Towards trust management for cloud-based ecosystems

Sini Ruohomaa, Lea Kutvonen
University of Helsinki
P.O. Box 68, FI-40014 University of Helsinki, Finland
firstname.lastname@cs.helsinki.fi

Abstract

Inter-enterprise collaborations allow service providers to focus on their key competences while providing a composed service to end customers. The actors involved must determine whether the gains from participating outweigh the risks of depending on other autonomous collaboration participants, in order to make trust decisions on their willingness to collaborate. We define trust as the extent to which an actor is willing to participate in a given action with a given partner, considering the risks and incentives involved.

In this paper, we present two high-level alternatives for trust management architectures for cloud-based service ecosystems: closed collaboration environments and open service ecosystems. Closed environments, such as traditional virtual organization breeding environments, are often built around a hub actor, centrally managed and apply pre-formed trust relationships in determining who is allowed into the breeding environment. Open service ecosystems, in contrast, allow service providers to enter the ecosystem by publishing a valid service offer, and trust relationships are formed and evolve within the ecosystem. We discuss the implications these choices have on further architecture refinement, and compare the strengths and weaknesses of the approaches, including their infrastructure needs, viability and ability to scale up in size.

Keywords: trust management, cloud, reputation, inter-enterprise collaborations, open service ecosystems

1 Introduction

As the need for networked business increases, so does the need for supporting inter-enterprise collaborations; they allow service providers to focus on their key competences while providing a composed service to end customers.

In traditional service ecosystems, enteprises aim for developing services and service compositions across enterprise boundaries in a secure way by ensuring a shared development and operational environment. At present, the burden of the development and operational environment, as well as ensuring of interoperability, is often placed on cloud computing, as part of the support of SaaS (Software as a Service) and PaaS (Platform as a Service) concepts [1, 10]. Despite only having software construction concepts available, cloud computing is left to support business-level needs with them as well, even in cases where business processes can be repeatably utilized as templates for new business cases in the style of BPaaS (Business Process as a Service) [6] and other alternatives.

In open service ecosystems, the management of the inter-enterprise collaborations must be present and aligned with business-level concepts. With this in mind, we define cloud-based open service ecosystems as environments for setting up, operating, and managing service-oriented inter-enterprise collaborations, supported by technology-platform independent infrastructure and allowing the collaborations to effortlessly cross the boundaries of multiple cloud-computing environments. From the point of view of this paper, each cloud provides a technical platform for building

support functionalities or business application level services required in a service ecosystem. For this reason, only public clouds are considered. We focus our concern on management of the distributed processing and involvement of the business-level governance needs.

In particular, from the end customer point of view, outsourcing notable parts of business process functionality create difficult challenges in terms of trust and privacy management. We define trust as the extent to which an actor is willing to participate in a given action with a given partner, considering the risks and incentives involved. The actors involved must determine whether the gains from participating outweigh the risks of depending on other autonomous collaboration participants, in order to make independent trust decisions on their own willingness to collaborate.

The goal of our research is to explore trust management solutions in an environment where services from independent providers are discovered and chosen to collaborate for the purpose of fulfilling a business model. In this paper, we present two high-level alternatives for trust management architectures for cloud-based service ecosystems: closed collaboration environments and open service ecosystems. Closed communities, such as traditional virtual organization breeding environments, are often built around a hub actor, centrally managed and relying on pre-formed trust relationships to determine who is allowed into the breeding environment. Open service ecosystems, in contrast, allow service providers to enter the ecosystem by publishing a valid service offer, and trust relationships are formed and evolve within the ecosystem.

We discuss the implications these architecture choices have on further architecture refinement, and compare the strengths and weaknesses of the approaches, including their infrastructure needs, viability and ability to scale up in size.

Section 2 presents the closed and open collaboration architectures and the lifecycle of an inter-enterprise collaboration. Section 3 presents how objective reputation information is established to drive trust decisions. Section 4 explores the implications that the choice between closed and open architecture entails, and Section 5 concludes.

