to the overall security (respective category)
3	One category (question) is moderately favoured over the other
5	One category (question) is strongly favoured over the other
7	One category (question) is very strongly favoured over the other
9	One category (question) is favoured over the other in the highest possible order

The result from this step is a list of predefined security categories and a list of weighted questions from the CAIQ mapped to the categories. The security domains provided by the CAIQ would be quite natural to use, but its use has some drawbacks. We give an additional mapping, since not every question should have the same weight inside each category. Additionally, some questions may contribute to different security categories whereas each question is part of exactly one domain in CAIQ. Furthermore, answers are not distributed equally among the different domains. Some domains essentially contain almost only questions with yes answers (cf. Figure 4). Thus, our approach is more fine-grained. We also allow different granularity, for example, for one tenant confidentiality may be sufficient, since it is only one of the tenant's multiple security requirements. Another tenant may be especially interested in that category and regard data protection at rest and data protection at transport as different security categories instead. A sample table is given in the next section (cf. Table A1).

5.2. Tenant's Task

The following steps have to be performed by the tenant, but the tenant could also be supported by experts from the cloud broker.

1. *Security Requirements:* The tenant specifies the security requirements on the data and/or applications he would like to outsource to a CSP.
2. *Map requirements to security categories:* The tenant has to map the security requirements to the predefined security categories provided by the cloud broker and assign a weight to each category that quantifies its overall importance to the tenant. The weight can be either given by comparing categories pairwise or as an absolute score. The result is a subset of the security categories predefined by the cloud broker along with their score. This defines the 2nd layer of the AHP hierarchy.
3. *Confirming setup:* If the tenant does not agree with the choices made during the setup phase, he has to ask his cloud broker to specify an alternative version. Especially, the tenant may ask for additional predefined security categories if they do not fit his needs.

5.3. Ranking Providers

The evaluation of the previously gathered weights and scores is done bottom up by the cloud broker.

5.3.1. Scoring Security Categories

We assume, there are I security categories c_i with J_i questions each and $1 \leq i \leq I$. For each security category c_i the scores of the CSP's answers to the relevant questions q_{ij} have to be compared (with $1 \leq j \leq J_i$). We already described in Section 5.1.2 how we classified those answers. We compare them by building the difference of their scores and adding one. The interpretation of those comparison scores is shown in Table 9.

Table 9. Scores for Comparing Quality of Answers to CAIQ.

Score	Explanation
1	Two answers describe an equal implementation of the security control
3	One answer is moderately favoured over the other
5	One answer is strongly favoured over the other
7	One answer is very strongly favoured over the other
9	One answer is favoured over the other in the highest possible order

The scores are transferred to the matrix A_{ij} the following way: If their score is the same, the entry is 1 for both comparisons. For superior answers, the difference of the two scores plus one is used, for inferior answers its reciprocal is used (cf. Table 10 and Equation 1 for an example). Next, for each matrix A_{ij}, the matrix's principal right eigenvector α_{ij} is computed. For each question q_{ij} in category c_i the square matrix C_i is built from comparing the weights of the questions' importance to the corresponding category in the same way and its eigenvector γ_i is computed.

Table 10. Comparison Table.

Superior	Inferior	Comp.
CSP 1	CSP 2	x
CSP 3	CSP 1	y
CSP 3	CSP 2	z
⋮	⋮	⋮

$$\begin{pmatrix} 1 & x & \frac{1}{z} & \cdots \\ \frac{1}{x} & 1 & \frac{1}{y} & \cdots \\ z & y & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \tag{1}$$

The eigenvectors of the answers' scores α_{ij} are then combined to a matrix A_i. By multiplying A_i with the eigenvector γ_i of the questions' importance, the vector p_i is determined.

$$A_i \cdot \gamma_i = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{J_i} \end{pmatrix} \cdot \gamma_i = p_i, \tag{2}$$

p_i indicates each CSP's priority concerning category c_i.

5.3.2. Computing the overall score

The comparisons of the categories' weights as described in Section 5.2 are used to compute a matrix W analogous to the matrices representing the comparisons of the answers' quality and the questions' importance to a category. We denote its eigenvector with ω. The priorities of the categories p_i are then combined to a matrix P. By multiplying them, the overall priority p is obtained.

$$P \cdot \omega = \begin{pmatrix} p_1 & p_2 & \dots & p_{J_i} \end{pmatrix} \cdot \omega = p, \tag{3}$$

p adds up to 1 and shows the priority of CSPs' answers fulfilling the tenant's requirements.

