Towards a Model of Accountability for Cloud Computing Services

Daniele Catteddu[1], Massimo Felici[2], Giles Hogben[1], Amy Holcroft[2], Eleni Kosta[3], Ronald Leenes[3], Maartje Niezen[3], Christopher Millard[4], David Nuñez[5], Nick Papanikolaou[2], Siani Pearson[2], Daniel Pradelles[2], Chris Reed[4], Jean-Claude Royer[6], Dimitra Stefanatou[3], Vasilis Tountopoulos[7], Tomasz Wiktor Wlodarczyk[8]

[1]Cloud Security Alliance, [2]Hewlett-Packard, [3]Tilburg University, [4]Queen Mary - University of London, [5]Universidad de Malaga, [6]Ecole des Mines – Nantes, [7]Athens Technology Center, [8]University of Stavanger

Abstract. This paper presents a model of accountability for cloud computing services, based on ongoing work as part of the A4Cloud project[1]. We define a three-layer model of accountability as a general concept for data governance, distinguishing between accountability attributes, accountability practices, and accountability mechanisms and tools.

1 Introduction

Accountability is an important but complex notion that encompasses the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, to be transparent (give account) about how this has been done and to provide remediation and redress. This notion is increasingly seen as a key market enabler in global environments and in helping overcome barriers to cloud service adoption. However, the relative complexity of the service provision chain makes it very challenging both legally and technically to provide accountability for and in the cloud. We propose a co-designed approach that encompasses legal and regulatory mechanisms and a range of technological enhancements that can provide the necessary basis for initiating and sustaining trustworthy data processing and a trusted relationship between data subjects, regulators and cloud service providers.

We define a three-layer model of accountability as a general concept for data governance, distinguishing between accountability attributes, accountability practices, and accountability mechanisms and tools. Accountability attributes are the concepts from which accountability is built, and these are drawn from an extensive survey of

[1] The A4Cloud project is targeted at EU Framework 7 Call 8 Objective ICT-2011.1.4 Trustworthy ICT, and particularly on objective (c) (i.e. data policy, governance and socio-economic ecosystems). See http://www.a4cloud.eu/.

the literature; they include responsibility, liability, transparency, observability, verifiability, sanction, provision of assurance and satisfaction of obligations. Accountability practices are sets of behaviours that an organisation should have in order to be accountable, and are distinguished into four broad categories:

1. defining governance to comply in a responsible manner with internal and external criteria,
2. ensuring the implementation of appropriate actions to actualise such governance,
3. explaining and justifying those actions, namely, demonstrating regulatory compliance,
4. remedying any failure to act properly.

The practices listed above are part of the definition of accountability used by the project. Accountability mechanisms and tools – often technical tools, including software, but also legal procedures and other mechanisms – by which accountability practices are supported and implemented.

There are numerous references to accountability in regulatory frameworks, and these are surveyed in this document. The most relevant opinions expressed by the EU's Article 29 Working Party (an independent advisory body on the interpretation of the data protection framework set up under article 29 of Directive 95/46/EC) as well as the European Data Protection Supervisor (EDPS), among others, are described. In addition, data governance best practices, as well as risk assessment guidance for the handling of personal data by organisations, are surveyed. Definitions and models of accountability used in computer science are also reviewed, from high-level presentations to low-level cryptographic models used for proving properties about systems.

The problems presented by cloud service provision ecosystems, and how they may be addressed by an accountability approach, are considered; these include multi-tenancy, the dynamic, ever changing environment, data duplication, and easy access to data from multiple locations. This paper is structured as follows. Section 2 proposes our definitions of accountability in the cloud. Section 3 describes an accountability model based on the given definitions. Section 4 draws some concluding remarks.

2 Proposed Definitions of Accountability in the Cloud

The following definition captures a shared understanding of accountability based on reviewing previous related work and discussion within the project:

> **Conceptual Definition of Accountability:** *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

The conceptual definition of accountability encompasses different understandings drawn from different disciplines. It is intentionally generally applicable across different domains. Further to this generic definition, we tailor the conceptual definition of accountability to the domain of focus of the A4Cloud Project, namely to data protec-

tion in the cloud [1]. Thus, the following A4Cloud definition contextualises the notion of accountability (that is, the Conceptual Definition of Accountability) and makes it relevant to the scope of the project:

> **A4Cloud Definition of Accountability:** *Accountability for an organisation consists of accepting responsibility for the stewardship of personal and 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 is destroyed (including onward transfer to and from third parties). It involves committing to legal, ethical and moral obligations, policies, procedures and mechanisms, explaining and demonstrating ethical implementation to internal and external stakeholders and remedying any failure to act properly.*

The definitions highlight the main conceptual aspects of accountability. They characterise the necessary practices emerging in organisations that take an accountability-based approach, with respect to specific attributes supporting accountability.