2 Architecture and collaboration lifecycle

Trust management systems support risk evaluation and making decisions on whether a collaboration is worth joining and continuing in. Collaboration experiences are shared through reputation systems in order to help establish inter-enterprise collaborations in a service ecosystem where first-hand experiences are not always available. This section discusses two alternatives for trust management and the underlying collaboration architectures, and presents the lifecycle of an inter-enterprise collaboration to bind the trust management support into its different stages.

2.1 Closed collaboration environments and open service ecosystems

On a high level, we can divide approaches to trust management for inter-enterprise collaborations into two categories: closed collaboration environments focus effort on setting up a perimeter defense and selectively grant membership in the environment itself, while open service ecosystems focus on distributed defense, where every service fends for themselves; membership in the open service ecosystem is available to essentially all interested actors.

In closed collaboration environments, depicted in Figure 1, new actors are admitted into the virtual breeding environment based on pre-existing trust relationships. Actors within the environment are trusted, and additional resources are not spent on a continuous screening process. This model most resembles traditional access control: once an actor has been centrally authorized, it is expected not to misbehave. The gatekeeper typically focuses on authentication: it ensures that the origin

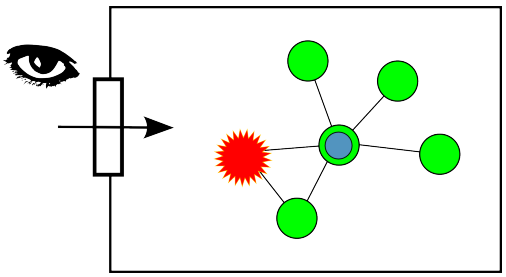

Figure 1. A closed collaboration environment.

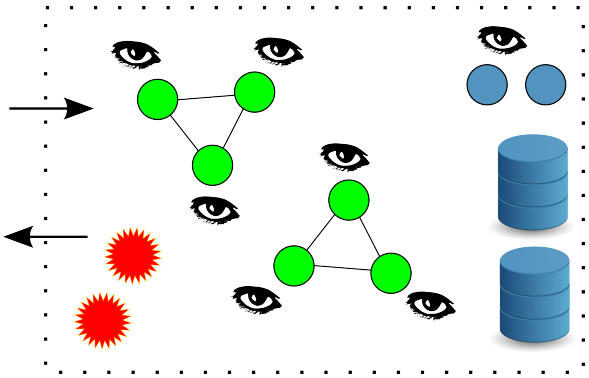

Figure 2. An open service ecosystem.

of a service request is authorized. The problem of correctly mapping the identity of a service to other, real-world identities is particularly relevant when authorization decisions are tied to actors providing the services rather than the service instances themselves.

In open service ecosystems, depicted in Figure 2, there are no trust-based limitations on entering the ecosystem. Defense is distributed into each autonomous service making their own trust decisions. As actors within the environment are not inherently trusted, continuous and localized monitoring must be applied to ensure that the risks do not grow too high [7]. Both collaboration contracts and the experience information shared through reputation systems are primarily attached to specific services, rather than the identities of their specific providers.

We see the closed and open architectures as having developed around different business patterns. A closed environment can serve a supply chain built around a hub actor and its subcontractors, for example. The subcontractors have specialized on participating in the hub actor's business process, and their systems are integrated together based on the needs of the supply chain. A strategic network of partners has been formed beforehand over the years, and the collaborations reflect these pre-formed relationships. The infrastructure needed to govern the collaboration is built into the hub actor's service, and decision-making power is delegated to it.

An open service ecosystem, on the other hand, can serve a large community of competing and independent services, who can each participate in multiple collaborations simultaneously and change partners opportunistically based on the best available offers. At all times, the ecosystem contains collaborations at different stages of their life cycle, following different setups of reusable business processes. Shared collaboration experiences support peer-based control in the ecosystem, where continuously misbehaving actors are shut out of future collaborations.

