Interoperability Analysis of Accountable Data Governance in the Cloud

Vasilios Tountopoulos[1(✉)], Massimo Felici[2], Alain Pannetrat[3],
Daniele Catteddu[3], and Siani Pearson[2]

[1] Athens Technology Center S.A., Athens, Greece
v.tountopoulos@atc.gr
[2] HP Labs, Bristol, UK
{massimo.felici,siani.pearson}@hp.com
[3] Cloud Security Alliance, Edinburgh, Scotland, UK
{apannetrat,dcatteddu}@cloudsecurityalliance.org

Abstract. Cloud computing has emerged as a promising technology to drive innovation and leverage business development in various sectorial applications. Large scale enterprises and SMEs take advantage of cloud computing in order to benefit from cost-effective technological deployments allowing flexibility and scalability, and to offer added value solutions to their customers. However, customers' perceptions of the risks affecting data and IT governance, especially in complex service provision ecosystems, result in a lack of trust in the ability of the providers to handle their assets in a responsible way. This paper elaborates on the general aspects of an accountability-based approach, which can facilitate organisations dealing with the cloud to comply with applicable legislation and provide more evidence that confidential and/or personal data are handled in accordance with relevant data protection legislation.

Keywords: Accountability · Governance · Interoperability · Cloud computing

1 Introduction

Data governance in the cloud is of paramount importance. Unfortunately, cloud customers are faced with or perceive a loss of governance or lack of transparency about the way their data are processed in the cloud. Customers are clearly concerned about the loss of governance over their data in the cloud [1]. They worry about the possible uncontrolled replication or potential disclosure of their personal and/or confidential data to third parties. The uncertainty about who is able to access data stored in the cloud, and for what purposes, is aggravated by the complexity of cloud supply chains. This makes cloud customers feel uncomfortable about how their personal or confidential data are being managed. This concern is exacerbated as the legal framework is complex, failing to provide clarity around the rules that affect the cloud market. Thus, cloud deployments face two main barriers that have a direct impact on the adoption of cloud services for data-intensive business contexts: the uncertainty of the regulatory regimes regarding the processing of personal and/or confidential data, and the perception of emerging security threats [2, 3] in cloud service provisioning chains.

F. Cleary and M. Felici (Eds.): CSP Forum 2014, CCIS 470, pp. 77–88, 2014.
DOI: 10.1007/978-3-319-12574-9_7

This paper introduces an accountability-based governance framework as a means to complement existing data and IT governance practices and address privacy and data protection law compliance in complex cloud service provisioning ecosystems. We argue for an accountable cloud governance approach, which involves the ability to demonstrate, as appropriate, that the processing complies with data protection laws. The principle of accountability [4] addresses some important cloud customers' concerns regarding the use of cloud computing.[1] Accountability can be a valuable vehicle towards the implementation of improved mechanisms and procedures for data protection, efficient data stewardship and demonstration of compliance with regulatory regimes [4, 5]. The principle of accountability could be addressed across different levels, each of which relate to regulatory, organisational and technological aspects of a cloud service chain. From a regulatory perspective, various legal challenges arise from the current regulatory framework, which defines specific rules and introduces certain legal requirements in relation to data governance [6]. The organisational perspective includes the policies that implement cloud governance, raising responsibilities that should be, legally and ethically, accepted by all parties involved in the cloud business or cloud service supply chain. An ethical dimension of being accountable can also be considered as an inherent incentive to respect the rights of those placing their confidential and/or personal data in the cloud, which can, further, drive achieving a better position in the global market landscape, by implementing policy-driven cloud computing solutions [7]. From a technical perspective, accountability involves using mechanisms to protect personal and/or confidential data.

This paper presents an accountability-based approach for data stewardship in the cloud [8, 9]. The approach involves an accountability model (and related framework) for data governance in the cloud. The accountability-based approach supports an analysis of the interoperability requirements for cloud ecosystems. This paper is structured as follows. Section 2 describes the problem of data governance in the cloud. Section 3 introduces the accountability model underlying our accountability-based approach to cloud governance. Section 4 elaborates on the interoperability aspects of cloud governance. Finally, Sect. 5 highlights some concluding remarks.