3 A Model of Accountability in the Cloud

An analysis that deconstructs the accountability definitions introduced in the previous section highlights a model consisting of *accountability practices*, *attributes*, *mechanisms and tools*, as discussed further below. Figure 1 shows the relationships between these aspects of accountability, and how together they form a model.

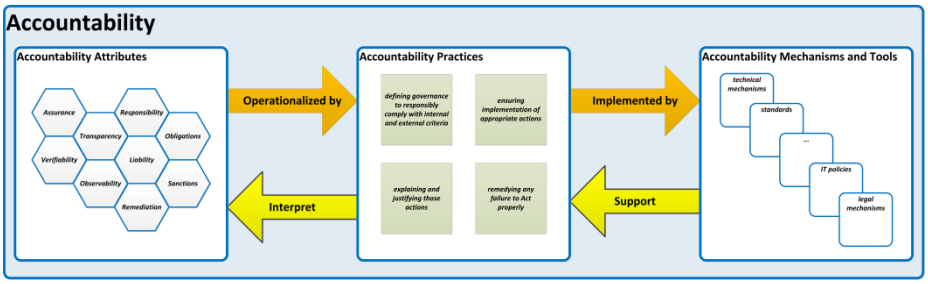

Figure 1 Accountability Attributes, Practices, Mechanisms and Tools

The central elements of this model are:

- **Accountability attributes** – conceptual elements of accountability as used across different domains (i.e. the conceptual basis for our definition, and related taxonomic analysis)
- **Accountability practices** – emergent behaviour characterising accountable organisations (that is, how organisations operationalize accountability or put accountability into practices)
- **Accountability mechanisms and tools** – diverse mechanisms and tools that support accountability practices (that is, accountability practices use them).

Next we shall consider these elements further in turn.

3.1 Defining Accountability Attributes

In order to interpret accountability clearly, we need to distinguish between *accountability practices* and *accountability attributes* (as shown in Figure 1). Accountability attributes encompass concepts that are considered part of and supporting accountability. Typical attributes, among others, include assurance, liability, remediation, responsibility and transparency. The identified attributes stem directly from the definitions of accountability. There exist emerging relationships (e.g. implication and inclusion) among attributes dependent on different viewpoints of analysis (which are related to different accountability perspectives, for instance, like societal, legal and ethical perspectives).

For instance, from a legal perspective, responsibilities imply obligations, which consequently may involve sanctions. From a social perspective, transparency implies both observability and verifiability (and vice versa, transparency is obtained by combining observability and verifiability).Accountability attributes are concepts that relate strongly to accountability. These include: key properties of accountability (e.g. transparency); conceptual elements (e.g. remediation); consequences (e.g. sanctions); related objects (e.g., obligations, insurance).

Obligations prove to be very important in terms of discussion of accountability within service provision networks. In general, there will be certain consequences if an obligation is breached.

> **Obligation:** Obligation is defined into three main types: contractual, regulatory, and normative normative (i.e. derived from social norms) obligation.

Other types of obligations, as defined, such as user preferences could fit under these different categories in different contexts; for example, in some contexts user preferences might create a legal obligation but in others they do not.

Other relationships may exist depending on the operationalization of accountability by organisational practices in different domains. It would be also of interest to extend the analysis of accountability to other related concepts and their relationship to accountability: *Access control, Attribution, Audit, Contract, Control, Data protection, Data stewardship, Demonstration, Evidence, Immutability, Non-repudiation, Penalty, Privacy, Privacy by design, Privacy impact assessment, Redress, Risk and Trust.*

> **Responsibility:** Responsibility may be defined as the state of being assigned to take action to ensure conformity to a particular set of policies or rules.

Attribution of responsibility is a key element of accountability, as is apparent from definitions given in dictionaries, which tend to centre on accountability as the quality or state of being held to account for one's actions and an obligation or willingness to accept responsibility for one's actions – for example: *"Accountability is the obligation and / or willingness to demonstrate and take responsibility for performance in light of agreed upon expectations. Accountability goes beyond responsibility by obligating an organisation to be answerable for its actions"* [2]. Specifically, an account-

able organisation is responsible for the stewardship of personal and confidential data with which it is entrusted.

