An Insight into Decisive Factors in Cloud Provider Selection with a Focus on Security

Sebastian Pape[0000−0002−0893−7856] and Jelena Stankovic

Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt, Frankfurt, Germany

Abstract. In the last ten years cloud computing has developed from a buzz word to the new computing paradigm on a global scale. Computing power or storage capacity can be bought and consumed flexibly and on-demand, which opens up new opportunities for cost-saving and data processing. However, it also goes with security concerns as it represents a form of IT outsourcing. We investigate how these concerns manifest as a decisive factor in cloud provider selection by interviews with eight practitioners from German companies. As only a moderate interest is discovered, it is further examined why this is the case. Additionally, we compared the results from a systematic literature survey on cloud security assurance to cloud customers' verification of their providers' security measures. This paper provides a qualitative in-depth examination of companies' attitudes towards security in the cloud. The results of the analysed sample show that security is not necessarily decisive in cloud provider selection. Nevertheless, providers are required to guarantee security and comply. Traditional forms of assurance techniques play a role in assessing cloud providers and verifying their security measures. Moreover, compliance is identified as a strong driver to pursue security and assurance.

Keywords: Cloud Provider Selection · Security Assurance · Interviews

1 Introduction

Cloud Computing has been emerging as the new computing paradigm in the last ten years, enabling consumers to purchase computing power and storage capacity on-demand, conveniently and cost efficiently from specialized providers. Recent studies claim that cloud computing has left the hype phase behind and can already be considered the norm for IT [10].

Besides the potential economic benefits of cloud adoption, it also goes with security concerns as it represents a form of IT outsourcing and exhibits technological peculiarities concerning size, structure and geographical dispersion [35]. With rising adoption rates of cloud services, security concerns remained unchanged or even rose as well. On the other hand, many technical reports also reveal benefits to security in the cloud. It is argued that a cloud provider (CP) enjoys economies of scale in terms of security as well, being able to invest more and thereby achieve

a higher security level on a much larger scale than most client companies would with an in-house data centre [24, 29]. Thus, in either case, one would expect companies to incorporate security into their provider selection and cloud use.

We investigate organizations' practises when selecting a secure CP: *"What role does security play in CP selection?"*. Despite expected "inherent differences in such things as the intended purpose, assets held, legal obligations, exposure to the public, threats faced, and tolerance to risk" between different companies or organizations [29], we expected to verify the importance of security. Under that assumption there would be an incentive for providers to invest in security measures, as potential customers might make their choice based on this characteristic [24]. Moreover, in order to prevent a market for lemons in cloud computing [1], we expected cloud service providers and customers to come up with quality/security assurance methods. Thus, we intended the follow-up question: *How are the providers' security measures verified?* – if security is a selection criteria. Or respectively: *Why is security not considered in CP selection?*

In order to find answers for the underlying research questions a qualitative approach is taken. Practitioners from eight German companies who are associated with CP selection are interviewed and questioned about their companies' provider selection and ways to establish assurance.

2 Related Work

Our research questions can be related to contributions on provider selection, the role of security and security assurance. Security concerns, which are seen as the inhibiting factor of cloud adoption, can be easily related to well researched issues. A bunch of issues is related to technical properties of cloud computing, i.e. the complex architecture [29], multi-tenancy in connection with isolation failures [24, 29], and network vulnerabilities The list of risks also includes the threat of a malicious insider on the CP's side [9], who may abuse his privileges. However, this is a general outsourcing issues due to a loss of governance which can bear dangers for the cloud customers [24]. Therefore, focus in this section is on measures for the CP to assure the security level of its service (corresponding to our extended research question). Assurance is also often necessary from a legal and compliance perspective since most companies underlie a variety of legal obligations, depending on the sector and the type of data they handle.

Since we follow the qualitative content analysis method which is considered hermeneutic and uses deductive examination (cf. Sect. 3.2), an inherent understanding of the topic was necessary in order to interpret the material. Therefore, we conducted a systematic literature survey on security assurance measures.

2.1 Security Assurance

We rely on a survey from Ardagna et al. [7] which covers contributions on security measures and assurance techniques until 2014 and followed their methods and definitions as close as possible to update it for our recent research. Due to space

Table 1. Reviewed Contributions

Assurance	Contribution	Model proposals
SLAs	Lee et al. [40], Luna et al. [44]	Casola et al. [11], Kaaniche et al. [31], Nugraha and Martin [53]
Monitoring	Ismail et al. [27]	Ba et al. [8], Deng et al. [17], Fernando et al. [21], Kanstrén et al. [32], Rios et al. [62], Zhang et al. [71, 72]
Testing		Sotiriadis et al. [67], Stephanow and Khajehmoogahi [68], Tung et al. [70]
Auditing	Ryoo et al. [64]	Ghutugade and Patil [22], Jakhotia et al. [28], Jiang et al. [30], Lins et al. [42, 43], Ma et al. [45], Majumdar et al. [47], Meera and Geethakumari [48], More and Chaudhari [50], Parasuraman et al. [55], Pasquier et al. [56], Rashmi and Sangve [59], Rewadkar and Ghatage [61], Thendral and Valliyammai [69]
Certification	Di Giulio et al. [18], Di Giulio et al. [19], Polash and Shiva [57], Schneider et al. [65]	Anisetti et al. [3, 4, 5], Anisetti et al. [6], Katopodis et al. [33], Krotsiani and Spanoudakis [34], Lins et al. [41], Munoz and Mafia [51]
Other		Henze et al. [25], Mohammed and Pathan [49], Ramokapane et al. [58], Rizvi et al. [63], Sen and Madria [66]

limitations, we can not show the results in detail, but only give a brief summary and list them in Tab. 1.

Almost all contributions reasoned with customers' security concerns as the main inhibiting factor of cloud adoption and that a contribution might provide the needed transparency to resolve that issue. A further justification for new contributions on security assurance were the "special properties" of the cloud which raise new requirements for that topic. Clearly each contribution presented the benefits of its solution, some also covered the challenges, but the drawbacks of certain assurance techniques could only be found in a few contributions from adjacent categories. Certification and security SLAs were presented as the more accessible and convenient measures. In these contributions the customer is clearly involved in the negotiation and provider choice. On the contrary, contributions on auditing, monitoring and testing are mostly technical models or frameworks. It might be difficult to apply these technical models and is it not clear if they are practical in reality and who would implement them.

