Guiding Lights for Cloud Accountability

Martin Gilje Jaatun
University of Stavanger
Stavanger, Norway
Email: Martin.G.Jaatun@uis.no

INVITED TALK EXTENDED ABSTRACT

I. Introduction

Security concerns are often cited as the most prominent reason for not using cloud computing [1]. At the same time, customers of cloud users, especially end-users, frequently do not understand the need to control access to personal information. This is particularly evident in the context of social media, where the users are not the customers, but the product (being sold to marketers). On the other hand, some users might understand the risk, and yet have inadequate means to address it [2]. In order to make the Cloud a viable alternative for all, accountability of the service providers is key.

To be able to hold cloud service providers accountable for how they manage personal, sensitive and confidential information, there is a need for an orchestrated set of mechanisms: preventive (mitigating risk), detective (monitoring and identifying risk and policy violation), and corrective (managing incidents and providing redress) [3].

Suppliers within the cloud eco-system need to be able to differentiate themselves in what ultimately is a commodity market, and being able to offer accountability as part of the service provision will represent a competitive edge for service providers catering to discerning cloud customers [4].

II. Objectives

Objective 1 – facilitate choice (tools)
Objective 2 – control and transparency (tools)
Objective 3 – compliance (tools)
Objective 4 – recommendations and guidelines

III. Requirements

The starting point is that an accountable organization must commit to responsible stewardship of other people's data, requiring that it:

- defines what it does,
- monitors how it acts,
- remedies any discrepancies between the former two,
- explains and justifies any action.

These elements can be elaborated as follows.

1) An accountable organization must demonstrate willingness and capacity to be responsible and answerable for its data practices.
2) An accountable organization must define policies regarding their data practices.
3) An accountable organization must monitor its data practices.
4) An accountable organization must correct policy violations.
5) An accountable organization must demonstrate policy compliance.

In addition to the above, there is a need for accountability across the cloud service provision and governance chains, and not just in isolation for organizational cloud consumers or cloud service providers. Hence there is a need for provision of evidence of satisfaction of obligations right along the service provision chain, as well as aspects such as checking that partners are accountable too and that there has been proper allocation of responsibilities along the service provision chain. These requirements need to be reflected within the processes for organizations described above, but in addition there are implications in terms of the way that the accountability governance chains will operate, the scope of risk assessment and the ways in which other stakeholders are able to hold this organization to account. In complex, dynamic or global situations there needs to be a practical solution for data subjects to obtain both requisite information about the service provision and remediation.

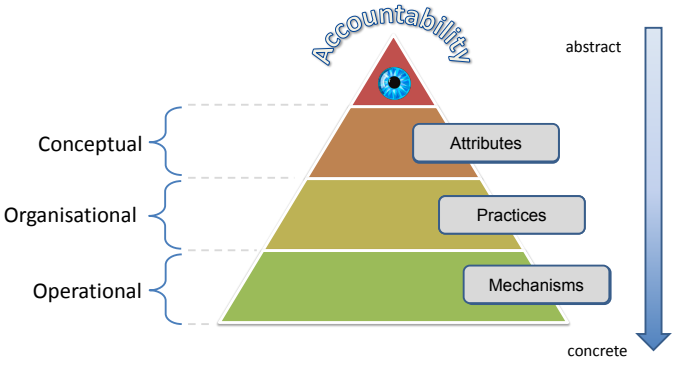

Fig. 1: A Conceptual Framework for Accountability

IV. Conceptual model

Our conceptual accountability model (see Fig. 1) elaborates on our definition accountability [3] by means of a set of

- *Accountability attributes:* conceptual elements of accountability applicable across different domains
- *Accountability practices:* emergent behavior characterizing accountable organizations (that is, how organizations operationalize accountability or put accountability into practices)
- *Accountability mechanisms:* diverse processes, non-technical mechanisms and tools that support accountability practices.

The core attributes of our accountability model are:

Transparency: the property of a system, organization or individual of providing visibility of its governing norms, behavior and compliance of behavior to the norms.