Attributability: Attributability describes a property of an observation that discloses or can be assigned to actions of a particular actor (or system element).

Accountability can be regarded as an extension of attributability when the action is governed by regulations [3]. This is related to liability since in order for liability to function, it must be attributable to a legal or natural person. In case of a deviation from the expected behaviour (fault), accountability should provide attribution in that it reveals which component is responsible [4].

Evidence is also important in the context of attributability (and hence liability), and thereby in proving non-compliance to governing rules, as well as compliance to governing rules. These governing rules could include obligations in the sense that we use them below, i.e. including legal requirements, contractual requirements and stakeholder requirements (including normative expectations about behaviour).

Liability: Liability is the state of being liable (legally responsible).

Correspondingly, a liable entity is an entity which is legally responsible for the (legal) consequences of a certain action. Often damages will trigger liability. The entity that is held liable is then responsible for repairing damages (e.g. through financial redress). Other forms of liability include criminal liability and other statutory liability (e.g. on the basis of data protection regulation). For example, if failure to report incidents results in a fine of 2% of total wealth and Bob is liable for reporting incidents, then if an incident is not reported, Bob is liable to a value of 2% of his total wealth for failure to report incidents. Liability is an element of almost every definition of accountability. For example, Koppell's five elements of accountability include [5]: *"Liability: Did the organisation face consequences for its performance?"* An accountable organisation takes liability in respect to the obligations (cf. policies) that they have defined. According to the A4Cloud definition, accountability extends liability in the sense that ethical elements are introduced when determining obligations.

Sanctions: Sanctions are the (legal) consequences of failing to comply with some requirement.

In the context of data protection, the legal consequences deriving from the lack of respect towards certain obligations lead to different forms of sanctions that are imposed by the member states to the accountable entities, ranging from court decisions to administrative measures.

Sanctions have a *post hoc* effect, they place a (financial) burden on the punished entity, and an *ex ante* effect, fear of being punished promotes compliant behaviour. Strong sanctions encourage adequate investment in an accountability-based approach; not only do there need to be strong penalties in case of failure to act properly, but they strengthen the motivation for an organisation to take an accountability-based approach if the organisation is treated more leniently if it can be demonstrated that it has

tried to ensure implementation of appropriate actions. The importance of holding to account is shown in this quotation from [6]: *"A vital theme is Accountability. Primary responsibility must be placed on organisations to get it right and they must be held to account if they get it wrong. Organisations must deploy the right technology and have a privacy-by-design approach at the heart of their plans."* Similarly, the working definition of an accountable entity given in [7] stresses this element as it is given in terms of *punishment*: *"An entity is accountable with respect to some policy (or accountable for obeying the policy) if, whenever the entity violates the policy, then with some non-zero probability it is, or could be, punished."*

Assurance: Assurance is a positive declaration intending to give confidence.

Assurance can take the form of evidence. An accountability system can produce evidence that can be used to convince a third party that a fault has or has not occurred [4]. In the context of accountability, assurance could refer to provision of *ex ante* evidence for compliance to governing rules, and possibly also to evidence that the governing rules and other factors provide appropriate grounds for trustworthiness. The Galway project includes in its definition of essential elements of accountability [2]: *"systems for internal, on-going oversight and assurance, reviews and external verification"*. An accountable organisation should provide assurance in order to demonstrate to relevant stakeholders (both internal and external to that organisation) that it has defined governance appropriately, implemented actions appropriately, and to explain and justify those actions.

Transparency: Transparency involves operating in such a way as to maximise the amount of and ease-of-access to information which may be obtained about the structure and behaviour of a system or process.

For example, a cloud provider offers transparency of its security processes if it provides a web page with current and historical availability. It provides further transparency if it offers explanations for outages. More specifically, *'ex ante transparency'* should enable the anticipation of consequences before data is actually disclosed (usually with the help of privacy policy statements), whereas *'ex post transparency'* informs about consequences if data already has been revealed (i.e. what data is processed by whom and whether the data processing is in conformance with negotiated or stated policies) [8].