2 Data Governance in the Cloud

The broad adoption of cloud services has driven different business models, which are based on complex service development and delivery supply chains, and, at the same time, have allowed cybercriminals to use reputable services to bypass many of the digital defences erected by companies [10]. Cloud data governance and management become highly challenging in order to overcome the problems, which set barriers in the wider adoption of cloud ecosystems. Such problems may relate to various cloud

[1] Note that accountability does not itself address important issues concerned with information security properties such as integrity, confidentiality and availability. However, this is only done indirectly by demonstrating that such properties are reflected within the designed system or service (which of course they might not be). Evidence supporting specific claims is necessary in order to assess how systems and services met specific requirements.

specific features and, in principle, they have a direct impact on building proper data governance policies for accountable approaches in the provision of cloud services.

Among the main concerns for prospective adopters of cloud services are loss of data control, compliance with laws and regulations, gaps in standards and specifications, the lack of simple mechanisms to assess the trustworthiness of potential partners and the effective implementation of incident response mechanisms [9]. These issues result in the lack of visibility and transparency within the service supply chain and the subsequent trust in data protection practices in the cloud. Accountability emerges as a cornerstone, where particular emphasis should be given to the proper definition of roles in the cloud service provisioning ecosystems and the subsequent allocation and enforcement of the responsibility for these, such as for data controller and data processors, and to facilitate the exercise of the rights of the data subjects.

Data governance in the cloud is not just effected by the complexity of the business and technical relationship between multiple parties and the increased sophistication of cyber-attacks, but also the legal uncertainty of the regulatory framework. More specifically, cloud governance is impacted by the cloud features, such as multi-tenancy of applications, where co-tenants may, for example, gain inappropriate access to the data of another application instance. Also, data duplication in the cloud creates problems in terms of compliance, since it can make the data lifecycle management difficult across various providers involved in a service provisioning chain. As a result, cloud customers are often sceptical about the cloud environment [11] due to a justifiable set of concerns, including how the ramification of any failures across the cloud provision chain can be discovered and mitigated, without losing control over data, and how compliance with established laws and regulations may be maintained.

When migrating to the cloud, data governance focuses increasingly on what security level the providers involved in the service chain can implement and guarantee. This means that of primary importance is the fact that critical privacy concerns are raised regarding the storage and processing (i.e. operations on data) of confidential or personal data in the cloud, any of which may be allocated to third parties. Given the technology-related challenges of building sustainable accountability-based cloud service chains [1], the legal requirements raise further barriers, which may affect the future of secure cloud computing. Indeed, a number of constraints have to be considered when designing and implementing accountability-based solutions for the cloud, which indicates that developing a perfect accountability solution is not feasible, and instead mechanisms for accountability should be evolved and improved over time.

3 An Accountability Model for Cloud Governance

We define a model of accountability (first introduced in [9]) that brings together different attributes, practices, and mechanisms. The accountability model consists of:

- **Accountability attributes** – conceptual elements of accountability applicable across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis), namely observability, verifiability, attributability, transparency, responsibility, liability and remediability.

- **Accountability practices** – emergent behaviour characterising accountable organisations (that is, how organisations operationalise accountability or put accountability into practice)
- **Accountability mechanisms** – diverse processes, non-technical mechanisms and tools that support accountability practices (that is, accountability practices use them).

Accountability attributes encompass the numerous elements and properties of accountability at the conceptual level. *Accountability practices* characterise organisational behaviour, and hence define what it means to be an accountable organisation. *Accountability mechanisms* are used in order to support such practices. Figure 1 illustrates how attributes, practices and mechanisms form a model of accountability.