2.2 CP Selection

In this section qualitative research which determined relevant criteria for CP selection will be discussed. The presented contributions suggest a formal and systematic selection process of a CP and identify security as a relevant criterion. They pursue similar research questions and use a qualitative approach like we do. Nevertheless, their results are narrowed down into compact lists, where security is identified as a requirement but not further discussed. We aim to close this gap, by giving further insight into experts' answers and the role of security.

Repschläger et al. [60] develop a CP classification model with a focus on infrastructure as a service (IaaS). The relevant target dimensions are determined as a result of expert interviews and validated and expanded through a literature

review. The authors conduct five interviews with experts providing different perspectives on common objectives in cloud computing.

Similarly, Hetzenecker et al. [26] derive a model of requirements to support the user in evaluating CPs. Their model consists of six categories with in total 41 requirements. "Information security" is derived as a category with 15 requirements, such as integrity, availability, data disposal, encryption or scalability. All requirements are only presented by a title but not further elaborated.

Lang et al. [39] conduct a Delphi study with 19 decision makers in order to determine relevant selection criteria with a high abstraction level. Security is only identified as a component of the highest rated criterion "functionality" which does not permit to make any statements about the importance of security at all. The authors call for further research to investigate their identified requirements on a lower abstraction level.

2.3 Security, Threat Models and Compliance

Following the CSA top threats to cloud computing [12, 13, 14, 15] as shown in Tab. 2 one can see that most of the threats are related to security and that data breaches soon evolve as the top threat. In an extensive survery Kumar and Goyal [37] map the threats also to requirements, vulnerabilities and countermeasures. Alhenaki et al. [2] investigate some of the threats mentioned by the CSA, do also a mapping to countermeasures and additionally identify the relevant cloud service models (Saas, PaaS, IaaS) which are concerned by the threats. Mahesh et al. [46] elaborate aspects of cloud computing that need special attention, i.e. by audits. They also list most prominent frameworks and working groups that are widely accepted across industries and describe some approaches from industry practices.

3 Methodology

In this section we briefly describe how the interviews were conducted and how the data was analysed.

3.1 Sample Selection and Conduction of Interviews

We conducted semi-structured interviews with practitioners engaged in the selection of a CP, e.g. with the role of network or cloud architect or a management position. With semi-structured interviews we were able to get answers to a set of predetermined questions but were still flexible enough to include spontaneous questions arising from the discussion with the practitioners.

Since we could not offer financial compensation, we tried to get in touch with relevant practitioners at the Cloud Expo Europe 2018 and completed the set of interviewees with contacts from our personal network. The process of the invitation and the interviews was as follows: When inviting the participants, we already included the information that we were looking for experts in the field of cloud computing to find out which criteria were considered when choosing a CP

Table 2. Top Threats to Cloud Computing identified by CSA [12, 13, 14, 15]

#	2010	2013	2016	2019
1	Abuse and Nefarious Use of Cloud Computing	Data Breaches	Data Breaches	Data Breaches
2	Insecure Application Programming Interfaces	Data Loss	Weak Identity, Credential and Access Management	Misconfiguration and Inadequate Change Control
3	Malicious Insiders	Account Hijacking	Insecure APIs	Lack of Cloud Security Architecture and Strategy
4	Shared Technology Vulnerabilities	Insecure APIs	System and Application Vulnerabilities	Insufficient Identity, Credential, Access and Key Management
5	Data Loss/Leakage	Denial of Service	Account Hijacking	Account Hijacking
6	Account, Service & Traffic Hijacking	Malicious Insiders	Malicious Insiders	Insider Threat
7	Unknown Risk Profile	Abuse of Cloud Services	Advanced Persistent Threats (APTs)	Insecure Interfaces and APIs
8	-	Insufficient Due Diligence	Data Loss	Weak Control Plane
9	-	Shared Technology Issues	Insufficient Due Diligence	Metastructure and Aplistructure Failures
10	-	-	Abuse and Nefarious Use of Cloud Services	Limited Cloud Usage Visibility
11	-	-	Denial of Service	Abuse and Nefarious Use of Cloud Services
12	-	-	Shared Technology Issues	-

and which requirements were imposed on the provider. Ideally, the participants should either be involved in such a decision.In order to be able to verify security as a criterion without revealing it beforehand, the research focus on security was not given in the invitation.

We first conducted a pilot interview to test and validate the interview guidelines. Respondents Ra and Rb were from the financial sector and related security closely to compliance, i.e. regulations imposed by the national supervisory authority BaFin. Therefore, the remaining interviews were further enriched by the question whether there was the intrinsic motivation or personal responsibility to select a secure provider. Afterwards, from October to December 2018, we interviewed eight respondents (cf. Tab. 3) face to face and in German. In order to maintain continuity all interviews were conducted by the same interviewer. Interviews had an average duration of around 37 minutes.

Due to space limitations, we describe the interview guideline only briefly. After the warm-up, the second block of questions addressed the provider selection. According to the research questions if respondents claimed to consider security when selecting a CP they were asked about possible assurance techniques their company used. In case security was not mentioned, the respondents were asked about the importance of security. Although security was not among the first criteria mentioned, it was present in most discussions. Eventually this lead to covering both sides of the decision tree in most of the interviews. Finally, the transparency on the cloud market was addressed to generate additional ideas for possible improvements to a non-transparent market.

