Accountability for Cloud and Other Future Internet Services

Siani Pearson*, Vasilis Tountopoulos†, Daniele Catteddu‡, Mario Südholt§, Refik Molva¶, Christoph Reich‖, Simone Fischer-Hübner**, Christopher Millard††, Volkmar Lotz‡‡, Martin Gilje Jaatun[x], Ronald Leenes[xi], Chunming Rong[xii], and Javier Lopez[xiii]
*HP Labs, Bristol, UK
†ATC, Greece
‡CSA EMEA, UK
§École des Mines de Nantes, France
¶EURECOM, France
‖Hochschule Furtwangen, Germany
**Karlstad University, Sweden
††Queen Mary University of London, UK
‡‡SAP, Germany
[x]SINTEF ICT, Norway
[xi]Tilburg University, the Netherlands
[xii]University of Stavanger, Norway
[xiii]University of Malaga, Spain

***Abstract*—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 honour their obligations. The A4Cloud project will create solutions to support users in deciding and tracking how their data is used by cloud service providers. By combining methods of risk analysis, policy enforcement, monitoring and compliance auditing with tailored IT mechanisms for security, assurance and redress, A4Cloud aims to extend accountability across entire cloud service value chains, covering personal and business sensitive information in the cloud.**

I. Introduction

This poster describes the A4Cloud project [1], which commenced on October 1st 2012. A4Cloud is an Integrating Project (IP) in the EU's 7th Framework Programme (FP7), led by HP Labs in Bristol, and with partners from France, Germany, Greece, the Netherlands, Norway, United Kingdom, Spain and Sweden.

II. Accountability: the pre-requisite for a trustworthy Internet

The work of A4Cloud addresses several major trends that determine the development of information services in the Internet, both in the cloud and in more conventional networks: The ever-increasing quantities of data that are captured and used to provide value added services to customers; the increasing dependency on remotely provided third-party IT services; complex chains of responsibility; new trust and governance models; the consecutive complexity and difficulty to ensure traditional levels of user based transparency and control.

Cloud service users may hand over valuable and sensitive information to cloud service providers without an awareness of what they are committing to or understanding of the risks, with no control over what the service does with the data, no knowledge of the potential consequences, or means for redress in the event of a problem.

A4Cloud focuses on accountability [2] as the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services. The project aims to assist holding cloud (and other) service providers accountable for how they manage personal, sensitive and confidential information "in the cloud", and how they deliver services. This will be achieved by an orchestrated set of mechanisms: preventive (mitigating risk), detective (monitoring and identifying risk and policy violation) and corrective (managing incidents and providing redress). Used individually or collectively, they will make the Internet in the short- and longer-term more transparent and trustworthy for:

- users of cloud services who are not convinced by the balance of risk against opportunity
- their customers, especially end-users who do not understand the need to control access to personal information
- suppliers within the cloud eco-system, who need to be able to differentiate themselves in the ultimate commodity market.

A4Cloud will combine socio-economic, legal, regulatory and technical approaches and bring these together into a coherent and interoperable system of tools and services, enabling a shift to "Accountability-based approaches for trust

and security" in the cloud.

We will, for example, use sophisticated models combined with legal insight so that cloud service contracts can be selected that are appropriate to the context in which they are used, novel forms of measurement combined with data tracking technology to automate evidence gathering for compliance verification and machine-readable policies combined with innovative risk and impact modelling to add richer contextual provisions for consent to the use of personal information.

III. The Need for Accountability

Cloud services allow enterprises to outsource non-core aspects of their business to third parties. The complexity of the service provision eco-system may not be visible to an individual or business end user. However, it should ideally be possible to hold each provider accountable for how it manages, uses, and passes on data and other related information (e.g. metadata).

Over the past four decades, legislation and associated regulatory structures regarding the handling of personal data have become established in over sixty countries. Values and regulations vary across the globe but legislation typically creates obligations on service providers to engage in sound data governance and stewardship. What it cannot yet do is empower the end customer to make informed choices about selection of a service provider based on a solid understanding of the consequences of its choices.

Several major international reviews of these regulatory frameworks are currently underway, including that of the European Data Protection Framework, due for delivery within the lifetime of A4Cloud. Europe's strong position on data protection reflects European values on the protection of the rights of individuals, including privacy, and the A4Cloud approach will help to address societal fears about loss of privacy and data protection, especially with regard to "generation Facebook". The balance of power is firmly on the side of the service provider, since the user does not normally have the ability to negotiate redress, even if they knew it was theoretically possible. Only a large-scale multidisciplinary approach with industrial and scientific participation, addressing technical, legal, and socio-economic issues, can realistically achieve a significant change in the balance of power and instil confidence in the cloud business model. A4Cloud provides such an approach to accountability.

A chain of accountability allows the members of a cloud ecosystem to ensure that obligations to protect data are observed by all who process the data, irrespective of where that processing occurs. This not only applies when a data subject directly uses cloud services, but also when services are provided in an enterprise cloud setting.