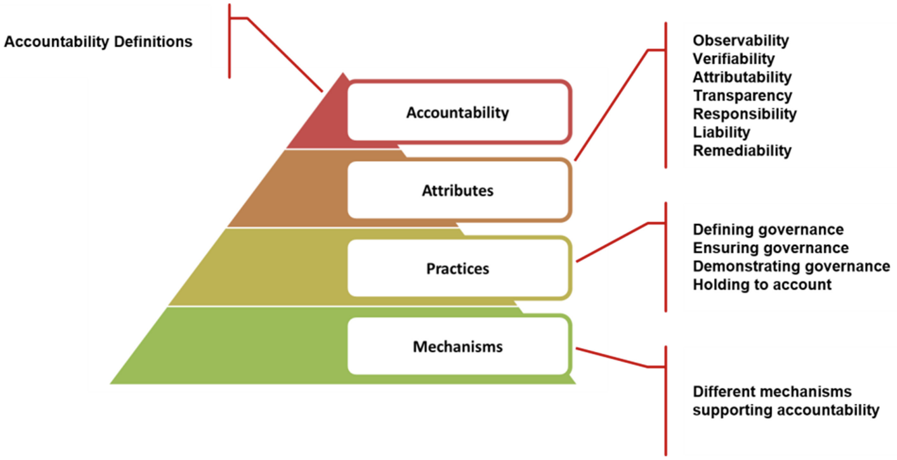


Fig. 1. Accountability attributes, practices and mechanisms

Accountability is interpreted in terms of accountability attributes. These accountability attributes are operationalised (that is, put into practice) by organisational accountability practices. Accountability practices need to comply with and mediate between external (drawn from relevant regulatory regimes and ethical attitudes) and internal (characterising organisational culture) criteria. In order to implement such practices, organisations use different accountability mechanisms tailored to their domains. The emerging relationships between accountability attributes, practices and mechanisms give rise to an operational interpretation of accountability (further descriptions of accountability attributes, mechanisms and practices is provided in [9]).

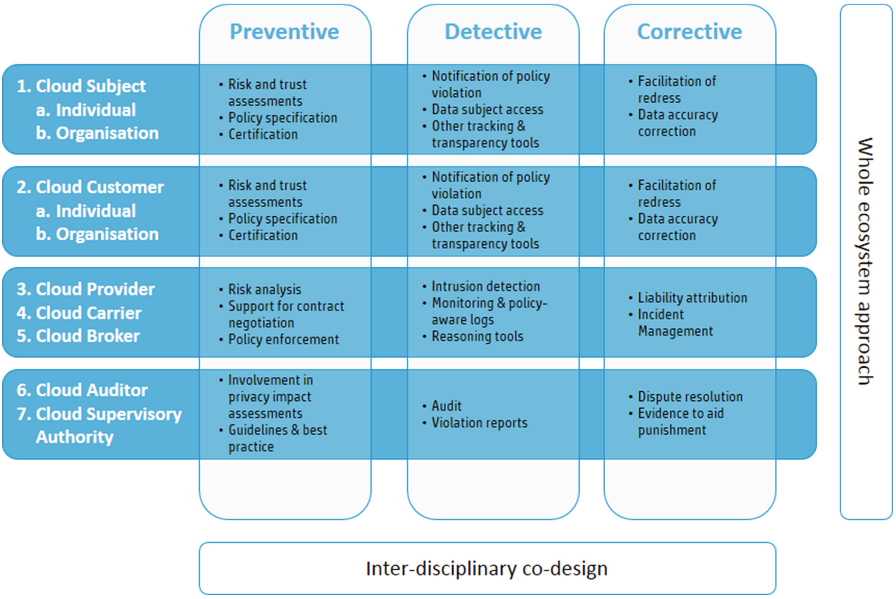
3.1 Accountability Framework

The relative lack of transparency in the cloud as to the providers and sub-providers that may be involved has given rise to concern regarding how risks and regulatory obligations may be assessed and managed – *"the lack of transparency of an outsourcing chain consisting of multiple processors and subcontractors"* [5]. It is necessary to establish *chains of accountability*. Accountable organisations have to fulfil legal (as well as contractual and ethical) obligations for the usage or processing of personal and/or confidential data, and to ensure that contracted partners to whom they supply data enable themselves to remain compliant, wherever in the world the partners may be. We provide a definition of accountability tailored to the cloud:

