Towards Accountable Services in the Cloud

Volkmar Lotz and Anderson Santana de Oliveira

SAP Research, France
{volkmar.lotz,anderson.santana.de.oliveira}@sap.com

1 Control as a Foundation of Accountability in the Cloud

Today, it is highly attractive for businesses to use the cloud as the platform to run their enterprise IT and business transactions: scalable infrastructures provide flexibility and cost efficiency, while the participation in service ecosystems allows building applications on demand by exploiting the vast amount of functionality that is ready to be consumed over the cloud. But taking advantage of all these opportunities is still obstructed by trust concerns. Handing over sensitive data to a third-party for processing, together with the complexity of the service ecosystem, the lack of visibility of its structures and the increased dependency on service providers constitute a non-negligible risk for businesses.

This risk can be mitigated by providing accountability in the cloud. By accountability, we refer to the ability of a service consumer to identify who was handling their data in which way and under which context (for instance, location or business purpose) and to provide evidence for that to other parties. For instance, a privacy policy may restrict the usage of data handed over to a service to the context of the actual transaction, and not permit further data sharing with, say, a profiling service used by the service provider. In the cloud, these requirements do not only refer to a direct relation between service consumer and provider, but reach out to a number of additional ecosystem entities, including the platform provider, additional providers of value added services, data center operators etc. The more complex the structure, the more difficult it gets to provide the necessary visibility of events and activities (e.g., who receives data and may be able to store a copy). Additional means to enforce certain behaviors need to be in place to support accountability and, ultimately, trust in the cloud. Given the above, transparency and control turn out to be the major constituents of accountability. The two principles are complementary: while transparency contributes to the detection of policy violations and allows identifying the initiator, control is aiming at preventing such violations, thus mitigating risk. Accountability in the cloud relies on both principles, since none of them can achieve the goal on its own. Transparency is often difficult to achieve due to the complexity of structures, the speed of their change and the sheer amount of data and events. Control, on the other hand, may require ownership of infrastructure and platform components or the existence of specific technical components to enforce it.

In this paper, we focus on control for service-oriented architectures and review which level of control can be achieved across different layers and views, in

R. Meersman et al. (Eds.): OTM 2012, Part II, LNCS 7566, pp. 470–474, 2012.

particular, when services are defined, deployed, orchestrated and consumed over a Platform as a Service offering.

We use privacy as an example for a subject where accountability is critical already today, following data protection regulations. Based on these concepts, we give an outlook on future work towards accountability in the cloud.

2 Achieving Control in the Cloud Today

Establishing control is one of the first steps towards accountability in today's cloud, particularly because of the limited transparency of the price-focused offers made available by the majority of the existing providers. In this context, operational details are hidden by obscure contracts and by the lack of supporting services. The end customer must be able to establish a model of the cloud's behavior, in order to customize a set of mechanisms that enact control on: how data is being handled, how processes are executed, and by whom. Allowing the cloud costumers to have control allows to increase the level of trust as to the expected behavior of the services and of the vendor. Taking such step may also be fundamental for the vendor to meet organizational compliance, and/or regulatory requirements.

As service-oriented architectures (SOAs) are central to the cloud delivery models, we introduce a model for aspect-oriented composition for SOA, which is able to provide the level of control necessary in today's cloud. It is founded on the concepts of horizontal and vertical compositions, allowing to reach control at different abstraction levels, thus different cloud delivery models.

SOA can be seen as a continuum of different components at different levels of system abstraction, like the infrastructure, platform/middleware, and software viewpoints, as illustrated in Figure 1. The fundamental assumption of SOA, where the service consumer needs not to worry about service implementation details and the underlying infrastructure: the availability of a software view to the application designer makes it possible to hide the unnecessary complexity in the implementation of business services originating from the underlying layers. Lower layers enforce different business logics, security policies, or functional constraints and have to be coordinated together with the execution of the application in order to give access to services and resources of the infrastructure[2].

Functional and specifically non-functional requirements (such as security, trust, QoS) have to be consistently managed throughout the cloud landscape, thus involving complex service orchestrations and choreographies. The implementation of these cross-cutting concerns often involve invasive modifications [3], *e.g*, to enable accountability related functionalities that depend on and require modifications to low-level infrastructure, for instance secure logging.

Therefore, cloud services, as in SOA, are also subject to evolution using *vertical composition*, that is, the coordination of multiple architectural layers over which the SOA is deployed, including operating systems, application servers, enterprise service buses, orchestration engines, etc. In contrast, *horizontal composition* consists in high level service compositions towards the achievement of business goals, typically expressed as orchestrations or choreographies.

