Accountability Requirements for the Cloud

Martin Gilje Jaatun*†, Inger Anne Tøndel†, Nils Brede Moe†,
Daniela Soares Cruzes†, Karin Bernsmed† and Børge Haugset†
*University of Stavanger, NO-4036 Stavanger, Norway
†SINTEF Digital, NO-7465 Trondheim, Norway

***Abstract*—In order to be responsible stewards of other people's data, cloud providers must be accountable for their data handling practices. The potential long provider chains in cloud computing introduces additional accountability challenges, and this paper examines requirements which must be fulfilled to achieve an accountability-based approach.**

I. Introduction

The emergence of cloud computing is providing new opportunities for business development. Unfortunately, it is exposing both customers and providers to new challenges (e.g., in terms of data management), which require a shift in the way Information and Communication Technology (ICT) is deployed in business contexts. Cloud customers and providers are exposed to various problems. The increasing amount of data and resources requires new mechanisms that enable cost-effective management while guaranteeing critical features such as security and privacy. Challenges arise from the redistribution of responsibilities across cloud supply chains. Different stakeholders relate to and contribute to data governance in the cloud. Moving data from centralized and proprietary systems to the cloud involves a shift in responsibilities across organizational boundaries. Although security and privacy threats affect any form of ICT (including cloud computing), moving to the cloud changes risk fundamentals (e.g., likelihood of occurrence and severity of impact) as well as risk perceptions of such threats. On the one hand, it is necessary to understand any limitations of technologies (e.g., security mechanisms) within cloud ecosystems. On the other hand, it is necessary to identify new mechanisms to enhance trustworthiness in the cloud Moving to the cloud involves a change in control, a change in trust and security boundaries, and maybe also a change in legal requirements [1].

Accountability for a provider can be seen as "doing the right thing"; being a responsible steward of other people's information. An accountable provider defines how it manages information, monitors how it acts (to verify that it does what it says it does), remedies any discrepancies between the definition of what should occur and what is actually occurring, and explains and justifies any action [2]. Accountability can thus be seen as an important prerequisite for trust in online (cloud) services.

Many of the privacy and security challenges we face in the cloud are just variants of similar challenges in traditional computer networks [1], but one new aspect is the concept of long provider chains. In traditional outsourcing, the customer only has to relate to one provider where data processing and storage is performed in a single data center. In the cloud, a service provider will often re-use (parts of) another provider's service, who in turn uses services from a third provider, and so on. The most well-known example of this is Dropbox, which initially had no infrastructure of its own, but used processing and storage services from Amazon Web Services.

Cloud and IT service providers should act as responsible stewards for the data of their customers and users. However, the current absence of accountability frameworks for distributed IT services makes it difficult for users to understand, influence and determine how their service providers honor their obligations. Motivated by the current absence of accountability frameworks in the cloud, the A4Cloud project has developed tools and technologies that enable accountability for how personal and business confidential information is used in the cloud, taking into account the chain of responsibilities that needs to be built throughout the cloud service supply network.

This paper is based on an elicitation effort that has involved more than 300 stakeholders who contributed to the identification of detailed accountability requirements. This has allowed the project to gather requirements from different stakeholders, ranging from individual cloud customers to organizational cloud customers and cloud providers, additionally including data protection commissioners, auditors, consumer groups, trade bodies and SME organizations. The requirements elicitation workshops highlighted how stakeholders understand accountability and what their priorities and concerns are about data protection in the cloud.

The remainder of this paper is organised as follows: In Section II we present relevant background. We present the method employed in eliciting and analyzing requirements in Section III, and the results in Section IV. We discuss our finding in Section V, and conclude in Section VI.

II. Background

We define accountability [3] for an organization as follows:

> Accountability consists of accepting responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed (including onward transfer to and from third parties). It involves the commitment to norms, explaining and demonstrating compliance to stakeholders and remedying any failure to act properly.