> **Definition of Accountability for Data Stewardship in the Cloud:** *Accountability for an organisation consists of accepting responsibility for the stewardship of personal and/or confidential data with which it is entrusted in a cloud environment, for processing, storing, sharing, deleting and otherwise using the data according to contractual and legal requirements from the time it is collected until when the data are destroyed (including onward transfer to and from third parties). It involves committing to legal and ethical obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.*

Our approach is to integrate legal, regulatory, socio-economic and technical approaches into a framework to provide accountability pre-emptively, to assess risk and avoid security and privacy threats and reactively to provide transparency, auditing and corrective measures for redress. This enables us to implement chains of accountability, including interdisciplinary mechanisms to ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs. To achieve this for the cloud a chain of responsibility needs to be built throughout the cloud service supply network starting from the cloud service customers, which can be overseen by regulators, auditors and business governance. Accountability is the result of complying with a combination of public (e.g. derived from regulatory regimes) and private (e.g. derived from organisational practices) accountability criteria in cloud ecosystems. Actors within cloud ecosystems can use mechanisms to support accountability practices, and thereby help them to comply with relevant regulatory regimes within specific application domains. Businesses need to meet these obligations, as well as obligations and requirements imposed by other stakeholders that include customers and data subjects. We provide a framework (Fig. 2) that embodies our accountability-based approach combining legal, governance and technical measures that may be used to support accountability in cloud service provision chains. The accountability framework involves different functional aspects of accountability: Preventive (investigating and mitigating risk in order to form policies and determine appropriate mechanisms to put in place; putting in place appropriate policies, procedures and technical mechanisms), Detective (monitoring and identifying policy violation; putting in place detection and traceability measures), and Corrective (managing incidents and providing notifications and redress).

New data governance models for accountability can serve as a basis for providing data protection when cloud computing is used. Accountability is becoming more integrated into self-regulatory programs as well as future privacy and data protection frameworks globally. It is an upcoming challenge to strengthen this approach and make it more workable by developing ways in which accountability and information stewardship can be provided. This goes beyond traditional approaches to protect data, in that it includes complying with and upholding values, obligations, and enhancing trust.



	Preventive	Detective	Corrective
1. Cloud Subject a. Individual b. Organisation	• Risk and trust assessments • Policy specification • Certification	• Notification of policy violation • Data subject access • Other tracking & transparency tools	• Facilitation of redress • Data accuracy correction
2. Cloud Customer a. Individual b. Organisation	• Risk and trust assessments • Policy specification • Certification	• Notification of policy violation • Data subject access • Other tracking & transparency tools	• Facilitation of redress • Data accuracy correction
3. Cloud Provider 4. Cloud Carrier 5. Cloud Broker	• Risk analysis • Support for contract negotiation • Policy enforcement	• Intrusion detection • Monitoring & policy-aware logs • Reasoning tools	• Liability attribution • Incident Management
6. Cloud Auditor 7. Cloud Supervisory Authority	• Involvement in privacy impact assessments • Guidelines & best practice	• Audit • Violation reports	• Dispute resolution • Evidence to aid punishment

Fig. 2. Accountability framework

The framework based on the accountability definitions and concepts involves different mechanisms. These mechanisms form a reference architecture supporting accountable data governance, hence chains of accountability in the cloud.