Table 3. Respondents' profiles

Respondents	**Relation to the cloud**	**Sector**	**Employees**	**Expert's position**
Ra / Rb	User	Financial Services	>1000	Infrastructure Specialists
R1	Consultant	IT Consulting	>100000	Cloud Advisory Sen. Manager
R2	Provider	IT	<50	CEO
R3	User	Financial Services	>10000	Network Architect
R4	User	Energy Supply	>10000	Cloud Architect
R5	User	Automotive	>100000	Solution Architect
R6	User	Financial Services	>1000	IT Security Manager
R7	User	Metal Processing	>1000	Project Manager (IT Infrastr.)
R8	User	Fintech	<50	CTO

3.2 Data Analysis

The interviews were transcribed word by word and analyzed with MAXQDA following the qualitative content analysis method from Kuckartz [36], since it suited the data collected in the semi-structured interviews and allowed to analyze the data with regard to the research questions. To get well acquainted with the material, in the first phase of analysis each interview was summarized and the peculiarities of the given answers were noted. Next, master-codes were developed and tested on the first three interviews before coding the whole material. These codes were generated mostly deductively out of the interview questions. For instance, the codes "Provider Selection" and "Assurance Techniques" were rather straight forward, as these where the main research questions. The result of this phase was a list of master-codes. After coding the whole material with the master-codes, all passages coded with the same master-code were grouped and reread. At this point the aim was to differentiate the master-codes by inductively deriving sub-codes for each master-code. While proceeding from one interview to the next, the generated sub-codes were revised and sorted. The final product was a list of sub-codes which differentiated the master-codes. A sample of the derived coding can be found in Tab. 4.

4 Interview Results

The interviews and the data analysis were conducted with regard to the initial research questions. This resulted in a coding frame of five master-codes from which three address our research questions directly. In the next subsections, we briefly show the results of the role of security in CP selection, reasons for a moderate interest in security, and the verification of providers' security measures. Since in most of the interviews compliance was strongly connected with security, we also investigated the role of the General Data Protection Regulation (GDPR).

Table 4. Coding Frame for Assurance Techniques

Assurance Techniques	Respondents talk about how they establish security assurance.
Certification	Respondents talk about certification. The topic is either which ones they consider important or the advantages and drawbacks of certificates.
Audits	Respondents audit their providers or talk about auditing. Statements are also included if they are about financial auditing.
Contractual Agreements	User and provider agree contractually on certain requirements the provider has to fulfill or on the right of the user to audit.
Data Center Visits	Respondents place a value on being allowed to visit the provider's data center.
Documentation	Respondents place a value on checking the providers' documentation on processes or technical measures.
Penetration Tests	The respondents run penetration tests as a mean of assurance.
Cloud Risk Process	Companies' own process for risk assessment.
Questionnaire on Security Measures	A company uses a questionnaire (comparable to CSA's CAIQ) in order to obtain information from a provider.
Skepticism	Respondents express skepticism towards some assurance techniques, or the sense of assurance in general.

4.1 The Role of Security in CP Selection

The respondents were asked which criteria or requirements they considered when choosing a CP, instead of directly being asked about the role of security. Analogously, the master code "Provider Selection" was extracted from the material with several security related and unrelated sub-codes. The results were selection criteria, of which the ones unrelated to security will only be presented shortly. The most discussed selection criteria were costs (addressed by 5 respondents), size of provider (4) followed by ease of use (3).

Trust: In three interviews the providers' image came up in relation to their trustworthiness, which revealed divided opinions. R1 and R3 provided statements indicating that the image could serve as a proxy for security considerations. *R1: In our region Google did not manage to gain ground, which in my opinion can be contributed to the fact that we are a little bit more sensitive with regard to security and privacy than other countries. So many people shy away when they hear the name "Google" considering them a "data collector".* Similarly, R3 stated that he would consider any large provider except for the Chinese Alibaba cloud. R2 provided the contrary provider's view on this idea. His small company was able to benefit from the image of the local German cloud in the beginning.

Compliance: Non surprisingly, need for security because of compliance appeared referring to regulation authorities, e.g. BaFin or BNetzA (R4, R6, R8).

Availability: Also a great value was placed on the availability of services (R1, R2, R4, R8) in particular over different time zones and with a certain force. Additionally, the statement of R4 even exceeded availability by considering business continuity of the provider to be able to plan for the future.

Confidentiality: The respondents R3 and R4 considered security for the sake of confidentiality of their users' data. *B3: It is about customer data which is located somewhere and one cannot be sure who has access to it. Of course one would like to use cloud services and algorithms to generate an added value out of this data. But on the other hand, one wants to protect the customer from an unauthorized party to gain access to it. I think this is is incredibly difficult.* This

statement was the only one in the sample expressing a concern for confidentiality apart from any business goals.

Besides selection criteria, several respondents provided insights on how their organisations selected their current CPs. These additionally provided circumstances matter for understanding the provider selection in its context.

Multiple providers: Among others, it was stressed that current environments consisted of more than one main provider for the sake of independence, availability and freedom of choice (R3, R4). The decision which project or task was done with which provider was a per case decision, depending on the properties of the data and the provider (R4).

Hierarchy: R7 and R5 revealed that the provider decision was made on a higher hierarchical level. Particularly in the case of R7 a provider selection was unnecessary as the company had a strategic partnership with Microsoft.

Convenience: Several respondents admitted that the choice for a CP was partly made by chance, e.g. simply chose a convenient provider to make the first steps in the cloud (R1, R5), because a developer already had some experience (R4) or the company had a voucher (R8). In individual cases these first steps of conveniently testing out a new provider even contradicted corporate requirements and constituted a shadow IT. Despite these tendencies, a security analysis was done retrospectively (R4, R5). Even if it was done retrospectively, the analysis was not only formal but could have changed the decision. *R5: Basically the cloud risk process could have stopped the decision for the product.*

4.2 Reasons for Moderate Interest in Security

The respondents could not be asked why security was only of moderate interest, as security was sooner or later addressed in all the discussions. Nevertheless, most of the answers could be related to "coping with risk". The related topics came up when the respondents were asked about the role of trust or whether they had possible concerns about confidentiality. Most respondents agreed that these concerns do exist but revealed different "coping mechanisms".

Mitigation: Two ways of mitigating the risk raised by respondents were the choice of a large provider and a national or EU-located data centre. In four interviews the location of a data centre came up as a signal of a trustworthy or preferable provider (R2, R3, R4, R5). The assumption, that especially large providers are secure and trustworthy was found in all the interviews except the one with R3. Most respondents argued that large providers invested more in security and thereby also provided a higher level of security than even possible in the own company, which is in line with academic findings [23, 38]. Another benefit was stressed by R6 and R8, namely that large companies were also more likely to cover high compensations than small providers in case of a breach.