Figure 1 illustrates the concept of a chain of accountability. Providers, implementing accountability mechanisms, provide customers with control and transparency over data in the cloud. The links in the chain of accountability depicted above are not simply technical mechanisms; they represent accountability relationships between supplier and customer that are embodied in contracts, must address regulatory obligations, ensure each

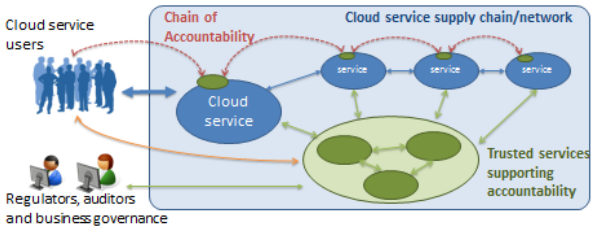

Fig. 1. A Chain of Accountability

partner uses interoperable policies and function efficiently and effectively for the supplier and the service user. Chains of accountability within the supply chain are possible as a result of deployment of accountability-enhancing mechanisms throughout the service network.

Trusted third party services provide monitoring, certification, trust modelling and other services that support accountability in the cloud. They enable providers to implement accountability, support users in assessing the trustworthiness of services, and give governance actors a way to check and monitor the use of data in the cloud.

IV. A4Cloud Objectives

A4Cloud has four interlocking objectives to bring users, providers, and regulators together in chains of accountability for data in the cloud, clarifying liability and providing greater transparency overall (Fig. 2. These objectives are the control and transparency of what is happening to your data, the ability to make informed choices of service and provider, demonstration of compliance and identification of breach and, finally, a way to implement accountability ethically and effectively.

A4Cloud aims to:

1) Enable cloud service providers to give their users appropriate control and transparency over how their data is used
2) Enable users to make choices about how cloud service providers may use and will protect data in the cloud

Fig. 2. A4Clouds objectives and their interconnections

3) Monitor and check compliance with users expectations, business policies, and regulations
4) Implement accountability ethically and effectively

The data-centric nature of cloud computing creates a tension between service suppliers who perceive that the business data they hold could be a strategic business resource and their customers who are increasingly aware of risks posed by the lack of control on data in the cloud. Service providers need a way to meet customer expectations that their interest in data will be protected with greater transparency and control, and therefore accountability, over what they do with data.

A. Objective 1

Develop tools that enable cloud service providers to give their users appropriate control and transparency over how their data is used, confidence that their data is handled according to their expectations and is protected in the cloud, delivering increased levels of accountability to their customers.

There are a number of potential innovative data-centric approaches based on rules which can capture users specifications, regulatory requirements, and business policies and their initial implementation or redeployment can be automated.

This provides an efficient way to meet customer demand for control over data and processes in the cloud, to keep them informed about when, how and by whom a certain resource has been used, and to implement changes when the customer, the business, or regulations require it.

There are challenges to applying these approaches in a complex technical landscape of cloud services in which infrastructure, platforms, and software are interlinked in complex supply chains. Providers may initially be resistant to giving their users a solution that alters their relationship with customers, while users need to understand what happens to data in the cloud and need to be able to specify rules that providers can implement. The contracts and SLAs between customer and supplier have to be aligned to the business processes for implementing security and data protection obligations, especially satisfying legal and regulatory requirements) should be clear.

If these issues can be addressed, then offering increased accountability in this way will give providers a way to differentiate themselves against their competition and to attract customers to their services. To this end, A4Cloud will provide:

- A Policy Configuration and Enforcement System to give (a) service providers a way to implement users' specification for data use, provide logs of how it is used in support of evidence collection, and pass obligations through the supply chain, e.g. for consent management (b) service users the possibility to interact with enforcement systems, specify and update policies (e.g. privacy preferences and consent) and correct/delete data online if permitted by the enforcement system.
- An Accountability Validation Tool that, using the framework and tools described above and in concert with external certification schemes, enables assertions about accountability to be made.

B. Objective 2

Create tools that enable cloud end users to make choices about how cloud service providers may use and will protect data in the cloud, and be better informed about the risks, consequences, and implementation of those choices.

To this end, A4Cloud will address worries about data proliferating in social media, and business concerns over the protection and control of proprietary data passed to cloud service providers. Businesses must consider their obligations under data protection regulation and corporate governance accounting when considering the use of services in the cloud. Formal risk and impact assessments are specialised, complex and time consuming activities, beyond the experience of smaller companies and individual users. There is currently almost no support to guide them through the daily decisions they will make about cloud services. Risk and trust models provide a foundation for supporting users in their interactions with cloud services. Hence, A4Cloud will provide a scalable risk methodology to meet the needs of organisations with complex systems and requirements as well as SMEs with simpler business environments and limited resources, and:

- A Risk Assessment Tool, based on a dynamically updated trust model reflecting service provider and user context, configured with different front ends for individual and business users, will provide users with an assessment of potential risks and impact of a cloud service.
- A Contract Support Tool, linked to the trust model, and based on the legal and regulatory approaches covered by the Accountability Framework, will support users and service providers in identifying the contract terms that are appropriate to the context of use.