Transparency encompasses the property of an accountable system that it is capable of "giving account" of, or providing visibility of how it conforms to its governing rules and commitments: "*Information Accountability means that Information usage should be transparent so it is possible to determine whether a use is appropriate under a given set of rules"* [9]. More broadly, an accountable organisation is transparent in the sense that it makes known to relevant stakeholders the policies defined about treatment of personal and confidential data, can demonstrate how these are implemented and provides appropriate notifications in case of policy violation, as well as responding adequately to data subject access requests. Note that transparency does not involve revealing the personal or confidential data itself, as that should be

kept confidential, with the exception that data subjects have the right to access their own data (cf. data subject access). This is analogous to the privacy principle of transparency, which is about the need for transparency of privacy policies and not of the personal data (e.g. as elucidated in the OECD privacy guidelines [10].

Remediation: Remediation is the act or process of correcting a fault or deficiency.

In IT literature, remediation generally refers to being able to restore systems to earlier states in case of system failures, which may require going back many months for a known-good configuration. In relation to data and securities breaches, remediation is part of the *incident response*, *notification*, and *remediation*. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism [2], which can be triggered by an incident report. The organisation acts upon the incident report by notifying the relevant stakeholders (e.g. affected data subjects, regulators, services elsewhere in the service chain) and by repairing the damages. This may involve restoring data to the state prior to the incident, but also support forensic recording of incident data. In a broader context remediation also relates to legal remedies. When data is lost or misused, users may suffer financial damage. Remediation in this sense may refer to claiming compensatory damages or even punitive damages.

In the context of accountability, the accountable organisation is required to take corrective action in case of failure to apply governing rules and honour commitments. This is one of the five elements of accountability mentioned by the Galway project [2]. Remediation is also explicitly specified in our definition of accountability.

Verifiability: Verifiability is a property of an object, process or system that its behaviour can be verified against a requirement or set of requirements.

Quality or level of verifiability depends directly on the available evidence [11]. It is important to notice that some argue that verifiability can be purposefully limited in the contract specification [12]. A closely related notion is *validation*, which relates to the property of accountability whereby it allows users, operators and third parties to verify a posteriori if the system has performed a data processing task as expected [4]. Similarly, *verification* is a process that evaluates whether a system complies with related governing regulations [13], and in the context of accountability is the ability to provide *ex post* evidence for compliance to governing rules (again mentioned by the Galway project [2]).

Observability: Observability is a property of an object, process or system which describes how well the internal actions of the system can be described by observing the external outputs of the system.

The term observability originates from control theory and was introduced by Kalman in [14]. While the formal matrix-based definitions of system observability might be difficult to directly apply to service accountability, they do offer a strong and useful basis for guiding metric definition and construction of framework of evidence.

Particularly of interest is a related weaker term *detectability*. Detectability is property that assumes that all unobservable elements are stable, that is, they do not change the outputs of the system [15]. Observability may have additional effects. Experiments in the psychology of economics have shown that a considerable improvement in contribution towards a public good (which could also include responsible data stewardship) can be achieved by increasing the degree to which a human process is observable – see, for example, [16]. The strong link between accountability and deterrence is also brought out within [7].

> **Responsiveness:** being responsive to your public's viewpoint and debates, being familiar with its key influences and styles, and aware of its ideas and frames of reference is an essential part of being accountable.

When developing tools or mechanisms to demonstrate accountability, being responsive entails that these mechanisms and tools take into account the specific circumstances and practices within which these mechanisms and tools are implemented. The mechanisms and tools that entail such responsiveness are more likely to have a greater trickle-down effect and therefore more efficient.

3.2 Accountability Practices

In accordance with the conceptual definition of accountability, accountable organisations need to define and implement appropriate governance mechanisms relating to treatment of personal data and confidential data. They need to explain what actions are taken, particularly in the sense of demonstrating regulatory compliance. In particular, they need to provide transparency of those actions in order to show that stakeholders' expectations have been met and that organisational policies have been followed. Moreover, they need to remedy any failure to act properly, for example, notifications (to the affected data subjects and/or regulators), redress to affected data subjects or organisations (e.g. sanctions intend to discourage inappropriate behaviour), even in global situations where multiple cloud service providers are involved.

Accountability practices, derived directly from the definitions given, characterise emerging behaviour (highlighting operational and organisational goals to be met) manifested in accountable organisations:

- **defining governance to responsibly comply with internal and external criteria**, particularly relating to treatment of personal data and confidential data
- **ensuring implementation of appropriate actions**, for example:
- **explaining and justifying those actions**, namely, demonstrating regulatory compliance, that stakeholders' expectations have been met and that organisational policies have been followed
- **remedying any failure to act properly**, for example: notifying the affected data subjects or organisations, and/,or providing redress to affected data subjects or organisations, even in global situations where multiple cloud service providers are involved.