Responsibility: R2, R5, R7 and R8 agreed that security was not only the responsibility of the CP, but rather a shared one. R2 stressed the differences compared to traditional technologies with regard to responsibility. *R2: Who bears which responsibility often changes in the cloud compared to traditional methods.[...] Before, I either used to run an in-house data centre or I outsourced it.* R5 stressed

the importance of creating awareness in-house for the new technology and its specific risks.

Encryption: Four respondents reported encryption as a mean to secure the cloud. R6 and R8 attached great importance on encrypting their outsourced data and R1 and R2 reported on means of encryption implemented by their clients. Additionally, R2 pointed out the potential drawbacks for the cloud customer. *R2: When we provide the infrastructure only, encryption is mostly in the hands of the customer. But then he has to manage the keys, which represents an additional complexity he has to handle.*

Data Criticality: In addition, some users saw security relatively to the criticality of data they placed into the cloud. R1 and R6 stated that business critical-data was preferably not outsourced at all. *R1: In my opinion, it will always be the case that for a certain part the companies say: "These are my crown jewels, which I don't give away. No matter how much I trust a provider, I want to have these with me".*

Trust: As the opposite side of mitigation, ideas were raised resonating with trust towards the provider. Maybe the most prominent statement to this topic was given by R1: *I believe that many give their providers a few laurels in advance. "Okay they do this on such a large scale and I either I do not trust them per se. In this case I address encryption and other topics. Or as I said, I give them laurels in advance and say, yes this is going to work out"*, assuming that many users trust their providers without any proof. R2, R4, R5 and R8 expressed their belief that the incentives for providers were set in such a way that they cannot afford to make mistakes with customers' data.

Personal Responsibility: R2 tried to explain the popularity of Amazon with the "IBM Effect". *R2: Well I can rely on them (AWS), at least at most times. And when there is a service failure, it applies to everyone and one can say: "Yes, you know it, AWS just had an outage". So it's the IBM effect: "No one ever got fired for buying IBM", applies to AWS nowadays.* R3 agreed with this idea. Finally, independently of mitigation or trust one question had to be included in light of the given answers concerning the importance of security. Throughout some discussions one could have gotten the impression that some companies simply avoided being held accountable in case of a data breach. Therefore the respondents were asked whether there was a personal responsibility or even an intrinsic motivation to pursue security conscientiously. Consequently, the code "Personal Responsibility" was covered with six respondents.

Compliance: The resulting discussions with R1 and R2 were leaned on the fulfillment of GDPR and compliance requirements and both respondents revealed the belief that the choice of a secure provider is rather extrinsically motivated by the need to comply. They also agreed that the regulating authorities still have not drawn any consequences but most likely would do so in the future in order to set an example. *R1: [...] I believe that many (companies) still wait until the first penalties are issued, as surprisingly it (GDPR) did not have that many impact yet. [...] I think the first time something happens and jurisdiction is drawn, and a company really has to pay for it, many others will have a second awakening.* R4

and R6 agreed that compliance is decisive for the final choice. However, according to R4 intrinsic motivation is individual and depends on the employee's training. *R4: Well it depends on who is dealing with the topic. As I already said, the energy sector has very high security requirements, so if a classic energy economist deals with it, then security and compliance are in his blood. [...] If it is a developer, he may not care. He only asks where to put the data, but does not really think about it himself.* However, R4 adds that in recent years the awareness has risen among all the employees.

4.3 Verification of Providers' Security Measures

The first part of the interviews showed that although security was not the top criterion when selecting a CP, it was present as a requirement. For this reason, it could not be directly asked how the respondents compared different providers with regard to security beforehand, but it could be discussed whether they verified the security levels of their CPs.

Certification: The probably most discussed assurance technique in this sample was certification. According to R1, R2, R4, R6 and R8 two kinds of certification seemed to be of importance when a provider was checked. This was either certification after the ISO norm 27001 or the C5 by BSI (R1, R2, R4, R6), a German governmental agency, which among others incorporates the ISO norm and is combined with an audit. R1 expressed his doubts about C5 being attractive to providers who want to achieve global standardization, as it was a German norm. R4 and R6 agreed that certification in general provided a solid basis for trusting a provider, as for one thing certification institutions could be considered credible and for the other their certification process was very demanding. R2 as well stressed the convenience of certificates but later on also warned of misunderstandings, as one always had to look closely at the coverage. *R2: Another important thing is that certificates are often misunderstood. For instance a 9001 certificate can be done for different domains of my company. I could only certify the administration and in that case a production- or data center is not covered at all.* Moreover, R2's small company could not be certified as the formalization of processes was not possible in the dynamic environment of a start-up. These aspects were also picked up by R8 who criticized exactly that certification was for the most parts focused on processes on paper, which in his view would not provide real security.

Audits: Another assurance technique discussed was external auditing, although it has to be said that the audits most respondents considered were not of technical but rather a financial nature. R6 and R7 for instance stated to have sent public accountants or financial auditors to their providers who apparently only in the broadest sense verified provider security. R1 admitted that he did not know of anyone who really audited their CPs and predicted it rather as a future trend after the clients had made some experiences in the cloud. R7 and R8 stressed the benefits of a third party audit, namely that an expert was checking the status of a system and giving advice on how to improve it, which was according to R8 an advantage compared to certificates. While R4 doubted

the competence of some auditors, R8 pointed out the conflict of interest. *R8: Exactly, it depends on what kind of auditor you get. You can entrust someone who issues an affirmation for you: "Audit accomplished", or you can entrust someone who works conscientiously. The only problem is that the ones who work conscientiously, are often those who are not well received and afterwards have trouble reselling. There is a slight conflict of interest.*

Contracts: It was often discussed in connection to assurance that respondents had contractual agreements with their providers (R4 and R6). R6 added the possibility to contractually seal where data is located and processed. R2 pointed out that contractual agreements were often not only an option but a requirement in light of GDPR, while R4 and R6 gave the important reason for having a contractual agreement, namely that in case of non-fulfillment a compensation was ensured. R1, R2 and R4 mentioned the possibility to contractually include the users' right to visit the data center in person. According to R2 such a clause may be necessary or important to a client, who handles personal data. Nevertheless, the respondents admitted that in reality such a visit hardly ever happened. Additionally, R2 doubted the sense of sending company representatives to visit a data center. *R2: If someone like you or me went there, what would we be supposed to see? If the door is not open somewhere or a cable hanging loosely, we would have no idea how secure this is and whether it is in accordance to the norm.* R1 added that the providers tried to avoid such visits as they considered the interior of their data centre as a company secret. Additionally, checking technical documentation or documentation of processes was found in the interviews (R4, R6, R7).