3.2 Accountability Governance

A major driver for an accountability-based approach is to provide an incentive for organisations to ‘do the right thing’ with respect to relevant regulatory regimes. Various aspects of accountability as an evolving regulatory and enforcement approach (e.g. operationalization of accountability in Binding Corporate Rules,[2] provision of flexibility in terms of measures taken to support compliance etc.) can make things easier for organisations in terms of compliance and this, coupled with stronger penalties for non-compliance, can provide business incentives for organisations to use privacy data protection and security controls more effectively. For example, in response to the seemingly insufficient reflection of EU data protection principles and obligations in concrete measures and practices used by organisations, the Article 29 Data Protection Party advocated in their opinion on the principle of accountability that such a general principle could help move data protection ‘from theory to practice’, as well as provide a means for assisting data protection authorities in their supervision and assessment tasks [4]. There would be an associated requirement for data controllers to be able to

[2] Article 29 Data Protection Party has issued various documents on different aspects of Binding Corporate Rules, e.g. Explanatory Document on the Processor Binding Corporate Rules [12].

demonstrate their compliance to supervisory authorities upon request [13]. Hence, organisations would be allowed some increased control over aspects of compliance, e.g. which tools and mechanisms to use in order to achieve compliance, but at the expense of having to demonstrate on an ongoing basis that these mechanisms are appropriate for their business context, and operationally work as expected.

All actors involved (in particular, those directly involved in governance) have a role to play in making cloud services accountable for how data are used and managed in the cloud – *"Cloud governance encompasses two main areas: internal governance focuses on a provider's technical working of cloud services, its business operations, and the ways it manages its relationship with customers and other external stakeholders; and external governance consists of norms, rules, and regulations which define the relationships between members of the cloud community and attempt to solve disputes between them"* [14]. Both internal and external governance pertain to the collection, storage, processing operations on and dissemination of personal and/or confidential data, and other processing. Figure 3 shows the interaction between two organisations (as a continuous process) driven by accountability governance (constrained by external criteria and regulatory regimes but managed independently).

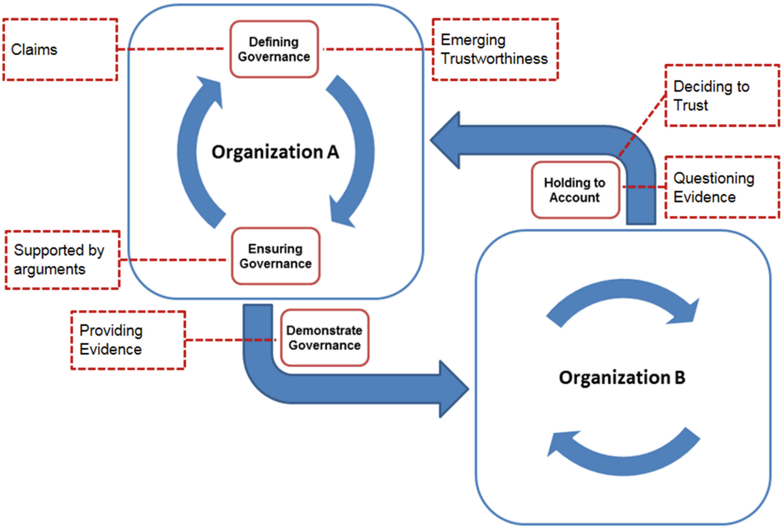


Fig. 3. Accountability governance

The legal and contractual context defines obligations, responsibilities and liabilities of actors in a given cloud ecosystem. Accountability entrusts organisations with the practical aspects of complying with data protection obligations. This involves clarification of requirements of the different actors within cloud ecosystems, as well as transparency and provisions of trustworthy accounts (in the sense of accountability) by organisations that collect or handle personal data. Accountable organisations need to define and implement appropriate governance mechanisms relating to the treatment of personal and/or confidential data in cloud environments.

Accountability governance then consists of taking responsibility for specific accountability criteria, with the aim of ensuring accountability by deploying suitable mechanisms and demonstrating them by compliance with such criteria through evidence. Organisations need to provide transparency regarding their systems and actions taken in order to show that stakeholders' expectations have been met and that organisational policies have been followed. They also need to remedy any failure to act properly (e.g. by notifications, remedies, sanctions), even in cloud-supply chains involving multiple service providers. Accountability governance redefines interactions between providers and customers/regulators as well as between providers themselves. The ethical nature of an accountability-based approach and the organisational obligations that result from taking this approach represent a shift from reactive to proactive governance of personal and/or confidential data. Organisations commit to the stewardship of personal and/or confidential data by accepting and addressing legal, contractual and ethical obligations. In order to do so, organisations deploy and use different mechanisms (e.g. policies, standards), take into account social norms, provide evidence to internal and external stakeholders, and remedy any failure to act properly.