5.4. Implementation

We have implemented our approach in the R programming language. The classifications and score of the answers and the security categories were stored in a SQL database. In the same database we also imported the CAIQ's answers from the providers. As we already discussed in Section 3.2 this is not a trivial task. From the submitted document formats, it is by far the easiest to export the data from spreadsheets (XLS) compared to text editor files (DOC) or the Portable Document Format (PDF). Referring to the different styles of answering it was easier to extract information from CAIQ version 1.1 if it had two columns or from version 3.0.1 since here answers and comments are separated. In addition, many CSPs changed the number of columns by inserting or deleting columns, and thus we needed to manually select the columns containing the CSPs' answers. Additionally some of the CSPs answered questions in blocks. This resulted either in a listing of answers in the same cell (separated with spaces or line breaks), or by answers prefixed with the control id (CID). Thus, most of the questionnaires' data could only be processed semi-automatically and had to be manually verified.

As described in Section 3.2, some of the CSPs did not provide a clear "yes/no"-answer and only had a verbal answer. To limit the impact of our interpretation of the CSPs' answers, we only processed the questionnaires where there were "yes/no"-answers to all questions or at least to most of them. For the few remaining questions without explicit answer, we derived the answer manually by examining the comment. If no comment was given, we classified the answer as "empty", if it was not possible to conclude whether the comment means, yes, no or not applicable, we classified it as "unclear". Given these restrictions, we ended up with answers from 37 CSPs for version 1.1 and 189 for version 3.0.1 in July 2017.

5.5. Implications for Practice

In this section, we introduced a novel approach to select a secure CSP, showed that it is feasible by a proof of concept implementation. Within the necessary steps some effort is needed for the setup, in particular for classifying and scoring the CSPs' answers to the CAIQ. Since this effort is only needed once, we propose that a cloud broker can offer this as a service. Besides assessing the security requirements, the most difficult task for the tenant is to map the security requirements to the security

categories provided by the cloud broker and to prioritize the requirements' categories. Again, the cloud broker may offer to support the tenant and offer a (paid) service. With the requirements from the tenant and the assessment of the questionnaires, the ranking of the CSPs can be done automatically. As a last step, the tenants may select a CSP, should carefully double-check if the CSP's service level agreements are in line with the questionnaire and in particular include the requirements important to them.

If tenants are on their own terms, they suffer from the amount of different CSPs to consider and from the effort needed to classify all questionnaires. In particular, since we learned during our implementation that the assessment of the questionnaires can only be done semi-automatic, for example, for answers without a comment and many of the questionnaires and their answers have to be processes manually. On the other hand, once the assessment is done, it can be used for multiple selection processes, so a (trusted) third party is necessary. The third party could only be avoided with additional effort either from the tenant's side or from the CSPs' side when they would be required to provide their answers in a specific machine-readable form.

6. Evaluation

In this section we assess different aspects of our approach to cloud provider ranking based on CAIQs. First of all we evaluate how ease is for the tenant to map the security categories to the security requirements and assign a score to the categories. Then, we evaluate the effectiveness of the approach with the respect to correctness of CSP selection. Last, we evaluate the performance of the approach.

Scoring of Security Categories. We wanted to evaluate how ease is for a tenant to perform the only manual step required by our approach to CSP ranking: map their security requirements to security categories and assign a score to the categories. Therefore, we asked to the same participants of the study presented in Section 4 to perform the following task. The participants were requested to map the security requirements of Bank Gemini with a provided list of security categories. For each category they were provided with a definition. Then, the participants had to assign an absolute score from 1 (not important) to 9 (very important) denoting the importance of the security category for Bank Gemini. They had 30 min to complete task and then 5 min to fill in a post task-questionnaire on the perceived ease of use of performing the task. The results of analysis of the post-task questionnaire are summarized in Table 11. Participants believe that the definition of security categories was clear and ease to understand since the mean of the answers is around 2 which corresponds to the answer "Agree". We tested the statistical significance of this result using the one sample Wilcox signed rank test setting the null hypothesis $\mu = 3$, and the significance level $\alpha = 0.05$. The p-value is <0.05 which means that result is statistically significant. Similarly, the participant agree that it was ease to assign a weight to security categories with statistical significance (one sample t-test returned p-value = 0.04069). However, they are not certain (mean of answers is 3) that assigning weights to security categories was ease for the specific case of Bank Gemini scenario. This result, though, is not statistically significant (one sample t-test returned p-value = 0.6733). Therefore, we can conclude the scoring of security categories that a tenant has to perform in our approach does not require too much effort to performed.