Tests: Additionally, R4 and R6 talked about security tests as a mean of assurance. *R6: That means that for a cloud service we will not check whether it is externally attackable, as most data centres must have tested this already for about five-, six-, seven-, eight hundred times. What we check is whether the access point we have to the data centre is secure enough.* R4 also stressed that the tests were not done on the CPs' side but on the final application, which was supposed to run in the cloud or as a hybrid application. Both respondents pointed out some drawbacks of penetration-testing, first the costliness and second that such tests could only be run for known cases.

Two respondents stood out with their companies' specific assurance techniques. R5 reported of his companies' own cloud risk process which helped evaluating a provider with regard to the risk he poses to the company and its data. The process incorporated some of the already presented techniques, like demanding a certification and contractually sealing requirements, but more than this, it was a spreadsheet for assessing the likeliness of scenarios and finally presenting the risk imposed by a provider. Finally, the management was in charge of deciding whether this risk was acceptable or not. The other individual measure was taken by R4's company, which had designed their own questionnaire for CPs comparable to the CAIQ by the CSA.

Finally, besides all the collected assurance techniques it has to be mentioned that several respondents also expressed scepticism when talking about assurance.

According to R3 there was no gain from SLAs and contracts, as even if there was a written agreement one had to suffer in case of a data breach in terms of data loss. R4 pointed out the drawback of a third party audit, by telling his own experience with auditors who believed him anything he told them. R7 had doubts about assurance in general and pointed out how the need to control or verify everything although one had outsourced brought unnecessary costliness. Similarly, R8 criticized that certificates do not show real security.

4.4 Compliance and the General Data Protection Regulation

Due to the previous answers, we also elaborate how the GDPR influenced the decisions and to what extent interviewees reported about German and European cloud services which do not transfer data outside of the European Union.

GDPR: According to R2 and R6, a result of the GDPR is that more attention is turned to data protection. R2 claims that the GDPR allows to ensure technical and organisational measures by SLAs more easily.

R1 and R2 agree that since so far data protection authorities have not punished companies by a fine, most companies will assume the first cases will hit large companies and wait for that. R2 was more concerned about written warnings from competitors. R7 reported that his company's data security officer answered to a request about using cloud services that an agreement of the parent company (in Great Britain) with the cloud provider is seen as valid for all subsidiary companies. In contrast, R4 reported that the regulation requires data centres in the EU, which still did not work out for them, because of US employees with access to the stored data. However, they use a CP in Switzerland for non business critical data.

Localisation of CPs: Statements on the localisation of CPs were ambivalent. On the one hand, R3 was concerned about US industrial espionage facilitated by war on terror laws and thus demands a German/European solution with all components (software, hardware) built and run in Germany/EU. This is in line with the report of a "Robin Hood" bonus for a localised offer (R2).

On the other hand R1 and R2 report that at the beginning localisation seemed important, but then lost importance due to data centres in Germany (from the large CPs) and due to observations of other companies seemingly running their cloud services GDPR-compliant with non-EU CPs. An additional argument was that the advantages of localisation can not compensate higher costs (R3, R4, R7), missing features (R1, R2) or development tools (R3) for the German version, customers in the US (R1), and missing trust in the continuity of the service (R4). Many interviewees (R1, R2, R3, R4, R7) were referring to the "German cloud", a cooperation between Telekom and Microsoft which was ended last year [1].

[1] `https://heise.de/-4152650`

5 Discussion

Role of security: With regard to the original question on the role of security in cloud provider selection the collected findings are ambiguous. Selection criteria like usability and costs were expressed straightforwardly and matched the findings of the related work [26, 60]. Security however, was never the first answer the respondents extensively engaged in. Neither could they provide concrete security requirements comparable to those found in the related contributions. On the other hand, security as a requirement was present in all the discussions. Moreover, availability and in rare cases confidentiality could be extracted as goals. Two respondents revealed that although security had not been a selection criterion, it was considered in retrospect in some cases, where the companies analysed the services after having tested them first. Moreover, the findings from this sample challenge the idea of a systematic provider selection suggested in related works. In this sample it was rarely the case that providers were compared and evaluated in advance with regard to certain criteria.

Moderate interest in Security: Some respondents assessed the situation and acted in accordance to the mitigation measures proposed in cloud organizations' technical reports. For instance, one could identify the awareness of the separation of duties and the willingness to employ encryption on the user side. These users were aware that security in the cloud was not only the cloud provider's duty and took own responsibility. On the other hand, namely the capability of a provider to grant compensations speaks however again for a financial interest rather than an intrinsic motivation to establish security. The initial assumption that the requirement on security is extrinsically motivated by compliance was clearly supported by the respondents' answers on personal responsibility. The answers revealed as well a different side to the client provider relationship, which was a great amount of trust towards the cloud provider and the acceptance of risk to a certain extent. The idea that an "IBM effect" exists when choosing Amazon's services indicates that this could be a way for decision makers to be exonerated from responsibility.

Security Assurance: Overall, the respondents revealed to rely on certification, audits, contractual agreements and testing as common means of assurance. Besides those assurance techniques, two respondents presented own company-specific methods. The results from this sample show that except for C5 which is a cloud-specific certificate and audit, the companies rather rely on traditional forms of assurance than cloud-specific ones. Especially contractual agreements are considered a convenient method in order to establish compliance and guarantee for a compensation in case of non-fulfillment. Surprisingly, contractually agreed measures like data center visits are not often undertaken. These findings are one more indicator that security and also assurance are overshadowed by compliance, but that at the same time regulation may miss out on establishing real and not only paper-based assurance.