4 Interoperability as an Enabler of Accountability

One of the attractive aspects of the cloud ecosystem is the ability to build new cloud services and applications from other pre-existing cloud services and applications. This is typically exemplified by cloud services like Dropbox [15], which builds upon Amazon storage, or more complex services like Netflix,[3] which combine IaaS, PaaS, and content distribution networks across the globe. The ability to make services work together seamlessly across complex supply chains is made possible by two largely intertwined features: interoperability and automation. Interoperability describes the *"ability of a system or a product to work with other systems or products without special effort on the part of the customer"* and is "*made possible by the adoption of standards*".[4] Formal or de facto standards specify common data formats, semantics and communication protocols adopted by actors in the cloud supply chain. The adoption of standards in turn facilitates automation of the processes involved in the provision of cloud services, unleashing the efficiencies that make the cloud successful. We believe that, with adequate automation, we can reduce *real* or *perceived* costs associated with providing accountability in the cloud can be reduced. In turn, by reducing the cost of accountability we can encourage the greater adoption of best practices for data stewardship. In order to support automated mechanisms to enable accountability provision in the cloud, we first identified all actors typically involved in cloud accountability interactions. Next, we found that their accountability-related interactions could be classified in 4 general subgroups, which in turn could be used to shape requirements for interoperability for the purpose of accountability. In the A4Cloud project, we chose to extend the NIST cloud supply chain taxonomy [16] to create the following cloud accountability taxonomy composed of seven main roles:

[3] http://techblog.netflix.com/search/label/cloud%20architecture

[4] https://www.ieee.org/education_careers/education/standards/standards_glossary.html

1. **Cloud Subject:** An entity (individual or organisation) whose data are processed by a cloud provider, either directly or indirectly.
2. **Cloud Customer:** An entity (individual or organisation) that (1) maintains a business relationship with, and (2) uses services from a Cloud Provider.
3. **Cloud Provider:** An entity responsible for making a (cloud) service available to Cloud Customers.
4. **Cloud Carrier:** The intermediary entity that provides connectivity and transport of cloud services between Cloud Providers and Cloud Customers.
5. **Cloud Broker:** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Customers.
6. **Cloud Auditor:** An entity that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation, with regards to a set of requirements, which may include security data protection, information system management, laws or regulations and ethics.
7. **Cloud Supervisory Authority:** An entity that oversees and enforces the application of a set of rules.

The NIST role taxonomy was chosen as a foundation because of its vast adoption. However, it has some shortcomings when used to describe accountability scenarios. For example, if we look at the data protection domain, which is central in this project, we can observe that the “data subject” is invisible in the NIST taxonomy, except when she/he is also a cloud customer. This was among the reasons that led us to extend and modify the NIST taxonomy as proposed above [17]. Next, we classify the accountability interactions between these seven cloud actors into four main subgroups:

1. **Agreement** covers all interactions that lead to one actor taking legal responsibility for the handling of certain data provided by another party according to a certain policy. These interactions may include a negotiation phase. A policy may *express* requirements that apply to all 7 core accountability attributes, and contributes to the *implementation* of the attributes of *responsibility* and *liability*.
2. **Reporting** covers all interactions related to the reporting by an actor about current data handling practices and policies (e.g. reporting security breaches or providing security/privacy level indictors). This type of interaction mainly supports the implementation of the accountability attributes of *transparency* and *observability*.
3. **Demonstration** covers all interactions that lead to one actor demonstrating the correct implementation of some data handling policies. This includes external verifications by auditors or cryptographic proofs of protocol executions, for example. This type of interaction mainly supports the *implementation* of the accountability attributes of *verifiability* and *attributability*. We emphasise that *Demonstration* differs from *Reporting* in that it implies some form of proof or provision of evidence.
4. **Remediation** covers all interactions that lead one actor to seek and receive or offer remediation for failures to follow data handling policies. This mainly supports the *implementation* of the accountability attribute of *remediability*.