Table 11. Scoring of Categories Questionnaire—Descriptive Statistics.

Type	ID	Questions	Mean	Median	sd	*p*-Value
PEOU	Q_1	In general, I found the definition of security categories clear and ease to understand	2.29	2	0.93	6.125×10^{-5}
PEOU	Q_2	I found the assignment of weights to security categories complex and difficult to follow	3.4	4	1.4	0.04069
PEOU	Q_3	For the specific case of the Home Banking Cloud-Based Service it was ease to assign weights to security categories	3.06	3	1.06	0.6733
Overall PEOU			2.91	3	1.13	0.3698

Effectiveness of the Approach. To evaluate the correctness of our approach, we determined if the overall score assigned by our approach to each CSP reflects the level of security provided by the CSPs and thus if our approach leads to select the most secure CSP. For this reason we used the three scenarios from our experiment and additionally created a more complicated test case based on the FIPS200 standard [40]. The more sophisticated example makes use of the full CAIQ version 1.1 (197 questions) and comes up with 75 security categories. As we did for the results produced by the participants of our experiments, we have compared the results produced by our approach for the three scenarios and the additional test case with the results produced by the three experts on the same scenarios. Our approach results were consistent with the results of the experts. Furthermore, the results of the 17 participants who compared two CSPs by answers and comments on 20 questions, are also in accordance to the result of our approach.

Performance. We evaluated the performance of our approach with respect to the number of providers to be compared and the number of questions used from the CAIQ. For that purpose we generated two test cases. The first test case is based on the banking scenario that we used to run the experiment with the students. It consists of 3 security requirements, 20 CAIQ's questions and 5 security categories. The second test case is the one based on the FIPS200 standard and described above (15 security requirements, 197 questions, 75 security categories). We first compared only 2 providers as in the experiment and then compared all the 37 providers in our data set for version 1.1. The tests were run on a laptop with an Intel(R) Core(TM) i7-4550U CPU. Table 12 reports the execution time of our approach. It shows the execution time for ranking the providers (cf. Section 5.3) and the overall execution time, which also includes the time to load some libraries and query the database to fetch the setup information (cf. Sections 5.1 and 2).

Table 12. Performance Time of Our Approach as a Function of the Number of CSP and the Number of Questions.

N° CSP	N° Questions	N° Categories	Ranking	Total
2	20	5	∼0.5 s	<1 s
37	20	5	48 s	50 s
2	197	75	1 min 50 s	<2 min
37	197	75	34 min	<35 min

Our approach takes 35 min to compare and rank all 37 providers from our data based on a full CAIQ version 1.1. This is quite fast compared to our estimation that the participants of our experiment would need 80 min to manually compare only two providers with an even easier scenario. This means that our approach makes it feasible to compare CSPs based on CAIQ's answers. Another result is that as expected the execution time increases with the number of CSPs to be compared, the number of

questions and the number of security categories. This execution time could be further reduced if the ranking of each security category would be run in parallel rather then sequentially.

Feasibility. The setup of this approach requires some effort, which need only to be rendered once. Therefore, it is not feasible for the tenants to do the set-up for a single comparison and ranking. However, if the comparison and ranking is offered as a service by a cloud broker, and thus is used for multiple queries, the set-up share of the effort decreases. Alternatively, a third party such as the Cloud Security Alliance could provide the needed database to the tenants and enable them do to their own comparisons.

Limitations. Since security cannot be measured directly, our approach is based on the assumption that the implementation of the controls defined by the CCM is related to security. Should the CCM's controls fail to cover some aspects or be not related to the security of the CSPs the result of our approach would be effected. Additionally, our approach relies on the assumption that the statements given in the CSPs' self-assessments are correct. The results would be more valuable, if all answers would have been audited by an independent trusted party and certificates were given, but unfortunately as of today this is only the case for a very limited number of CSPs.