The A4Cloud project has analyzed and extended the different cloud roles for the actors in a cloud ecosystem. We have

extended the well-known NIST cloud supply chain taxonomy [4] to create the following cloud accountability taxonomy composed of 7 main roles:

1) *Cloud Subject*
2) *Cloud Customer*
3) *Cloud Provider*
4) *Cloud Carrier*
5) *Cloud Broker*
6) *Cloud Auditor*
7) *Cloud Supervisory Authority*

III. Method

The primary measure of success of a software system is the degree to which it meets the purpose for which it was intended [5]. Broadly speaking, requirements engineering (RE) is the process of discovering that purpose, by identifying stakeholders and their needs, and documenting these in a form that is amenable to analysis, communication, and subsequent implementation. There are a number of inherent difficulties in this process [6]. First, stakeholders may be numerous and distributed. Second, the stakeholders' goals may vary and conflict, depending on their perspectives of the environment in which they work and the tasks they wish to accomplish. Finally, the stakeholders' goals may not be explicit or may be difficult to articulate, and, inevitably, satisfaction of these goals may be constrained by a variety of factors outside their control. For addressing these challenges we have been following an approach based on requirements by collaboration [6]. The approach focuses on meeting two essential needs: efficiently defining user requirements while building positive, productive working relationships. We have engaged with a broad base of relevant stakeholders for elicitation purposes using different methodologies to elicit, refine and validate the requirements for the project.

A. The elicitation themes and events

Stakeholders were engaged through a set of elicitation events, structured by four themes, as illustrated in Table I. Theme T1 was concerned with identifying stakeholders' notion of accountability and elicited initial accountability requirements. Theme T2 dealt with risk perception, covering how emerging threats in the cloud are perceived by stakeholders and the emerging relationships between accountability, risk and trust. The third theme (T3) addressed different stakeholders' view and expectation of accountability mechanisms, and studied different stakeholders' operational experiences and expectations about accountability in the cloud in relation to prototype tools offering such accountability mechanisms. Finally, the fourth theme (T4) exposed stakeholders to metrics for accountability and incident response management in a cloud computing setting. Furthermore, a small number of external legal experts provided input on high-level descriptions of the key accountability mechanisms [7], and gave feedback on how they expected associated tools to be received by cloud customers and providers.

B. Method of data collection in the workshops

The T1 workshop relied on Open Space Technology [8], [9] and World Café [10]. Open Space is recommended for complex situations involving diverse participants and the need for quick decision making. The technique is highly flexible, because the topics discussed are entirely determined by the participants. The participants are encouraged to suggest topics that are regarded as the most important issues, which make Open Space an inventive, creative, and productive method well suited for eliciting initial stakeholder requirements. First, the workshop facilitator presented the Open Space question: *What would make you or the people you represent more comfortable in the cloud?* The stakeholders were then invited to suggest topics to discuss during the open space. Six of the suggested topics were discussed (three sessions, two parallels). The stakeholder who suggested a topic was responsible for taking notes from the discussion using a given template and flip-charts. Researchers acted as observers during the discussion.

In the second part of the T1 workshop the discussions were arranged according to the world café methodology, with the goal of getting feedback on the business use cases being developed in the project. First, three use cases were presented; health care services in the cloud, cloud-based ERP software, and multi tenant cloud. The presentation of the business use cases ended with the question *what are the accountability issues in the business case?* For each table and associated use case, one researcher acted as host. Stakeholders were encouraged to visit the table they found most interesting. The three hosts facilitated three discussions in parallel. Everyone participated in two discussions of 35 minutes.

Based on participants' expressed interest in more technical detail, the T2 workshop provided a more structured agenda. Data collection was based on the focus group research technique [11], [12], where a main advantage is the explicit use of group interactions to produce data and insight that would be less accessible without these interactions. Group discussions provide direct evidence about similarities and differences in the participant's opinions and experience. It is possible to collect large and rich amounts of data on a given topic, and focus groups serves as a quick way to obtain information on emerging phenomena. The T2 workshop consisted of four different sessions covering the following topics: security threats to cloud computing; risks related to each of the use cases from the T1 workshop; risk and trust modeling in cloud computing; and accountability-based approach to risk and trust modeling. Each focus group was moderated by one researcher that was supported by at least one observer. Three of the sessions were complemented by short questionnaires distributed at the end of the session.

The T3 events used accountability tools as a vehicle for stimulating discussions on accountability expectations and what stakeholders would like to experience (operationally) in the cloud. The following tools were used:

- *Data Track:* a transparency tool that displays an overview of a subject's data disclosures to different providers and

TABLE I
OVERVIEW OF THE FOUR THEMES AND EVENTS

Theme	Goal	Method	Participants	Results
T1	Accountability relationships and requirements	Open Space Technology; World Café	7 participants; authorities, providers, customer, vendor	57 accountability relationships, later refined into 53 requirements
T2	Risk perception; relationship between accountability, risk and trust	Focus groups	20 participants; authorities, providers, customers, vendors, academia	15 requirements
T3	Expectations about accountability; experience with accountability mechanisms	Four workshops (different actors and tools; discussions and questionnaires); interviews	About 90 participants (30 subjects, 20 customers, 40 providers)	62 requirements
T4	Previously uncovered topics: metrics; incident response; opinions of legal experts	Workshops (discussions and questionnaires); email survey and informal conversations	About 60 participants: academia and IT professionals	23 requirements

allows subjects to access data collected about them stored at the provider, etc. [13]

- *Cloud Offerings Advisory Tool (COAT):* a tool to support selection of cloud services based on customer preferences [14]

The T3 workshop with *cloud providers* included presentations of cloud initiatives and research on accountability, including the COAT tool, and the presentations were followed by round table discussions within focus groups.