In comparison to the findings from academic literature cloud-specific assurance techniques seemed to have not really thrived in practice. Certification which was most present in the literature review was similarly well accepted among the

practitioners as a convenient assurance technique. Testing in terms of application security was also present in both, literature and interviews. However, it is striking but not surprising that neither monitoring nor auditing, which offered many cloud-specific frameworks in literature, were present among the respondents. Contractual agreements could be compared to security SLAs with regard to how they work, except that there are no actual metrics agreed upon but rules.

5.1 Threats to Validity and Limitations

One of the major challenges of conducting the interviews turned out to be finding the right respondents. The ideal respondent given the research questions would have been someone in a C-Level position, who was involved in cloud adoption and knowledgeable about the processes in IT and security. Such persons were difficult to reach or to find time to schedule a face to face interview. In the current sample, respondents from the financial industry are a bit overrepresented and it would have been beneficial to have more respondents from small and medium enterprises. In particular, R8 answered from a perspective of a start-up and could contribute some new ideas. Thus, the interviews should be considered as a first insight and be extended by further interviews with representatives from small- and middle sized companies. Most respondents eventually talked about infrastructure- or platform providers, most likely because in the case of Software-as-a-Service one would rather talk about service- than provider selection.

6 Conclusion

Previous research identified security as a requirement considered by CP customers. Our sample indicates that security may not always be a selection criterion and neither the most decisive one. If considered in the CP selection, then mostly in terms of availability and for the sake of compliance. Especially the focus on compliance it not surprising as it has been observed in other sectors as well [16, 54]. Nevertheless, it is certainly a requirement companies have, which manifests itself in cloud use. This is indicated by retrospective analysis and considerations of multiple providers.

CP Selection Process: In our sample we could rarely find any elaborated process of eliciting requirements and then coming to a rational decision which CP to select. Instead, CP were chosen based on vouchers, by chance (just pick on CP for 'testing', but then stick with it), by the management because of established relationships, or because of previous experience from a developer. Even more, some companies make use of many CPs in an unstructured way, e.g. each department decides by its own. Another pattern we could identify was that companies often try to 'first get into the cloud' and then optimise costs and sometimes security (lift and shift) or try to sort out the collection of different CPs. Further research would be desired to investigate why the methodology proposed by research seems to be rarely used in practise.

For that purpose the different roles in the requirements / decision making process should be investigated in detail and elaborated at which step the relevant methodologies from research were not considered and why.

Assurance: The respondents reported on using more than one assurance technique, combined models from the literature were not present at all. Additionally, they saw flaws in the existing assurance techniques and may not even be acquainted with possible cloud-specific assurance. Thus, the noteworthy finding of this comparison is a divergence between the assurance methods adopted in practice and the cloud-specific ones proposed in literature. It can be speculated whether some academic approaches to assurance have never exceeded their theoretical approach or if they were not able to gain ground in practice yet.

Company Size: Although the results uncover many dimensions and patterns of cloud security, they are not complete. As mentioned earlier, no saturation of interviews could be reached among small and unregulated companies. In contrast, large regulated companies were well represented and most likely contributed to a strong focus on compliance in this analysis. Future work could examine on a larger scale whether and how companies have incorporated security into their provider selection and in particular investigate commonalities and differences between smaller and larger companies.

Big CPs vs. Localisation: It seems that the big CPs are in general trusted by the companies and the idea of a German cloud failed. Companies are trying to setup a compliant way to work with the big CPs. However, one interviewee was concerned about industrial espionage and strongly voted for a European or German CP with all components made in the EU. Further research should unfold the different dimensions of trust, and also investigate to which extent regulations or agreements as the EU–US Privacy Shield influence it.

Gaps Between Research and Practise: In the requirement elicitation and decision making process and in the use of assurance technologies there seems to be a gap between research and practise. This gap is something which seems to be quite common in a lot of areas [52]. Further work should investigate whether this is just a typical finding and already existing ideas can be applied to bridge it [20] or if it is a context specific problem and new ideas are needed.

Bibliography

[1] Akerlof, G.A.: The market for "lemons": Quality uncertainty and the market mechanism. In: Uncertainty in economics, pp. 235–251. Elsevier (1978)

[2] Alhenaki, L., Alwatban, A., Alahmri, B., Alarifi, N.: Security in cloud computing: A survey. International Journal of Computer Science and Information Security (IJCSIS) 17(4) (2019)

[3] Anisetti, M., Ardagna, C.A., Damiani, E.: A certification-based trust model for autonomic cloud computing systems. In: 2014 International Conference on Cloud and Autonomic Computing. pp. 212–219 (2014)

[4] Anisetti, M., Ardagna, C.A., Damiani, E.: A test-based incremental security certification scheme for cloud-based systems. In: 2015 IEEE International Conference on Services Computing. pp. 736–741 (2015)