Evolving CAIQ versions. While our approach is based on CAIQ version 1.1, it is straight forward to run it on version 3.0.1 respectively version 3.1 also. However, with different versions in use cross version comparisons can only be done with the overlapping common questions. We provide a mapping between the 169 overlapping questions for version 1.1 and 3.0.1 (cf. Section 3.1). If CAIQ version 1.1 will no longer be used or the corresponding providers are not of interest, the mappings of the questions to the security categories may be enhanced to make use of all 295 questions of CAIQ version 3.0.1.

7. Conclusions and Future Work

In this paper we investigated the issues related to CSP selection based on the CSPs' self-assessments and their answers to the Consensus Assessments Initiative Questionnaire (CAIQ). We have discussed first the issues related to processing the CAIQ, namely many CSPs did not follow a standard format to answer the questionnaire and some CSPs did not provide clear answers on which controls they support. Therefore, to facilitate the automatic data processing of CAIQ it would be helpful to have a more standardized data set with unambiguous statements. This could either be a simple text-based format like Comma Separated Variable files (CSV) or an XML-based format like a to be defined Cloud Service Security Description Language or a Multi-Criteria Decision Analysis Modelling Language such as XMCDA [41].

Given these issues we have conducted a controlled experiment with master students to assess whether manually selecting the CSP that best meets the security requirements of a tenant based on the answers to CAIQ is feasible in practice. The experiment revealed that such an approach is not feasible in practice. In fact, the participants took approximately eight minutes to compare two providers based on the answers given to a small subset (20 questions) of the questions included in the CAIQ. If we scale to the full questionnaire which contains around 200 questions, a tenant would take around one and a half hours to compare just two cloud providers.

For this reason, we have proposed an approach that facilitates a tenant in the selection of a provider that best meets its security requirements. The tenant has only to identify the security requirements, rank them, and assign them to predefined security categories. Then the cloud broker uses the Analytic Hierarchy Process to compute a score for each security category based on the answers given by the providers to corresponding questions in the CAIQ. The output is a ranked list based on the weighted overall score for each provider as well as each provider's ranking for each security category. Our approach is quite flexible and allows to be easily customized should the tenant want to change the included scoring, categories or mappings to his own needs.

An preliminary evaluation of the actual efficiency of the approach shows that it takes roughly a minute per provider to compare and rank CSPs based on the full CAIQ.

We are planning to extend our work in four main directions:

Classification of Answers and Questions. The classification of answers and questions are key steps in our approach for selecting CSPs but are also very time consuming. To automatize these steps we will use machine learning techniques to build a text classifier that automatically associates answers and questions to the corresponding class.

Visualization. We focused on providing input for a general CSP selection approach. However, it may be helpful to display the results of the selection process to the tenant. A simple idea could be to build an interface that follows the traffic light metaphor: for each category in the CAIQ it shows in green the categories that satisfy the security requirements of the tenant, in red the one that are not fulfilled and in grey the one that are not relevant with respect to the tenant's security requirements.

Measuring Security. Since security can not be measured directly we focused on experts' judgement to evaluate our approach. It would be interesting to conduct a standardized penetration testing for a couple of the CSPs and match the results with the providers' answers to the CAIQ.

Author Contributions: Conceptualization, F.M., S.P., F.P., and J.J.; methodology, F.M., S.P., F.P.; software, S.P.; validation, S.P., F.P., J.J., and F.M.; investigation, S.P. and F.P.; resources, S.P., F.P., and F.M.; data curation, S.P. and F.P.; writing–original draft preparation, S.P. and F.P.; writing–review and editing, F.M. and J.J.; visualization, S.P.; supervision, F.M. and J.J.; funding acquisition, J.J. and F.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partly funded by the European Union within the projects Seconomics (grant number 285223), ClouDAT (grant number 300267102) and CyberSec4Europe (grant number 830929).

Acknowledgments: We thank Woohyun Shim for fruitful discussions on the economic background of this paper and Katsiaryna Labunets for her help in conducting the experiment.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Example: Application of Our Approach

To illustrate our approach, we show how it is applied to the banking scenario we used in the controlled experiment described in Section 4.

Appendix A.1. Setup

The classification and scoring of answers as described in the previous section meets the fictitious tenant's needs. Since the tenant is interested in security, the corresponding scoring for security mentioned in Section 5.1.1 was chosen.