The T3 workshops with *cloud subjects* and cloud customers had a common structure, where data collection consisted of recorded discussions and questionnaires. Discussions were centered on the tools (Data Track [13] for cloud subjects, COAT [14] for cloud customers), and after a short presentation of the tool, the participants were divided into groups and were asked to discuss the tool for 20 minutes. The discussion was guided by questions that covered their willingness to use the tool, what they liked/did not like about the tool, feedback on the tool concept and suggestions for improvements. At the end of the workshops, participants handed in a post-questionnaire where they assessed their agreement on usability as well as accomplishment of project goals, and had the opportunity to provide free-text comments about the tool. For cloud subjects there was an additional pre-questionnaire aimed to understand the participants' behavior in the cloud, and to rate their trust in selected services as well as how sensitive (private) different personal data items are for the participants.

In addition to the workshops, Skype interviews were performed with cloud customers to understand more about the importance of transparency for customers, and verify and refine transparency requirements elicited in previous workshops. Questions [15] covered expectations on what information should be provided by cloud providers (in general and on security problems), factors that can increase customers' trust in the security of data in the cloud, and the extent to which customers want to be involved in decision making with the provider, in addition to their opinions about the previously elicited requirements.

T4 covered important gaps not resolved by the previous elicitation events, focusing on accountability metrics, incident management and additional legal input. Two workshops were arranged: the Malaga workshop on metrics for accountability and the Trondheim workshop on incident response. The *Malaga workshop* explained to the audience the need for measuring accountability and outlined how this can be done based on a metrics catalog created in the project. We then distributed a questionnaire where the participants' overall opinion about the metrics catalog was captured by a Likert scale. In the *Trondheim workshop* on incident response the data collection comprised a questionnaire distributed after a presentation. The questionnaire comprised three main sections. The first two sections asked the participants to assess their agreements with statements on requirements elicited from the CSA Guide [16] and from Grobauer and Schreck [17] respectively. The last section asked the participants to freely write other comments (extra requirements, improvements, suggestions, recommendations, justification of their answers) about the requirements for incident response. The workshops were supplemented by an email consultation survey from Queen Mary University London, attempting to gauge how legal experts would react to the Guiding Light requirements [7]; this last activity did not result in new requirements, but provided useful input for the ongoing work in the project.

C. Data analysis

Several researchers were involved in data analysis of the various workshops and requirements elicitation activities. All minutes, observation notes and questionnaires were analyzed, with the goal of identifying requirements. In T1 the goal was to identify cloud relationships, but these were later translated into requirements. For the interviews with cloud customers (T3), recommended steps for thematic synthesis [18] were followed.

D. Requirements repository

The stakeholder elicitation workshops resulted in a large number of requirements. In order to categorize them, to classify them with respect to what actor(s) they apply to, to preserve consistency, to simplify future management and to make all the requirements accessible to all the project partners, we created a requirements repository. This ensured that requirements could be effectively communicated to work packages that need them, particularly when these requirements were updated or changed during the course of the project. Furthermore, the repository served as the collection point for requirements created by other workpackages in the project.

It is important to note here that the requirements in each elicitation activity must be internally consistent, but no attempt has been made to enforce coherence between requirements in different activities; this is a consequence of how the requirements have been gathered and analyzed. The Excel sheets do not contain raw text, but the result of extracting individual requirements from (e.g.) workshop minutes. However, the versioning scheme in the requirements repository caters for an evolution of requirements as they are refined by validation activities in the development work packages.

IV. Results

In total 289 requirements have been identified [19]. 153 of these requirements stem from the elicitation events, while the rest of the requirements have been identified as part of other research activities in the A4Cloud project. 51 of the requirements are directly targeted towards tools or languages developed as part of the A4Cloud project.

In the following, we provide an overview of which requirements target which cloud actors, as well as give an overview of important points from the various discussions of the role of accountability in the cloud.