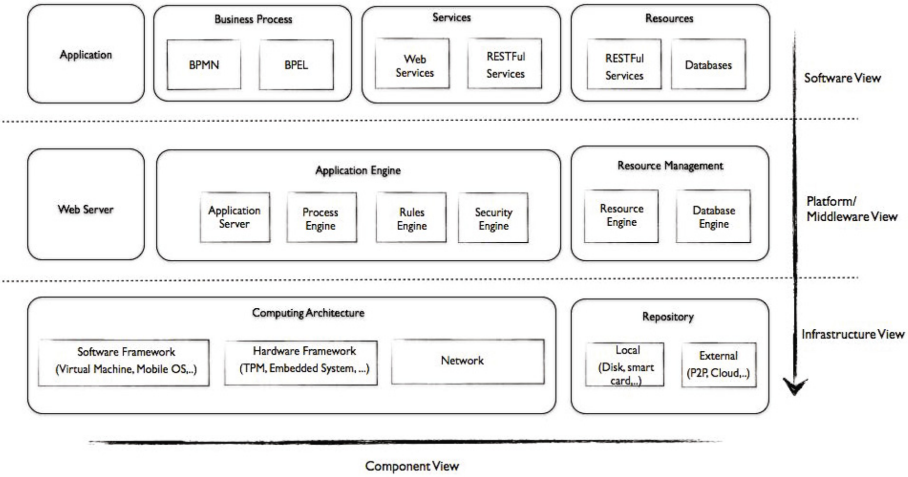

Fig. 1. A synthetic overview of Multi-layered Service-Oriented-Architecture

In order to provide the necessary level of control in the cloud, we designed an aspect model [1], able to handle vertical and horizontal cross-cuttting concerns based on the pointcut-advice concepts for aspects, with some important extensions. The pointcut-advice model is characterized by three main abstractions: aspects, pointcuts and advice that together provide means for the concise definition and effcient implementations. Services and their compositions can be seen as grayboxes in our formal message-passing model *i.e*, only external interfaces are visible and the aspects can only handle message interchange. However services can also be seen as whiteboxes, by adding rules to the model to govern how the "agents" evolve internally, such as process algebra, for instance. This allows one to suitably describe aspects, whether the actual code for the service is available or not.

Below, we focus on the platform layer of the Figure 1 and use privacy concerns as an example, to illustrate how accountability can be implemented via vertical/horizontal aspects compositions. The motivation behind privacy for this example are twofold, first, it is an important component of accountability, and second, that privacy policies are immediately understood in the context of cloud and SOA.

Enforcing Privacy Obligations. From a compliance point of view, it is important to impose control on cloud applications to ensure the execution of obligations when dealing with personal data. We presented in [4] how our aspect model can provide invasive modifications needed to associate events related to data handling to accountable entities in a service execution.

To ensure control in data handling, we provided modifications at the three views represented in Figure 1. The software view is impacted to ensure correct handling when personal data is transmitted in a service composition, for example, when a

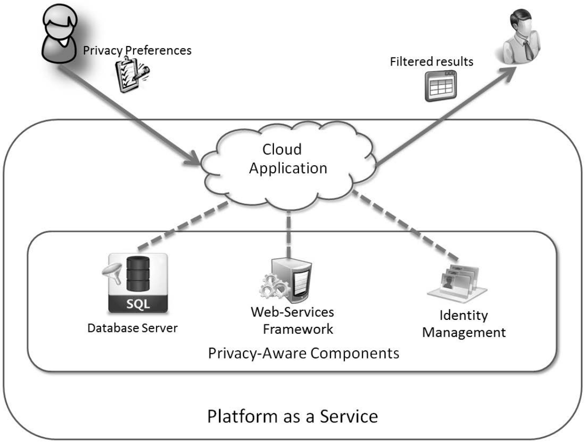

Fig. 2. Aspects control the behavior of the PaaS components

business process transmits customer data in a web service invocation. The obligation to respect the user preferences may require an alert to be sent to the data owner, or even that the message transmission to be aborted, depending on the purpose of the service call. At the platform view, some components can be invasively modified to filter out data that the end-user does not wish to share with the service provider. At the bottom layer, or the infrastructure view, the enforcement of the integrity of the logging takes place. That will ensure the reliability of the accountability information collected.

This use case is represented in Figure 2. The enforcement mechanisms are provided by the platform with the help of our approach for aspect-oriented programming where aspects can be manipulated at the process and at the platform level, making components "privacy aware". That approach gives possibility to maintain a more flexible configuration of the enforcement mechanisms. The mechanisms interpret end-user preferences regarding handling of the personally idetifiable information, presented in form of opt-in or opt-out choices among available privacy policies of a cloud application, and later perform the required actions (filtering, blocking, deletion, etc), but also to attach identity information about the entities responsible for action execution on a given piece of personal data. The platform provider can in this way achieve built-in compliance with t he personal data protection regulations in a transparent way.

3 Towards Accountability in the Cloud

We presented here some initiatives to provide control in existing cloud landscapes such that one can achieve a certain degree of accountability. In the quest for building accountability in the cloud for a large set Cloud and IT service providers, the upcoming EU Project A4Cloud 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. 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 aims to improve the acceptability of cloud-based infrastructures where critical data is perceived to be at risk. It will develop techniques for improved trustworthiness of cloud ecosystems as prerequisite for accountability. Therefore it will create policies and tools that enforce responsibilities while striking a balance between transparency and privacy, and determine issues and constraints for regulators, corporate and institutional service providers, users, and their end-users. 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.

References

1. Allam, D., Bourdier, T., Douence, R., Grall, H., Royer, J.C., Südholt, M., de Oliveira, A.S.: Language definition and aspect supportcextension of the service model for security and aspects. Deliverable D1.3, The CESSA project (May 2011), `http://cessa.gforge.inria.fr/lib/exe/fetch.php?media=publications:d1-3.pdf`
2. Idrees, M.S., Serme, G., Roudier, Y., de Oliveira, A.S., Grall, H., Südholt, M.: Evolving Security Requirements in Multi-layered Service-Oriented-Architectures. In: Garcia-Alfaro, J., Navarro-Arribas, G., Cuppens-Boulahia, N., de Capitani di Vimercati, S. (eds.) DPM 2011 and SETOP 2011. LNCS, vol. 7122, pp. 190–205. Springer, Heidelberg (2012)
3. Mejia, I., Südholt, M.: Structured and flexible gray-box composition using invasive distributed patterns. International Journal on Computer Science and Information Systems 6, 13 (2011) ISBN = ISSN: 1646-3692
4. Yu, P., Sendor, J., Serme, G., de Oliveira, A.S.: Automating privacy enforcement in cloud platforms. In: Pietro, R.D., Herranz, J. (eds.) 7th International Workshop on Data Privacy Management. Springer (2012)