By cross matching these four subgroups of interactions with the cloud accountability roles above, we identified 31 key interoperability requirements for accountability in the cloud. While we refer the reader to [18] for the details, we can highlight two key elements of this analysis. First and foremost, an essential requirement for enabling interoperability for the purpose of accountability in the cloud is the ability of two communicating parties to share a common understanding of security and data protection policy semantics and their associated metrics, be it for the purpose of agreement, reporting, demonstration and/or remediation. Unfortunately, this common ground for semantics hardly exists today [19]. For example, all major cloud providers use different semantics and metrics for availability [20]. The same can be said if two interacting actors use different technical standards to interpret properties such as "consent", "confidentiality level" or "user information" (independently of their legal meaning), just to give a few examples. Second, interoperable accountability mechanisms have to be interoperable across the cloud supply chain. For example, if a cloud provider needs to report data stewardship information to a customer, it may need itself to obtain information from other providers acting as its sub-providers, while still preserving a common understanding of policy semantics.

With so many actors and interactions, we need to set priorities in attempting to automate accountability interactions in the cloud. The logical step is to focus first on the most frequent and necessary interactions and later on the most uncommon ones. In this respect, *Information* and *Agreement* are the two subgroups of interactions we should start with, focusing in particular on Cloud Customers, Cloud Providers, and Cloud Subjects (*data subjects*). At the other end of the spectrum, we expect *remediation* interactions and more generally interactions with supervisory authorities and auditors to be rarer and therefore less of a priority for automation.

There are currently some significant initiatives that could provide interoperability and automation supporting accountability in the cloud. To begin with, the A4Cloud project itself is proposing a policy language A-PPL, which is an extension of the PPL language [21], itself based on XACML [22]. More broadly, the A4Cloud project will produce a set of novel tools that will aim to tackle the interoperability issues highlighted above. The Cloud Security Alliance is developing two relevant RESTful APIs: CloudAudit[5] to access audit data from cloud provider, and the Cloud Trust Protocol[6] for constant monitoring of security properties of cloud services, both contributing to automated *Information* and *Demonstration* interactions. Similarly, the NIST has begun examining how to define metrics applicable to the monitoring of security properties described in an SLA.[7] The European Commission is also investigating model terms for cloud SLAs [1], while ISO in [23] is developing a new standard for cloud SLAs. As these initiatives mature, we hope to see *accountability as a service* become a reality in the cloud in the next few years.

[5] http://www.cloudaudit.org/

[6] https://blog.cloudsecurityalliance.org/ctp/

[7] http://www.nist.gov/itl/cloud/

5 Concluding Remarks

This paper presented an accountability-based approach for cloud data governance, as a means for addressing interoperability requirements relating to the protection of personal and confidential data involved in complex service provision chains in the cloud. Through the description of an accountability model and the related framework, we emphasised the need to integrate together legal, regulatory, and technical aspects as an effective way to build sustainable chains of accountability. We then elaborated on the interoperability aspects, which can be identified across the interactions that happen between stakeholders involved in cloud data governance practices. As an extension to this work, the interoperability requirements can be aligned to legal requirements for cloud data governance, as they arise from the analysis of the implications of the established regulatory framework on the data protection in the cloud service provision ecosystem. An initial analysis of some data governance challenges in the cloud from a data protection regulatory perspective has been made in [6].

As future steps, we will be focusing on the implementation of algorithms and tools, which will enable realisation of the accountability framework and respective technical functions, which will be implemented by software components to provide technical support for the adoption of accountability mechanisms by the parties involved in complex service provision chains. In order to better illustrate the business benefits of accountability-based cloud data governance, prototype use case examples will be developed. These examples will showcase different aspects of the data and IT governance problem in the cloud and how accountability can practically work with the deployed security and privacy controls to foster higher levels of cloud consumers and providers' trust in both the cloud environments and the privacy and data protection mechanisms followed in them.