In order to support these evolving activities, the open service ecosystem requires additional infrastructure: repositories of shared information, such as service offers and collaboration models [4], and infrastructure services, such as a populator [3] to match together a set of interoperable service offers to fill the roles of a collaboration model, contract negotiation support [3], and a reputation system to store reports of breaches of contract and support peer control in the ecosystem [8]. Reputation information encodes past behaviour, and provides a central input for risk evaluations. All actors perform private trust and risk analysis on which collaborations to join and whether to continue in a collaboration [7]. The economies of scale that make infrastructure service provision sustainable rely on a large number of actors in the ecosystem, which is why it is particularly important to ensure that open service ecosystems can scale up in size.

In practice, the division is not strict, but does have implications on how the collaboration can evolve. While a closed collaboration environment does not have to be strictly hiearchic, its reliance on pre-formed trust relationships and tight integration between the services makes the struc-

ture rigid: adding new collaborators to replace old ones provides overhead both in background checking and integration work. An open service ecosystem can similarly support collaborations based on strategic networks, while evolution, such as changing collaboration models and the collaborators, is not disruptive for this architecture approach. We discuss the trust-related infrastructure support in different parts of the collaboration lifecycle in the following section.

2.2 Trust management support in the collaboration lifecycle

An inter-enterprise collaboration can be divided into four stages, as depicted in Figure 3: population, negotiation, operation and termination. In closed, specialized environments, the collaboration lifecycle is often also the lifecycle of the community: there is only one collaboration in this kind of community, although it can be repeated. Service ecosystems, in contrast, contain multiple collaborations at different stages of their life cycle, and following different business processes.

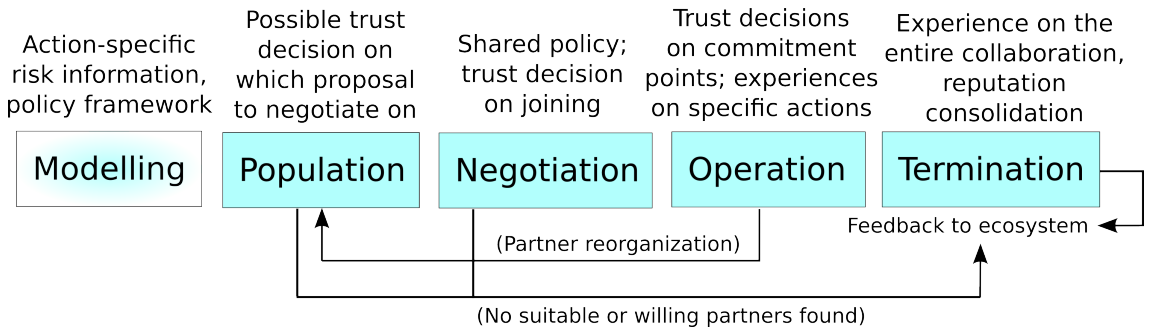

Figure 3. Trust information and decisions at different phases of the collaboration.

The four stages of a specific collaboration instance are preceded by a modelling phase, where the type of collaboration, its structure and process, and the individual offered services are specified. Collaboration models provide a framework for best practices on a given type of collaboration, and domain experts producing these models can formulate what kinds of risks are inherent in different actions within the collaborations. For example, when buying goods, an availability query is a low-risk action that does not warrant extensive background checking, while paying for the goods commits actual resources to the collaboration, with the risk that the goods are never received.

In the population phase, a given collaboration type is populated with partners providing a specific part of the joint effort, and the interoperability of the participating services ensured. The collaboration initiator may use a risk evaluation backed by reputation information to decide which of the technically possible different population options it is willing to start negotiations on. If the proposed actors are unknown to it from before, it bases its trust decisions on reputation information shared by third parties.

In the negotiation phase, the collaboration contract is refined and agreed upon by the proposed participants, each of which must estimate their risks and gains and make a trust decision on whether they are willing to join the collaboration. The contract brings with it a shared policy that the collaborators must follow on threat of compensation demands from other participants, and eventual litigation if the conflicts cannot be otherwise resolved.

In the operation phase, the local monitors controlled by each participant collect experience information on how the collaboration progresses, and whether other members follow the shared policy specified in the collaboration contract or break it in their interactions with the observing member service. Violations such as delays in delivery can be compensated; these processes are defined in the contract. If a contract violation is severe or not appropriately compensated, it may trigger a partner reorganization, where the offending service is removed and replaced with a new one.