The mapping of questions to security categories along with their importance to the respective category is shown in Table A1.

Table A1. Weighted Mapping from Questions to Categories.

Number	CID	Weight	Category
1	IS-03.1	7	Privacy
1	IS-03.1	7	Confidentiality
2	IS-03.2	7	Confidentiality
2	IS-03.2	7	Privacy
3	IS-03.3	3	Confidentiality
3	IS-03.3	3	Privacy
4	IS-08.1	9	Confidentiality
5	IS-08.2	9	Confidentiality
6	IS-18.1	9	Key Management
7	IS-18.2	9	Key Management
8	IS-19.1	9	Confidentiality
9	IS-19.2	9	Confidentiality
10	IS-19.3	5	Key Management
11	IS-19.4	7	Key Management
12	IS-22.1	7	Availability
⋮	⋮	⋮	⋮
20	SA-14.1	5	Integrity

Appendix A.2. Tenant's Task

The following security requirements were assumed from the description of the scenario:

- The cloud provider should protect the confidentiality of data during transport and at rest
- The cloud provider should protect the privacy of the accounting data
- The cloud provider should protect the integrity of data during transport and at rest
- The cloud provider should guarantee the availability of accounting applications and data

Based on the requirements the following predefined security categories (weights in brackets) were chosen: Confidentiality (9), Privacy (9), Integrity (9), Availability (9), and Key Management (5).

Appendix A.3. Ranking Providers

Appendix A.3.1. Scoring Security Categories

We report here only the computation of the score for the security category "Key Management" (i = 5). The score for the other categories can be computed in a similar way. For "Key Management" questions 6, 7, 10, and 11 are relevant. The scoring of the providers' answers is shown in Table A2.

Table A2. Scorings of CSPs for Questions Relevant for Key Management

Number	Weight	CSP A	CSP B
6	9	3	4
7	9	3	4
10	5	7	7
11	7	8	7

$$A_{51} = \begin{pmatrix} 1 & 0.5 \\ 2 & 1 \end{pmatrix} \tag{A1}$$

$$A_{53} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{A2}$$

For the first question (number 6, j = 1), the difference between the two scorings is one in favour to CSP B, thus the result for the comparison matrix A_{51} shown in Equation A1. The resulting matrix's

principal right eigenvector is shown in Equation (A3). In the same manner, the weights of the questions are compared, a (4×4)-matrix is built and its resulting eigenvector γ_5 is left multiplied. So the priority p_5 for category c_5 ends in 0.395 versus 0.605 in favour of CSP B.

$$\begin{pmatrix} 0.391 & 0.391 & 0.0675 & 0.151 \end{pmatrix} \begin{pmatrix} 0.333 & 0.667 \\ 0.333 & 0.667 \\ 0.500 & 0.500 \\ 0.667 & 0.333 \end{pmatrix} = \begin{pmatrix} 0.395 & 0.605 \end{pmatrix} \tag{A3}$$

In the same manner, the priorities for the other security categories are determined resulting in P shown in Equation (A4).

Appendix A.3.2. Computing the overall score

From the weights of the categories the eigenvector ω is computed in the same manner. The result of the multiplication $P \cdot \omega$ (see Equation (A4)) delivers the overall score. The result favours CSP B with roughly 60:40 over CSP A regarding the banking scenario. In the supplementary material the result for all 37 providers for all three scenarios is given.

$$\begin{pmatrix} 0.358 & 0.606 & 0.319 & 0.292 & 0.395 \\ 0.642 & 0.394 & 0.681 & 0.708 & 0.605 \end{pmatrix} \begin{pmatrix} 0.238 \\ 0.238 \\ 0.238 \\ 0.238 \\ 0.048 \end{pmatrix} = \begin{pmatrix} 0.394 \\ 0.606 \end{pmatrix} \tag{A4}$$