In the context of A4Cloud, the actions in question pertain to the collection, storage, processing and dissemination of personal and confidential data by cloud service pro-

viders and associated actors. More specifically, the A4Cloud definition of accountability enhances these aspects to include a focus on the treatment of personal and confidential data in cloud environments. It highlights the need for management of data across the whole data lifecycle (from the time it is collected until and including the destruction of the data). 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 confidential data. Organisations commit to the stewardship of personal and confidential data by addressing legal, ethical and moral obligations. In order to do so, they deploy and use different mechanisms and tools (e.g. policies, procedures, standards), provide evidence to internal and external stakeholders, and remedy any failure to act properly.

3.3 Accountability Mechanisms and Tools

The **accountability mechanisms and tools** referred to above are to be understood as concrete tools and techniques supporting accountability practices; in a broader social science sense, these may be thought of as accountability objects. These include, for example, IT security controls and policies as well as technical mechanisms, standards, legal mechanisms, financial penalties and insurance.

Some of these mechanisms and tools will be developed by A4Cloud; others are available from other parties. Depending upon the context, they may be used individually, or in combination. Organisations may select from different alternatives: for example, they may choose to use the Privacy Level Agreement format specified within CSA [17] to express privacy-related obligations, or the Cloud Trust protocol [18] to ask for and receive information from cloud service providers about the elements of transparency, or they may take another approach to do so.

4 Concluding Remarks

This paper describes a model of accountability in the context of data governance for cloud computing services. It is the first to present the A4Cloud project's definitions of accountability, which will form the basis of further discussions and analyses.

5 References

1. Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September.
2. Center for Information Policy Leadership (CIPL) (2009) 'Data protection accountability: the essential elements. A document for discussion', available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (accessed on 1 March 2010).
3. Watson, Gary (1996), "Two Faces of Responsibility." Philosophical Topics 24: 227–248
4. Castelluccia, C., Druschel, P., Hübner, S., et al. (2011). Privacy, Accountability and Trust - Challenges and Opportunities, ENISA.

5. Koppell, J. (2005) “Public administration review,” *Public Administration Review*, vol. 65, pp. 94–108.
6. Thomas, R. (2009). Foreword of RAND study “Review of Data Protection Directive Summary”, Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf
7. Feigenbaum, J., Jaggard, A.D. and Wright, R.N. (2011) ‘Towards a Formal Model of Accountability’, In Sean Peisert, Richard Ford, Carrie Gates, and Cormac Herley, editors, NSPW , page 45-56. ACM, 2011, http://dl.acm.org/citation.cfm?id=2073276.
8. Hildebrandt, M. (2009). *Biometric Behavioural Profiling and Transparency Enhancing Tools*. FIDIS Project Deliverable 7.12. Available at: http://www.scribd.com/doc/72120638/Fidis-wp7-Del7-12-Behavioural-biometric-Profiling-and-Transparency-Enhancing-Tools
9. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.J. (2008). Information accountability. Communications of ACM 51(6), p. 87, June.
10. OECD (1980) ‘Guidelines for the protection of personal data and transborder data flows’, available at http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html (accessed on 2 July 2012).
11. Bull J., Watson J., "Evidence disclosure and verifiability", Journal of Economic Theory, Volume 118, Issue 1, September 2004, Pages 1-31, ISSN 0022-0531
12. Bernheim B. D., Whinston M., (1999), Incomplete contracts and strategic ambiguity, Amer. Econ. Rev., 88, 902–932.
13. PMBOK (2011) IEEE Guide--Adoption of the Project Management Institute (PMI(R)) Standard A Guide to the Project Management Body of Knowledge (PMBOK(R) Guide)--Fourth Edition.
14. Kalman R. E. (1961), "On the General Theory of Control Systems", Proc. 1st Int. Cong. of IFAC, Moscow 1960 1 481, Butterworth, London 1961
15. Zabczyk J. (1992), "Mathematical Control Theory: An Introduction", Birkauser Boston, 1992.
16. Filiz-Osbay, E. & Osbay, E.Y. (2012). Effect of an Audience on Public Goods Provision. May. http://econweb.umd.edu/~ozbay/audience.pdf (accessed on 23 December 2012).
17. Cloud Security Alliance (2012a) Privacy Level Agreement (PLA) Working Group, https://cloudsecurityalliance.org/research/pla/
18. Cloud Security Alliance (2012b) Cloud Trust Protocol (CTP), https://cloudsecurityalliance.org/research/ctp/