A. Requirements that target cloud providers

The majority of the requirements that target cloud actors (that is, not tools) are directed towards cloud providers. To further illustrate that the main security responsibility is put on cloud providers, 54 of the 57 accountability relationships identified in T1 concerned cloud provider responsibilities towards other actors, with 41 of these towards cloud customers (the rest towards auditors, regulators and data protection authorities).

The requirements make it clear that cloud providers are responsible for the way data is handled. All accountability practices [7] are covered in the requirements, so that cloud providers are expected to define what they do, monitor how they act, remedy any discrepancies between what should occur and what is actually occurring, and explain and justify any action. A wide variety of technical and organisational measures are expected for protecting the data, throughout its lifetime. This also implies documenting the security and being able to provide evidence, e.g. that the documented measures are actually carried out. In particular, the cloud provider is expected to inform cloud customers about relevant aspects of the service and the data management practices, in a way that helps customers to understand the implications. Customers should also be empowered, so that they are able to take action regarding the security of their data and access information on vulnerabilities and incidents. Central is the concept of consent, and providers need mechanisms to deal with customer consents in an efficient manner. Monitoring mechanisms should be in place so that the status of different data is known, e.g. where the data is stored, and audits should be supported and regularly performed. The cloud provider should also respond to any incidents in an effective manner, inform customers about incidents affecting their data, and support cloud customers in their incident management activities. For incident management, but also all other matters, cloud providers shall comply with legal requirements.

B. Requirements that target cloud subjects or cloud customers

As of now, it seems data subjects are not completely aware of what being in the cloud means. For at least some of the cloud subjects participating in T3 events, the cloud was just another web service or "online", and they were happy to learn more about the cloud. None of the identified requirements are directly targeted towards cloud subjects, but there are a few requirements that more indirectly put some responsibility on cloud subjects. One example is a requirements that states that cloud subject (and likewise cloud customers) may be consulted by the cloud provider on how they want their personal data to be handled in the cloud. Then cloud subjects can be said to be responsible for giving input to the cloud provider on data handling preferences, if given the opportunity to do so. The same can be said with requirements regarding reporting of data breaches, sending of complaints and providing reviews of cloud providers. These are not direct requirements on cloud subjects, but when implemented, requirements that provide opportunities for the cloud subjects to contribute to improved accountability in the provider chain.

Cloud customers, on the other hand, are given more responsibilities, especially for taking measures to select accountable cloud providers and follow up on contract terms. Still, less than 20 requirements directly target cloud customers. Selection of cloud providers is expected to be risk based, but as was discussed by T2 workshop participants, it is challenging to understand and assess risk in a cloud environment. The analysis of the different use cases showed that even when it is relatively straightforward to identify the assets, it is far more ambitious to evaluate related risks and the impact of the loss, dissemination or misuse of these assets. Different factors contribute to this difficulty:

- *Technical:* The variety and the amount of data collected make it difficult to understand the scope of the exposure and the usages after multi-source aggregation and complex data mining
- *Lack of transparency:* While some data are de facto already sold, it is nearly impossible for a citizen to know who the buyers are and how sound are the anonymization techniques are (if any), equally incidents are barely reported and unlikely linked to the data sources

- *Legal:* The coexistence of a "borderless" cloud and multiple jurisdiction frameworks may impeach users to make use of their rights or may expose the companies involved in the data processing chain

While these concerns were pre-existing the cloud era (e.g. IT outsourcing), the growth of data collection, the capacity of data processing and the broader attack perimeter make them more acute. Despite these challenges of assessing risk for customers, the workshop participants were however clear that customers, and not cloud providers, are the ones that are responsible for performing risk assessments.

Risk analysis is one mean to help educate users of cloud computing to better perceive the risks. With improved risk perception they can make more informed decisions when moving their data and services to the cloud. So, despite the current obstacles for obtaining meaningful risk analysis results, the participants nevertheless state that risk analysis is essential. Requirements to provide information that support cloud customers to perform risk analysis is put on cloud providers. Additionally, risk assessments can be supported by certifications and accreditation mechanisms.

C. Requirements that target cloud brokers

Only eight requirements target cloud brokers. These are related to:

- *Interpretation and negotiation of policy:* It is expected that cloud brokers should be able to negotiate policy requirements with both cloud providers and cloud customers, and be able to interpret and possibly enhance policy terms, as well as report subsets of policies.
- *Evidence of non-data aggregation:* It is expected that cloud brokers are able to provide evidence that data are not aggregated, or alternatively, that there is effective data segregation in place
- *Relay messages:* Brokers are expected to relay messages between cloud providers and cloud customers, i.e. demonstration requests, remediation requests, data breach notifications and compliance and performance indicators.