References

1. NIST Special Publication 800-53—Security and Privacy Controls for Federal Information Systems and Organizations. Available online: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (accessed on 31 March 2020).
2. KPMG. 2014 KPMG Cloud Survey Report. Available online: http://www.kpmginfo.com/EnablingBusinessInTheCloud/downloads/7397-CloudSurvey-Rev1-5-15.pdf#page=4 (accessed on 31 March 2020).
3. Böhme, R. Security Metrics and Security Investment Models. Advances in Information and Computer Security. In Proceedings of the 5th International Workshop on Security, IWSEC 2010, Kobe, Japan, 22–24 November, 2010; Echizen, I., Kunihiro, N., Sasaki, R., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010, Volume 6434, pp. 10–24.
4. Akerlof, G.A. The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *Q. J. Econ.* **1970**, *84*, 488 – 500.
5. Tirole, J. Cognition and Incomplete Contracts. *Am. Econ. Rev.* **2009**, *99*, 265–94, doi:10.1257/aer.99.1.265.
6. Pape, S.; Stankovic, J. An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security. Computer Security. In Proceedings of the ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, ADIoT, Luxembourg, Luxembourg, 26–27 September, 2019; Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., et al, Eds.; Revised Selected Papers; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2019; Volume 11980, pp. 287–306.
7. Anastasi, G.; Carlini, E.; Coppola, M.; Dazzi, P. QBROKAGE: A Genetic Approach for QoS Cloud Brokering. In Proceedings of the 2014 IEEE 7th International Conference on Cloud Computing (CLOUD), Anchorage, AK, USA, 27 June–2 July 2014; pp. 304–311.
8. Ngan, L.D.; Kanagasabai, R. OWL-S Based Semantic Cloud Service Broker. In Proceedings of the 2012 IEEE 19th International Conference on Web Services (ICWS), Honolulu, HI, USA, 24–29 June 2012; pp. 560–567.
9. Sim, K.M. Agent-Based Cloud Computing. *Serv. Comput. IEEE Trans.* **2012**, *5*, 564–577.
10. Wang, P.; Du, X. An Incentive Mechanism for Game-Based QoS-Aware Service Selection. In *Service-Oriented Computing*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8274, pp. 491–498.