Acknowledgments. This work has been partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD – http://www.a4cloud.eu/) Cloud Accountability Project. We would like to thank our project partners and colleagues who provided valuable comments to early drafts of this paper.

References

1. European Commission: Unleashing the potential of cloud computing in Europe. COM529 (2012)
2. Cloud Security Alliance: The notorious nine: cloud computing top threats in 2013. CSA Top Threats Working Group (2013)
3. European Network and Information Security Agency: Cloud computing: benefits, risks and recommendations for information security. ENISA report (2009)
4. Article 29 Data Protection Working Party: Opinion 3/2010 on the principle of accountability. 00062/10/EN WP 173 (2010)
5. Article 29 Data Protection Working Party: Opinion 05/2012 on Cloud Computing. 01037/12/EN WP 196 (2012)
6. Kuan Hon, W., Kosta, E., Christopher, M., Stefanatou, D.: Cloud accountability: the likely impact of the proposed EU data protection regulation. Queen Mary School of Law Legal Studies, Research Paper No. 172/2014; Tilburg Law School, Research Paper No. 07/2014

7. International Data Corporation (IDC): Quantitative estimates of the demand for cloud computing in Europe and the likely barriers to up-take, July (2012)
8. Felici, M., Jaatun, M.G., Kosta, E., Wainwright, N.: Bringing accountability to the cloud: addressing emerging threats and legal perspectives. In: Felici, M. (ed.) CSP EU FORUM 2013. CCIS, vol. 182, pp. 28–40. Springer, Heidelberg (2013)
9. Felici, M., Koulouris, T., Pearson, S.: Accountability for data governance in cloud ecosystems. In: 2013 IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2013), Proceedings, pp. 327–332. IEEE Computer Society (2013)
10. Georgia Tech Information Security Center (GTISC) and Georgia Tech Research Institute (GTRI): Emerging cyber threats report 2014. Georgia Institute of Technology, Georgia Tech Cyber Security Summit (2013)
11. Organisation of Economic Cooperation and Development (OECD): The future of internet economy: a statistical profile. OECD Report, June 2011
12. Article 29 Data Protection Working Party: Explanatory document on the processor binding corporate rules. 00658/13/EN WP 204 (2013)
13. Article 29 Data Protection Working Party: Opinion 01/2012 on the data protection reform proposals. 00530/12/EN WP 191 (2012)
14. Reed, C.: Cloud governance: the way forward. In: Millard, C. (ed.) Cloud Computing Law. Oxford University Press, Oxford (2013)
15. Drago I., Mellia M., Munafo M.M., Sperotto A., Sadre R., Pras A.: Inside dropbox: understanding personal cloud storage services. In: Proceedings of the 2012 ACM Conference on Internet Measurement Conference (IMC'12), pp. 481–494. ACM, New York (2012)
16. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D.: NIST cloud computing reference architecture. NIST special publication, 500-292 (2011)
17. A4Cloud: MS:C-2.3 conceptual framework. Milestone Report, May 2014
18. A4Cloud: D:C-3.1 requirements for cloud interoperability. Public Deliverable, November (2013)
19. Hogben G., Dekker M.: Procure secure, a guide to monitoring of security service levels in cloud contracts. European Network and Information Security Agency (ENISA) Report (2012)
20. Hogben G., Pannetrat A.: Mutant apples: a critical examination of cloud SLA availability definitions. In: IEEE 5th International Conference Cloud Computing Technology and Science (CloudCom), December 2013
21. Ardagna A.C., et al.: Primelife policy language (2009). http://www.w3.org/2009/policy-ws/papers/Trabelisi.pdf
22. OASIS: eXtensible Access Control Markup Language (XACML) Version 3.0 (2013)
23. ISO/IEC NP 19086, Information technology - Distributed application platforms and services - Cloud computing - Service level agreement (SLA) framework and terminology. Under development, November (2013)