D. Requirements that target cloud auditors or cloud supervisory authorities

Both cloud auditors and cloud supervisory authorities are considered to have responsibilities for clarifying requirements to cloud providers, in particular they should clarify compliance with respect to extraterritorial legislative requirements and provide a list of certifications required. The cloud auditor is then the actor performing audits and certifications. In that work they are expected to monitor accountability levels of cloud providers and make sure that collection of implicitly collected data is made transparent. It is additionally expected that audits are provided in a standard way across the chain of service so that it is possible to visualise differences between SLAs along the cloud supply chain.

Cloud supervisory authorities, are not directly involved in making audits, but have the possibility to accept or reject authorizations of providers. They additionally have an important role in handling complaints from cloud subject, receiving data breach notifications from cloud subjects and customers and request actions to remediate compliance failures. Both actors are considered to be responsible to societal institutions, e.g. regulators.

E. Requirements not directly targeted towards a particular cloud actor

In addition to the 51 requirements that consider specific tools or languages that is developed as part of A4Cloud, a number of the other requirements are not directly targeted towards particular cloud actors, but concern the need for better methods or the need to consider the whole provider chain. Requirements for methods are provided when it comes to settings management, communication between cloud provider and customer, risk monitoring and assessments, remediation, observability and transparency, and assessment of cloud provider accountability. Requirements may concern user-friendliness, on-the-fly settings management, ability to perform impact assessments and test claims made by providers, indicators, and ways to model risk and trust-relationships in cloud provider chains. Additionally, a number of requirements concern the need for language support, in particular for information considered important to cloud subjects, cloud customers and cloud supervisory authorities or cloud auditors (or other regulators). Tools and methods should consider large corporations and organizations, ability to quickly take into account any changes (e.g. in legal requirements and practices), the need to support different user groups (including novice users) and the need for independent tools, so that there are no hidden criteria that favor particular cloud providers.

The need for new methods and tools are grounded in key challenges on dealing with provider chains. This was discussed in several of the workshops, also related to main challenges for trusting the cloud (T2):

- not knowing where the resources were moved in the cloud
- the potential lack of accountability when buying from a provider that purchases services from another provider, not knowing who is responsible for what
- the risk of trusting people with a conflict of interest

This led to the following statement by one WP2 participant: "one should carefully think through what data to put in the cloud." Uncertainties additionally stem from the insufficient transparency and the conflicting laws among countries.

To meet these challenges, there are requirements that consider the provider chain in more general terms. The need for a legal framework to steer proper handling of information in the cloud is covered by the requirements. This legal framework then needs to be taken into account in the binding and enforceable written data governance policies and procedures in service provision chains. All parties in the provision chain are expected to perform ongoing risk assessments. The need for clearly allocated responsibilities in the provider chain is pointed out, in particular who is liable to the cloud customer, who is responsible for executive oversight and responsibility

for data privacy and protection, and who is responsible for responding to inquiries, complaints and data protection breaches.

F. The role of accountability

In addition to identifying requirements, the workshops included more general discussions. In the following we provide important insights from discussions on the role of accountability, both how accountability relates to risk and trust, and how accountability fits with the cloud business model.

1) Unclear relationship between accountability, risk and trust: The workshops uncovered uncertainties on the effects of accountability on risk and trust. In particular the effects on risk was unclear. This topic was covered in most detail in T2, where twelve of the workshop participants responded to a small questionnaire with ten statements describing to this relationship. From the responses one can observe that the participants do not have an agreement among themselves in their answers. In some questions, their answers are dispersed throughout the scale almost equally. The responders think that accountability may not always mitigate risks and accountability may not always support interactions in the cloud. In the same way, one can see from the data subjects in T3 that they, although they generally were very positive to the Data Track tool, were neutral or disagreed to the the statements that Data Track would "substantially increase users' trust in cloud services" and that it would "substantially reduce the number of serious security problems". Cloud customers (T3) however mentioned accountability-related functionality as something that would increase their trust that data is secure, in particular they mentioned upfront transparency, community discussions, costumer awareness, way out, reputation, encryption, data processor agreements and location.

Follow up discussions in T2 on the relationship between accountability, risk and trust, led to a converging understanding that the relationships between accountability and risk and accountability and trust are different (or of a different nature).