Responsiveness: the property of a system, organization or individual to take into account input from external stakeholders and respond to queries of these stakeholders.

Remediability: the property of a system, organization or individual to take corrective action and/or provide a remedy for any party harmed in case of failure to comply with its governing norms

Responsibility: the property of an organization or individual in relation to an object, process or system of being assigned to take action to be in compliance with the norms

Verifiability: the extent to which it is possible to assess norm compliance (i.e. a property of a system, service or process that its behavior can be checked against norms)

Appropriateness: the extent to which the technical and organizational measures used have the capability of contributing to accountability.

Effectiveness: the extent to which the technical and organizational measures used actually contribute to accountability.

To support and implement the main accountability attributes, we have developed a 'toolkit' [3] that forms the bottom layer in Fig. 1 and from which organizations can select as appropriate.

V. Discussion

Accountability is a difficult concept to define, and many European languages even lack a word for it. Numerous definitions of accountability exist in different domains (such as public policy, financial sector or enterprise operations) and each focuses on slightly different, context specific, aspects. Hence there is no consensus on a single definition. Ten years ago, Lampson [5] listed accountability as one of the three core objectives of having a security policy, alongside usage control and availability. It is thus surprising that accountability has had such a little impact on the Cloud services that are currently on offer.

The big Cloud providers that currently dominate the international market have such economic power that they effectively could ignore any European attempts at forcing them to run their business the way the European Union (EU) thinks they should. However, the EU General Data Protection Regulation (GDPR), with its significantly higher economic penalties, is poised to change that.

What we have presented is only part of the puzzle for modern services. The kind of tools that we have outlined [3] will need to be complemented by other security tools to make security and privacy stronger, for instance by enforcing confidentiality and anonymity where desired.

VI. Conclusion

In this paper we have presented fundamental requirements that we believe must be met by Cloud providers wishing to be accountable stewards of their customers' data.

The kinds of tools we have outlined [3] all contribute to an accountability-based approach, increasing transparency for Cloud users, and enabling Cloud providers to "do the right thing" with respect to accountability along the provider chain. We believe that providers soon will be required to justify their practices and mechanisms for handling customers' data to external parties [6], and that a certification scheme inevitably will emerge, much like we see for the Payment Card Industry Data Security Standard (PCI-DSS) [7].

Keywords—Cloud computing, accountability, security, privacy

Acknowledgments

This work has been partly funded from the European Commissions Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD) Cloud Accountability Project, and builds substantially on our previous journal paper [3]. Thanks to Siani Pearson, Frédéric Gittler, Ronald Leenes and Maartje Niezen for your collaboration in A4Cloud.

Biography

MARTIN GILJE JAATUN [SM] is an adjunct professor at the University of Stavanger, and a senior scientist at SINTEF Digital in Trondheim, Norway. He was the elicitation stream lead for the A4Cloud project.

References

[1] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 39, no. 1, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0045790612000870

[2] G. Cattaneo, M. Kolding, D. Bradshaw, and G. Folco, "Quantitative estimates of the demand for cloud computing in europe and the likely barriers to take-up," IDC, Tech. Rep. SMART 2011/0045 D2 Interim Report, February 2012.

[3] 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: //www.sciencedirect.com/science/article/pii/S0268401216301475

[4] J. Prüfer, "How to Govern the Cloud? Characterizing the Optimal Enforcement Institution that Supports Accountability in Cloud Computing," in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, vol. 2, Dec 2013, pp. 33–38.

[5] B. W. Lampson, "Computer security in the real world," *Computer*, vol. 37, no. 6, pp. 37–46, 2004.

[6] S. Pearson, "On the relationship between the different methods to address privacy issues in the cloud," in *On the Move to Meaningful Internet Systems: OTM 2013 Conferences*, ser. Lecture Notes in Computer Science, R. Meersman, H. Panetto, T. Dillon, J. Eder, Z. Bellahsene, N. Ritter, P. Leenheer, and D. Dou, Eds. Springer Berlin Heidelberg, 2013, vol. 8185, pp. 414–433. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-41030-7_30

[7] (2013) Payment Card Industry Data Security Standard. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0