11. Karim, R.; Ding, C.; Miri, A. An End-to-End QoS Mapping Approach for Cloud Service Selection. In Proceedings of the 2013 IEEE Ninth World Congress on Services (SERVICES), Santa Clara, CA, USA, 28 June–3 July 2013; pp. 341–348.
12. Sundareswaran, S.; Squicciarini, A.; Lin, D. A Brokerage-Based Approach for Cloud Service Selection. In Proceedings of the 2012 IEEE 5th International Conference on Cloud Computing (CLOUD), Honolulu, HI, USA, 24–29 June 2012; pp. 558–565, doi:10.1109/CLOUD.2012.119.
13. Ghosh, N.; Ghosh, S.; Das, S. SelCSP: A Framework to Facilitate Selection of Cloud Service Providers. *IEEE Trans. Cloud Comput.* **2014**, *3*, 66–79, doi:10.1109/TCC.2014.2328578.
14. Costa, P.; Lourenço, J.; da Silva, M. Evaluating Cloud Services Using a Multiple Criteria Decision Analysis Approach. In *Service-Oriented Computing*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8274, pp. 456–464.
15. Garg, S.; Versteeg, S.; Buyya, R. SMICloud: A Framework for Comparing and Ranking Cloud Services. In Proceedings of the 2011 Fourth IEEE International Conference on Utility and Cloud Computing (UCC), Melbourne, Australia, 5–8 December 2011; pp. 210–218, doi:10.1109/UCC.2011.36.
16. Patiniotakis, I.; Rizou, S.; Verginadis, Y.; Mentzas, G. Managing Imprecise Criteria in Cloud Service Ranking with a Fuzzy Multi-criteria Decision Making Method. In *Service-Oriented and Cloud Computing*; Lau, K.K., Lamersdorf, W., Pimentel, E., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8135, pp. 34–48.
17. Wittern, E.; Kuhlenkamp, J.; Menzel, M. Cloud Service Selection Based on Variability Modeling. In *Service-Oriented Computing*; Liu, C., Ludwig, H., Toumani, F., Yu, Q., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7636, pp. 127–141.
18. Habib, S.M.; Ries, S.; Mühlhäuser, M.; Varikkattu, P. Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source. *Secur. Commun. Netw.* **2014**, *7*, 2185–2200, doi:10.1002/sec.748.
19. Mouratidis, H.; Islam, S.; Kalloniatis, C.; Gritzalis, S. A framework to support selection of cloud providers based on security and privacy requirements. *J. Syst. Softw.* **2013**, *86*, 2276–2293.
20. Akinrolabu, O.; New, S.; Martin, A. CSCCRA: A novel quantitative risk assessment model for cloud service providers. In Proceedings of the European, Mediterranean, and Middle Eastern Conference on Information Systems, Limassol, Cyprus, 4–5 October 2018; pp. 177–184.
21. Mahesh, A.; Suresh, N.; Gupta, M.; Sharman, R. Cloud risk resilience: Investigation of audit practices and technology advances-a technical report. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2020; pp. 1518–1548.
22. Bleikertz, S.; Mastelic, T.; Pape, S.; Pieters, W.; Dimkov, T. Defining the Cloud Battlefield—Supporting Security Assessments by Cloud Customers. In Proceedings of IEEE International Conference on Cloud Engineering (IC2E), San Francisco, CA, USA, 25–27 March 2013; pp. 78–87, doi:10.1109/IC2E.2013.31.
23. Siegel, J.; Perdue, J. Cloud Services Measures for Global Use: The Service Measurement Index (SMI). In Proceedings of the 2012 Annual SRII Global Conference (SRII), San Jose, CA, USA, 24–27 July 2012; pp. 411–415, doi:10.1109/SRII.2012.51.
24. Cloud Services Measurement Initiative Consortium. *Service Measurement Index Version 2.1*; Technical Report; Carnegie Mellon University: Pittsburgh, PA, USA, 2014.
25. Cloud Services Measurement Initiative Consortium. Available online: https://www.iaop.org/Download/Download.aspx?ID=1779&AID=&SSID=&TKN=6a4b939cba11439e9d3a (accessed on 31 March 2020).
26. Saaty, T.L. *Theory and Applications of the Analytic Network Process: Decision Making with Benefits, Opportunities, Costs, and Risks*; RWS Publications: Pittsburgh, PA, USA, 2005.
27. Saaty, T.L. Decision making with the analytic hierarchy process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98.
28. Buckley, J.J. Ranking alternatives using fuzzy numbers. *Fuzzy Sets Syst.* **1985**, *15*, 21–31.
29. Chang, D.Y. Applications of the extent analysis method on fuzzy AHP. *Eur. J. Oper. Res.* **1996**, *95*, 649–655, doi:10.1016/0377-2217(95)00300-2.
30. Cloud Security Alliance. Available online: https://cloudsecurityalliance.org/ (accessed on 31 March 2020).
31. Cloud Security Alliance. Cloud Controls Matrix. v3.0.1. Available online: https://cloudsecurityalliance.org/research/cloud-controls-matrix/ (accessed on 31 March 2020).

32. Cloud Security Alliance. Consensus Assessments Initiative Questionnaire. v3.0.1. Available online: https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/ (accessed on 31 March 2020).
33. Levenshtein, V.I. Binary codes capable of correcting deletions, insertions and reversals. *Sov. Phys. Dokl.* **1966**, *10*, 707–710.
34. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* **1989**, *13*, 319–340.
35. Svahnberg, M.; Aurum, A.; Wohlin, C. Using Students As Subjects - an Empirical Evaluation. ESEM '08. In *Proceedings of the Second ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*; ACM: New York, NY, USA, 2008; pp. 288–290.
36. Höst, M.; Regnell, B.; Wohlin, C. Using Students As Subjects: A Comparative Study of Students and Professionals in Lead-Time Impact Assessment. *Empir. Softw. Eng.* **2000**, *5*, 201–214.
37. Group, N.C.C.S.W.; others. NIST cloud computing security reference architecture. Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
38. Deutsche Telekom. Cloud Broker: Neues Portal von T-Systems lichtet den Cloud-Nebel. Available online: https://www.telekom.com/de/medien/medieninformationen/detail/cloud-broker-neues-portal-von-t-systems-lichtet-den-cloud-nebel-347356 (accessed on 31 March 2020).
39. Schneier, B. Security and compliance. *Secur. Priv. IEEE* **2004**, *2*, doi:10.1109/MSP.2004.22.
40. National Institute of Standards and Technology. Minimum Security Requirements for Federal Information and Information Systems (FIPS 200). Available online: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (accessed on 31 March 2020).
41. Decision Deck. The XMCDA Standard. Available online: http://www.decision-deck.org/xmcda/ (accessed on 31 March 2020).