- *Accountability and risk:* Although accountability addresses risk, it is yet unclear how. The relationship between accountability and risk is a generalized one. That is, it is believed that accountability addresses emergent risks in cloud ecosystems. However, stakeholders had difficulties to figure out in which way. Stakeholders questioned whether accountability addresses risk (by modifying risk profiles in terms of likelihood of occurrence or severity of impact) or changes risk perception of emerging threats in cloud ecosystems.
- *Accountability and trust:* The relationship between accountability and trust seem to be more context-dependent than the one with risk. Accountability helps to make trust decisions, however accountability itself seems to be necessary but not sufficient for (or implying unconditionally) trust. Accountability will help to make trust decisions. A critical aspect of trust decisions seem to be related to the evidence provided to stakeholders. Therefore, accountability (in particular transparency) plays an important role in trust decisions and supports trustworthiness (in particular based on accountability evidence).

Additionally, it was pointed out by cloud providers (T3) that the definition of accountability will be different depending on whom you ask. Enterprises will give different answers about accountability from what the customer will say, and legal people will have different understandings than more technical people.

2) Accountability and the cloud business model: From the discussions of various accountability tools with lawyers (T4), it is clear that they see the main beneficiaries of the tools to be (a) cloud customers, who furthermore are (b) consumers or SMEs. Little benefit to cloud providers is foreseen. It is also clear that practicing lawyers think that the main obstacles to adoption of the tools will be the potential commercial disadvantages to providers, and the possible increase in their legal risks. Easy visibility of failures would be a commercial disadvantage against providers who are not providing such visibility. Still, as pointed out by providers (T3), the adoption of accountability mechanisms would push towards a standardization of cloud offerings. This would enable comparisons across different cloud providers and ease the adoption from cloud customers. This is the reason why accountability is perceived as a potential market enabler for the cloud. The cloud providers are clear that the business models of accountability mechanisms must be clarified in order to facilitate their deployments in operational environments. Related to this, the following two inputs from the workshops are highly relevant. First, it was stated by providers that the promise of cloud is 'something magic' (that is, 'not transparent'). Second, not all cloud customers are willing to pay for accountability. Based on the discussions among cloud customers in the T3 event, explicit consent for data operations is seen as an overkill by some customers, and though custom-made security levels are a "nice to have feature", customers understand that it costs and that not all providers will offer that. Additionally, many customers do not want highest security as default; this may be a reflection on a "you get what you pay for" attitude, and thus preferring the cheapest version as default.

Cloud customers' demand for cloud accountability can additionally be influenced by a lack of understanding about the risk associated with the cloud. The T2 event discussed the lack of understanding of the cloud among cloud customers, and its implications for cloud services adoption and risk management. A representative from the bank domain said: "Those that make purchasing decisions in banks do not understand cloud. The promise of cloud seems very large to the executives - they understand the benefits, but not the risks. One bank executive recently stated: "our core services will be in the cloud in 3-4 years" - but this attracted critical attention from regulatory body." Another participant said that "the main threat for Cloud Computing is the lack of education and supporting materials for security officers. Security officers need to talk to CEOs why to move to the cloud. However, since they lack knowledge they will not opt for going to the cloud and form an obstacle for cloud adoption."

V. Discussion

Accountability is clearly not a one-way concept; all actors in the cloud ecosystem have to cooperate to make it work. Organisations that consume cloud services, the end-users of the services, the data subjects whose data is being processed by the services, as well as the organisations that audit, certify and regulate the services, all of these have important roles to play. To illustrate, the customer need to find out if the cloud provider can deliver and can be trusted, but then the cloud provider need to demonstrate somehow that they can take care of the data. Standards bodies or auditors can support this by saying "this is the list of certifications you need to look for".

Since the majority of the requirements concern the cloud provider, it is relevant to consider whether cloud providers have the necessary motivation to adhere to these requirements. Many requirements can be considered quite strict and, as was pointed out by legal experts (T4), they will probably hamper business if following them in full.

Customer demand, audit requirements and legal requirements may motivate more accountable behavior. But as of now, the positive effect of accountability has not been demonstrated. This does however not mean that the strive for accountable cloud services should stop. There is a need for more research on understanding the positive and negative effects of accountability on the business of cloud providers, as well what aspects of accountability should get priority. The workshops described in this paper, and the resulting requirements, provide a broad view of what accountability can mean in practice for different actors in the cloud ecosystem. Some requirements are likely to be more important than others, both when it comes to being accountable and regarding cost/benefit. Improved knowledge on this can support providers that see the value of accountability in deciding where to focus their effort. For requirements that are essential for accountability, but come at a potentially high cost, it should be investigated how to reduce the potential negative impact of the accountability practice.