[5] Anisetti, M., Ardagna, C.A., Damiani, E., Gaudenzi, F., Veca, R.: Toward security and performance certification of open stack. In: 2015 IEEE 8th International Conference on Cloud Computing. pp. 564–571 (2015)
[6] Anisetti, M., Ardagna, C.A., Gaudenzi, F., Damiani, E.: A certification framework for cloud-based services. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing. pp. 440–447. SAC '16, ACM (2016)
[7] Ardagna, C.A., Asal, R., Damiani, E., Vu, Q.H.: From security to assurance in the cloud: A survey. ACM Comput. Surv. 48(1), 2:1–2:50 (2015)
[8] Ba, H., Zhou, H., Bai, S., Ren, J., Wang, Z., Ci, L.: jMonAtt: Integrity monitoring and attestation of jvm-based applications in cloud computing. In: ICISCE. pp. 419–423 (2017)
[9] Bleikertz, S., Mastelic, T., Pape, S., Pieters, W., Dimkov, T.: Defining the cloud battlefield – supporting security assessments by cloud customers. In: IC2E. pp. 78–87 (2013)
[10] Briggs, B., Lamar, K., Kark, K., Shaikh, A.: Manifesting legacy: Looking beyond the digital era. 2018 global CIO survey. Tech. rep., Deloitte (2018)
[11] Casola, V., Benedictis, A.D., Rak, M., Villano, U.: SLA-based secure cloud application development: The SPECS framework. In: SYNASC. pp. 337–344 (2015)
[12] CSA: Top threats to cloud computing v1.0. Tech. rep., Cloud Security Alliance (2010), https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
[13] CSA: The notorious nine: Cloud computing top threats in 2013. Tech. rep., Cloud Security Alliance (2013), https://cloudsecurityalliance.org/download/artifacts/the-notorious-nine-cloud-computing-top-threats-in-2013/
[14] CSA: The treacherous 12 - cloud computing top threats in 2016. Tech. rep., Cloud Security Alliance (2016), https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
[15] CSA: Top threats to cloud computing the egregious 11. Tech. rep., Cloud Security Alliance (2019), https://cloudsecurityalliance.org/download/artifacts/top-threats-to-cloud-computing-egregious-eleven/
[16] Dax, J., Ivan, A., Ley, B., Pape, S., Pipek, V., Rannenberg, K., Schmitz, C., Sekulla, A.: IT security status of German energy providers. https://arxiv.org/abs/1709.01254 (2017), https://arxiv.org/abs/1709.01254
[17] Deng, L., Liu, P., Xu, J., Chen, P., Zeng, Q.: Dancing with wolves: Towards practical event-driven VMM monitoring. In: Proceedings of the 13th ACM SIGPLAN/SIGOPS International Conference on VEE. pp. 83–96. ACM (2017)
[18] Di Giulio, C., Kamhoua, C., Campbell, R.H., Sprabery, R., Kwiat, K., Bashir, M.N.: IT security and privacy standards in comparison: Improving FedRAMP authorization for cloud service providers. In: CCGrid. pp. 1090–1099 (2017)
[19] Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R.H., Bashir, M.N.: Cloud standards in comparison: Are new security frameworks improving cloud security? In: CLOUD. pp. 50–57 (2017)
[20] Ferguson, J.: Bridging the gap between research and practice. Knowledge management for development journal 1(3), 46–54 (2005)
[21] Fernando, R., Ranchal, R., Bhargava, B., Angin, P.: A monitoring approach for policy enforcement in cloud services. In: CLOUD. pp. 600–607 (2017)
[22] Ghutugade, K.B., Patil, G.A.: Privacy preserving auditing for shared data in cloud. In: CAST. pp. 300–305 (2016)

[23] Gupta, P., Seetharaman, A., Raj, J.R.: The usage and adoption of cloud computing by small and medium businesses. International Journal of Information Management 33(5), 861–874 (2013)
[24] Haeberlen, T., Dupré, L.: Cloud Computing - Benefits, Risks and Recommendations For Information Security. Tech. rep., ENISA (2012)
[25] Henze, M., Matzutt, R., Hiller, J., Mühmer, E., Ziegeldorf, J.H., v. d. Giet, J., Wehrle, K.: Practical data compliance for cloud storage. In: 2017 IEEE International Conference on Cloud Engineering (IC2E). pp. 252–258 (2017)
[26] Hetzenecker, J., Kammerer, S., Amberg, M., Zeiler, V.: Anforderungen an cloud computing anbieter. In: MKWI (2012)
[27] Ismail, U.M., Islam, S., Islam, S.: Towards cloud security monitoring: A case study. In: Cybersecurity and Cyberforensics Conference (CCC). pp. 8–14 (2016)
[28] Jakhotia, K., Bhosale, R., Lingam, C.: Novel architecture for enabling proof of retrievability using aes algorithm. In: ICCMC. pp. 388–393 (2017)
[29] Jansen, W., Grance, T.: Sp 800-144. guidelines on security and privacy in public cloud computing. Tech. rep., NIST (2011)
[30] Jiang, T., Chen, X., Ma, J.: Public integrity auditing for shared dynamic cloud data with group user revocation. IEEE Transactions on Computers 65(8), 2363–2373 (2016)
[31] Kaaniche, N., Mohamed, M., Laurent, M., Ludwig, H.: Security SLA based monitoring in clouds. In: IEEE EDGE. pp. 90–97 (2017)
[32] Kanstrén, T., Lehtonen, S., Savola, R., Kukkohovi, H., Hätönen, K.: Architecture for high confidence cloud security monitoring. In: IC2E. pp. 195–200 (2015)
[33] Katopodis, S., Spanoudakis, G., Mahbub, K.: Towards hybrid cloud service certification models. In: IEEE Int. Conf. on Services Computing. pp. 394–399 (2014)
[34] Krotsiani, M., Spanoudakis, G.: Continuous certification of non-repudiation in cloud storage services. In: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. pp. 921–928 (2014)
[35] Krutz, R.L., Vines, R.D.: Cloud security: a comprehensive guide to secure cloud computing. Wiley (2010)
[36] Kuckartz, U.: Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung. Beltz Juventa (2016)
[37] Kumar, R., Goyal, R.: On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review 33, 1–48 (2019)
[38] Lacity, M.C., Reynolds, P.: Cloud services practices for small and medium-sized enterprises. MIS Quarterly Executive 13(1) (2014)
[39] Lang, M., Wiesche, M., Krcmar, H.: What Are the Most Important Criteria for Cloud Service Provider Selection? A Delphi Study. In: ECIS (2016)
[40] Lee, C., Kavi, K.M., Paul, R.A., Gomathisankaran, M.: Ontology of secure service level agreement. In: 2015 IEEE 16th International Symposium on High Assurance Systems Engineering. pp. 166–172 (2015)
[41] Lins, S., Grochol, P., Schneider, S., Sunyaev, A.: Dynamic certification of cloud services: Trust, but verify! IEEE Security Privacy 14(2), 66–71 (2016)
[42] Lins, S., Schneider, S., Sunyaev, A.: Trust is good, control is better: Creating secure clouds by continuous auditing. IEEE Transactions on Cloud Computing 6(3), 890–903 (2018)
[43] Lins, S., Thiebes, S., Schneider, S., Sunyaev, A.: What is really going on at your cloud service provider? creating trustworthy certifications by continuous auditing. In: 48th HICSS. pp. 5352–5361 (2015)