C. Objective 3

Develop tools to monitor and check compliance with users' expectations, business policies and regulations.

Attributing responsibility for breach of contract or policy (identifying a breach and the entity responsible) requires great trust in the integrity of the attribution process. In a cloud service environment the problem is made more difficult due to the multiple possible paths taken by the data. It becomes as important to verify that the other paths were not faulty as it is to identify the fault. A comprehensive accountability monitoring solution must be capable of gathering the information needed to provide predictive assurance of compliance, notification of significant events and robust evidence. It must address the fundamental issue of preserving privacy and protecting confidential information whilst at the same time enabling attribution, supporting audit and maintaining information that must be retained for regulatory or commercial reasons.

- A system for Evidence Collection that captures, integrates and processes the information including logs, policies and context in a way that preserves privacy and confidentiality, and supports audit and attribution.
- A Remediation Tool that provides support for remediation and redress.

- A Policy Monitoring Tool that enables continuous configuration checking and keeps the users informed about where and how data is being used and whether policies have been followed.

D. Objective 4

Develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.

The concept of accountability is already present in finance and public governance, and is becoming more integrated into business regulatory programs as well as emerging privacy and data protection frameworks globally. Accountability can decrease regulatory complexity in global business environments, which is especially helpful in EU due to the complex matrix of national laws that makes compliance with data protection legislation especially difficult. Further, as the scale of data in the cloud increases, data processing becomes more sophisticated and cloud supply chains become more complex, the need for a coherent approach that works from the end-user right through the supply chain and that integrates the legal and regulatory dimension effectively and efficiently becomes even more pressing. An interdisciplinary co-design approach is core to A4Cloud, as the necessary change in underlying structures can only be achieved by means of a combination of legal, regulatory, policies, business procedural and technical measures that are integrated into a coherent framework for accountability.

A4Cloud will produce an Accountability Framework that will be a comprehensive specification for how to create accountability for cloud services, spanning regulatory, legal, technical, business and user issues. This will provide:

- a conceptual foundation for accountability, including clarification of core functions
- a reference architecture for implementing accountability
- recommendations and guidelines on data governance in complex, multi-tenant IT infrastructures and the cloud, including analysis of the revised EU Data Protection Framework, reports on legal and regulatory dependencies for effective accountability and governance and guidelines for privacy-friendly design, liability and cloud contracts
- models of risk, trust, human understanding and economic data governance in cloud ecosystems
- languages for interoperable accountability policies, with associated mapping of higher level policy constraints to machine readable policies to evidence provided within logs
- metrics for measuring accountability

V. Measurable outcomes

Within the timeframe of the project, A4Cloud will have:

- established its approach to accountability for cloud services by introducing results into a programme or track in at least one relevant initiative such as those in the Cloud Security Alliance.
- published its guidelines for how to achieve accountability which will have been presented to relevant business, regulatory, and standardisation groups.
- developed and tested prototypes of each of the tools and demonstrated to the relevant stakeholder groups how each supports the goal of accountability.
- demonstrated a prototype of a use case identified by working with various stakeholder groups early in the project, that integrates the full set of tools, showing how A4Clouds approach to accountability works in practice, along with evidence that the use case is of more general interest due to its accountability properties, importance to stakeholders, etc.
- provided training for developers, cloud service providers and users, and business legal and regulatory communities, on the guidelines and tools for implementing accountability.
- published scientific results in at least four major journals and at four major conferences covering each of the disciplines, technical, regulatory and socio-economic addressed by the project.

VI. Conclusion

A4Cloud solutions will support service providers in preventing breaches of trust by using audited policy enforcement techniques, assessing the potential impact of policy violations, detecting violations, managing incidents and obtaining redress.

A4Cloud will have a lasting impact on the competitiveness of the European ICT sector by addressing major perceived barriers to trustworthy cloud-based services. These include concerns about complexity and enforceability of legal, regulatory and contractual provisions, socio-economic and corporate constraints, issues of trust for service-users such as risk-mitigation, privacy, confidentiality and transparency, and operational challenges such as interoperability and enforcing and monitoring compliance.

Acknowledgment

The A4Cloud project is funded by the EU's 7th framework programme. The A4Cloud partners are: HP Labs (coordinator), Athens Technology Center, Cloud Security Alliance EMEA, École des Mines de Nantes, EURECOM, Hochschule Furtwangen, Karlstad University, Queen Mary and Westfield College - University of London, SAP, SINTEF, Tilburg University, University of Stavanger, and University of Malaga. Except for the coordinator's representative, authors are listed alphabetically according to the name of their institution. We gratefully acknowledge the efforts of the numerous other individuals from the partner organisations who contributed to this text.

References

[1] A4Cloud Project Web. [Online]. Available: http://www.a4cloud.eu
[2] S. Pearson, "Toward accountability in the cloud," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 64 –69, july-aug. 2011.