Motivating individual cloud providers to demonstrate their accountability is of course essential, but there is additionally a need to consider the whole provider chain. Researchers can have an important role in providing tools and methods that adequately deal with accountability in provider chains. This is covered by the requirements, in addition to requirements on legal frameworks etc. In their current form, these requirements are not however directly targeting a particular cloud actor. Cloud brokers, cloud auditors and cloud supervisory authority may have a potentially important role related to provider chain overview and motivating the adoption of accountability mechanisms. This potential role need to be better understood.

A. The requirements

Most of the requirements in the repository have been specified at a high level. The main reason is that the requirements should be applicable to a broad spectrum of cloud services models that involve the processing of personal and/or business confidential data. By avoiding specifying detailed requirements on how, for example, the different SaaS, PaaS and IaaS services are implemented and operated we can make sure that sure that the requirements cover also other types of service models that may appear. This is in line with the scope of the A4Cloud project, whose focus is not only on today's cloud services but also future IT services. The exception is the requirements for accountability mechanisms, which are detailed enough to be (more or less) directly applied to the technologies and tools that the project is developing. In fact, some of these requirements have already been implemented in the project tools.

Most of the requirements in the repository originate from perceived challenges that the stakeholders associate with existing cloud services, and thus represent features that stakeholders would like to see in a future accountable cloud ecosystem. However, there are exceptions, for example, "R211 - The Cloud Subject (Cloud Customer) shall be made aware of the data processing and sharing practices of the Cloud Provider" is something that almost all providers already do (as they provide privacy policies that specify this).

B. The requirements elicitation method

Requirements elicitation is concerned with different objectives. On the one hand, elicitation aims to understand the problem space (how can we characterize the problem we are dealing with?) and to identify specific requirements. Addressing this objective tends to give rise to generic requirements charactering the problem we are concerned with. On the other hand, elicitation aims also to fit specific solutions (aligned with such requirements and addressing the characterized problem) to specific user domains. Addressing such objective highlights requirements drawn from stakeholders domains. Our aim of involving stakeholders in workshops was to gather a broad spectrum of requirements, good practices and risks related to the cloud eco-system covering the diverse range of geographical (including legal) constraints and challenges, sector/industry-specific requirements and cloud models.

Accountability requirements could also have been derived from the current and future data protection legislation. Many of the requirements in the repository are indeed compliant with the existing Data Protection Directive [20], which specifies a number of rules on the processing of personal data in Europe. Even though the Data Protection Directive has not been used as input to the elicitation of the requirements in our repository, it is clear that the stakeholders that were engaged in the elicitation activities are aware of both the rules in the Directive and the context in which it applies. Similarly, some of the requirements that were elicited form the stakeholders include rules covered by the proposal for a new European Union Data Protection Regulation[21].

A requirements workshop is a structured meeting in which a carefully selected group of stakeholders and content experts work together to define, create, refine and reach closure on deliverables that represent user requirements [6]. Requirements workshops are based on the premise that a small group of knowledgeable, motivated people is more effective than one or two development "heroes". The benefit of the workshop

process is that it nurtures team communication, decision-making, and mutual understanding. Workshops are also an effective way to bring together customers, users and software suppliers to improve the quality of software products. Requirements workshops can bridge communication gaps among project stakeholders. Co-creating models in a requirements workshop expedites mutual learning and understanding. By asking focused questions in the workshop, the workshop facilitator helps participants define requirements at different levels of specificity.

The workshops presented in this paper were clearly described and organized in such a way that the participants were recruited to contribute actively to the elicitation process. Participation was very good from the stakeholders who committed to be part of the events. All workshops proved to be fruitful with respect to generating further insights for the tools and accountability practices (or expectations). When reflecting on the method for generating discussions which led to stakeholder feedback, the methods used through all workshops showed to be effective.

C. Stakeholder participation

The elicitation activities have included a large number of external stakeholders who have been given the opportunity to express their opinions on and experiences with security, privacy, risk and trust issues of public cloud services. In addition, a number of researchers from the A4Cloud project have contributed with additional requirements for the technologies and tools that they are working on. While we overall are happy with the number of stakeholders that have attended the elicitation activities (in particular the T2 and T3 events attracted a large number of stakeholders) and the number of requirements that were generated from these events, we can conclude that not all of the identified stakeholders groups have been well represented. We have had a good representation of cloud customers, cloud providers and cloud subjects in our workshops, focus groups and interviews, but cloud auditors and consumer groups have not been equally well represented. Our stakeholder selection and invitation process was suitable for the project, although recruiting stakeholders to non-local events proved more difficult than firs envisaged.