[44] Luna, J., Suri, N., Iorga, M., Karmel, A.: Leveraging the potential of cloud security service-level agreements through standards. IEEE Cloud Computing 2(3), 32–40 (2015)
[45] Ma, M., Weber, J., van den Berg, J.: Secure public-auditing cloud storage enabling data dynamics in the standard model. In: DIPDMWC. pp. 170–175 (2016)
[46] Mahesh, A., Suresh, N., Gupta, M., Sharman, R.: Cloud risk resilience: Investigation of audit practices and technology advances-a technical report. International Journal of Risk and Contingency Management (IJRCM) 8(2), 66–92 (2019)
[47] Majumdar, S., Madi, T., Wang, Y., Jarraya, Y., Pourzandi, M., Wang, L., Debbabi, M.: User-level runtime security auditing for the cloud. IEEE Transactions on Information Forensics and Security 13(5), 1185–1199 (2018)
[48] Meera, G., Geethakumari, G.: A provenance auditing framework for cloud computing systems. In: SPICES. pp. 1–5 (2015)
[49] Mohammed, M.M.Z.E., Pathan, A.K.: International center for monitoring cloud computing providers (ICMCCP) for ensuring trusted clouds. In: IEEE 11th Int. Conf. on Ubiquitous Intelligence and Its Associated Workshops. pp. 571–576 (2014)
[50] More, S.S., Chaudhari, S.S.: Secure and efficient public auditing scheme for cloud storage. In: CAST. pp. 439–444 (2016)
[51] Munoz, A., Mafia, A.: Software and hardware certification techniques in a combined certification model. In: SECRYPT. pp. 1–6 (2014)
[52] Norman, D.A.: The research-practice gap: The need for translational developers. Interactions 17(4), 9–12 (2010)
[53] Nugraha, Y., Martin, A.: Towards the classification of confidentiality capabilities in trustworthy service level agreements. In: IC2E. pp. 304–310 (2017)
[54] Pape, S., Pipek, V., Rannenberg, K., Schmitz, C., Sekulla, A., Terhaag, F.: Stand zur IT-Sicherheit deutscher Stromnetzbetreiber (2018), http://dokumentix.ub.uni-siegen.de/opus/volltexte/2018/1394/
[55] Parasuraman, K., Srinivasababu, P., Angelin, S.R., Devi, T.A.M.: Secured document management through a third party auditor scheme in cloud computing. In: ICECCE. pp. 109–118 (2014)
[56] Pasquier, T.F.J.., Singh, J., Bacon, J., Eyers, D.: Information flow audit for paas clouds. In: IEEE IC2E. pp. 42–51 (2016)
[57] Polash, F., Shiva, S.: Building trust in cloud: Service certification challenges and approaches. In: 9th Int. Conf. on Complex, Intelligent, and Software Intensive Systems. pp. 187–191 (2015)
[58] Ramokapane, K.M., Rashid, A., Such, J.M.: Assured deletion in the cloud: Requirements, challenges and future directions. In: CCSW. pp. 97–108. ACM (2016)
[59] Rashmi, R.P., Sangve, S.M.: Public auditing system: Improved remote data possession checking protocol for secure cloud storage. In: iCATccT. pp. 75–80 (2015)
[60] Repschläger, J., Wind, S., Zarnekow, R., Turowski, K.: Developing a Cloud Provider Selection Model. In: EMISA (2011)
[61] Rewadkar, D.N., Ghatage, S.Y.: Cloud storage system enabling secure privacy preserving third party audit. In: ICCICCT. pp. 695–699 (2014)
[62] Rios, E., Mallouli, W., Rak, M., Casola, V., Ortiz, A.M.: SLA-driven monitoring of multi-cloud application components using the MUSA framework. In: IEEE 36th ICDCSW. pp. 55–60 (2016)
[63] Rizvi, S.S., Bolish, T.A., Pfeffer, III, J.R.: Security evaluation of cloud service providers using third party auditors. In: Second International Conference on Internet of Things, Data and Cloud Computing. pp. 106:1–106:6 (2017)
[64] Ryoo, J., Rizvi, S., Aiken, W., Kissell, J.: Cloud security auditing: Challenges and emerging approaches. IEEE Security Privacy 12(6), 68–74 (2014)

[65] Schneider, S., Lansing, J., Gao, F., Sunyaev, A.: A taxonomic perspective on certification schemes: Development of a taxonomy for cloud service certification criteria. In: HICSS. pp. 4998–5007 (2014)
[66] Sen, A., Madria, S.: Data analysis of cloud security alliance's security, trust & assurance registry. In: ICDCN. pp. 42:1–42:10. ACM (2018)
[67] Sotiriadis, S., Lehmets, A., Petrakis, E.G.M., Bessis, N.: Unit and integration testing of modular cloud services. In: AINA. pp. 1116–1123 (2017)
[68] Stephanow, P., Khajehmoogahi, K.: Towards continuous security certification of software-as-a-service applications using web application testing techniques. In: AINA. pp. 931–938 (2017)
[69] Thendral, G., Valliyammai, C.: Dynamic auditing and updating services in cloud storage. In: Int. Conf. on Recent Trends in Information Technology. pp. 1–6 (2014)
[70] Tung, Y., Lin, C., Shan, H.: Test as a service: A framework for web security taas service in cloud environment. In: 2014 IEEE 8th International Symposium on Service Oriented System Engineering. pp. 212–217 (2014)
[71] Zhang, H., Manzoor, S., Suri, N.: Monitoring path discovery for supporting indirect monitoring of cloud services. In: IEEE IC2E. pp. 274–277 (2018)
[72] Zhang, H., Trapero, R., Luna, J., Suri, N.: deQAM: A dependency based indirect monitoring approach for cloud services. In: IEEE SCC. pp. 27–34 (2017)

All references have been last checked on Apr 10th, 2019.