VI. Conclusion

The 289 requirements for accountability in the cloud can be accessed freely in the A4Cloud Requirements Report [19].

Acknowledgements

The research in this paper has been supported in part by the European Commission through the EU FP7 project A4Cloud, grant nr. 317550. We are grateful to our project partners and collaborators.

References

[1] M. Felici, M. G. Jaatun, E. Kosta, and N. Wainwright, "Bringing accountability to the cloud: addressing emerging threats and legal perspectives," in *Cyber Security and Privacy*. Springer, 2013, pp. 28–40.

[2] M. G. Jaatun, S. Pearson, F. Gittler, R. Leenes, and M. Niezen, "Enhancing accountability in the cloud," *International Journal of Information Management*, 2016. [Online]. Available: https://doi.org/10.1016/j.ijinfomgt.2016.03.004

[3] M. Felici, S. Pearson, B. Dziminski, F. Gittler, T. Koulouris, R. Leenes, M. Niezen, D. Nuñez, A. Pannetrat, J.-C. Royer, D. Stefanatou, and V. Tountopoulos, "Conceptual framework," A4Cloud Project, Tech. Rep. D:C-2.1, October 2014. [Online]. Available: http://a4cloud.eu/sites/default/files/D32.1%20Conceptual%20Framework.pdf

[4] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Nist cloud computing reference architecture," *NIST special publication*, vol. 500, no. 2011, p. 292, 2011.

[5] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Proceedings of the Conference on the Future of Software Engineering*. ACM, 2000, pp. 35–46.

[6] E. Gottesdiener, *Requirements by collaboration: workshops for defining needs*. Addison-Wesley Professional, 2002.

[7] M. G. Jaatun, S. Pearson, F. Gittler, and R. Leenes, "Towards strong accountability for cloud service providers." in *CloudCom*, 2014, pp. 1001–1006.

[8] H. Owen, *Open space technology: A user's guide*. Berrett-Koehler Publishers, 2008.

[9] "OpenSpaceWorld.ORG," http://openspaceworld.org/, accessed: 2013-03-11.

[10] "World Café," http://www.theworldcafe.com/, accessed: 2013-03-11.

[11] D. L. Morgan, "Focus groups," *Annual review of sociology*, pp. 129–152, 1996.

[12] ——, *Focus groups as qualitative research*. Sage publications, 1996, vol. 16.

[13] S. Fischer-Hübner, J. Angulo, and T. Pulls, "How can cloud users be supported in deciding on, tracking and controlling how their data are used?" in *Privacy and Identity Management for Emerging Services and Technologies*, ser. IFIP Advances in Information and Communication Technology, M. Hansen, J.-H. Hoepman, R. Leenes, and D. Whitehouse, Eds. Springer Berlin Heidelberg, 2014, vol. 421, pp. 77–92. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-55137-6_6

[14] R. Alnemr, S. Pearson, R. Leenes, and R. Mhungu, "COAT: Cloud Offerings Advisory Tool," in *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, Dec 2014, pp. 95–100.

[15] M. G. Jaatun, D. S. Cruzes, J. Angulo, and S. Fischer-Hübner, *Cloud Computing and Services Science: 5th International Conference, CLOSER 2015, Lisbon, Portugal, May 20-22, 2015, Revised Selected Papers*. Cham: Springer International Publishing, 2016, ch. Accountability Through Transparency for Cloud Customers, pp. 38–57.

[16] CSA, "Security guidance for critical areas of focus in cloud computing v3.0," Cloud Security Alliance, Tech. Rep., 2011.

[17] B. Grobauer and T. Schreck, "Towards incident handling in the cloud: Challenges and approaches," in *Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop*, ser. CCSW '10. New York, NY, USA: ACM, 2010, pp. 77–86. [Online]. Available: http://doi.acm.org/10.1145/1866835.1866850

[18] D. Cruzes and T. Dybå, "Recommended steps for thematic synthesis in software engineering," in *Empirical Software Engineering and Measurement (ESEM), 2011 International Symposium on*, Sept 2011, pp. 275–284.

[19] M. G. Jaatun, D. S. Cruzes, M. Felici, B. Haugset, K. Bernsmed, C. F. Gago, C. Reed, and R. Leenes, "Requirements report," A4Cloud Project, Tech. Rep. D:B-2.4, November 2014. [Online]. Available: http://a4cloud.eu/sites/default/files/D22.4%20Requirements%20report.pdf

[20] EU, "95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," *Official Journal of the EC*, vol. 23, no. 6, 1995.

[21] ——, "Proposal for a regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)," *COM*, vol. 11, no. Final, 2012.