Whenever an actor must commit new resources to the collaboration, it updates its the risk evaluation on that collaboration based on the latest experience information and makes a new trust decision on whether to continue with the collaboration or to cut losses and withdraw from it.

The termination phase is reached 1) when the collaboration has run its natural course or achieved its goal, 2) due to an unrecoverable failure, or 3) when suitable and willing partners cannot be found in the population and negotiation phases. In it, experience on the entirety of the collaboration is formed by the collaborators, transformed into reputation information and distributed to other members of the ecosystem. Long-lived collaborations may be divided into more or less independent epochs, whose completion triggers the reputation dissemination process periodically during the operation phase. Feedback flows back to the service ecosystem both on the performance of individual services, in the form of reputation information, and as e.g. an observed need to adjust the collaboration models.

3 Decision-making based on objective reputation information

The reputation information that encodes the past performance of a service can be divided into two categories: first-hand and shared, third-party reputation information. First-hand experiences gained from earlier collaborations with the target service are the most credible and semantically clearest, but they are expensive to gather due to the requirement of first collaborating with the target. Shared experiences are gained from third parties who have collaborated with the target service before, and distributed through a reputation system. Each service using such shared information must evaluate the credibility of the information locally before basing decisions on it.

Local credibility analysis of shared reputation information is needed so that services can protect themselves against fabricated reputation information [9]. These kinds of fabrications can take the form of undeserved positive experiences, or undeserved negative experiences towards competitors, for example. In addition, deserved positive experiences may be omitted and the publication of deserved negative experiences hampered. In the open service ecosystem, a good reputation increases the chances of a service to be chosen for a collaboration, which makes it an attractive target for attacks such as confidence fraud [2].

A reputation system has two tasks. First, from the perspective of a single enterprise, it provides information to support trust decisions for each individual service. This helps participants in the reputation system to find new partners and to steer clear of unreliable services.

Second, from the ecosystem perspective, it introduces a form of peer control, where misbehaviour towards other actors or the ecosystem infrastructure itself is punished through reputation loss. To achieve this task, fraudulent reputation information must also be detected and its sources punished [8].

In order to detect fraudulent reputation information, we must specify the differences between good behaviour and misbehaviour in an objective way that the ecosystem participants can agree on. We have therefore chosen to define misbehaviour as breaches of collaboration contracts: the contract encodes a signed, non-repudiable agreement of how the different participants in the collaboration should conduct themselves, and therefore forms an objective basis for reputation reports.

In order to align technical-level monitoring with the business agreement represented by the contracts, the contract representation itself must formally encode the business processes that are followed in the collaboration: for example, what messages should be exchanged at what time, and how compensation is handled if the default process cannot be fulfilled. For example in the Pilarcos open ecosystem infrastructure, this information is contained in the collaboration models produced during the modelling phase discussed in the previous section, and the agreed-upon models are

included in the collaboration contracts, or eContracts [4].

As a final step, due to the decentralized nature of open service ecosystems, we cannot rely on a trusted third party to monitor the entire collaboration, and must place monitoring within the domain of control of each service. Monitors controlled by individual service providers are subjective and cannot be blindly trusted by all members of the ecosystem. The word of a single service provider transacting with another service is not therefore sufficient as a basis for fair punishment: a non-repudiable audit trail must be established.

We have proposed a solution for building the audit trail based on optimistic fair receipt exchange [8]. In the defined protocol, the transacting services exchange signed receipts to acknowledge different actions that have been completed. If either participant refuses to provide a receipt, the other party can call upon a third-party witness, a kind of message-level notary, which is then included in the protocol. The notary can provide neutral evidence on whether the receipt exchange protocol was followed or, if not, who violated it. A similar centralized approach has been proposed earlier for electronic marketplaces, which only support very basic transactions for buying goods [5]; our proposal generalizes the solution to be applicable for more complex business processes as well, and discusses the details of how reputation information is backed up by the receipt evidence in a way that allows fraudulent reports to be rebutted and sources of misinformation punished [8].

In summary, objective reputation information is needed to support risk evaluations and peer-based control in inter-enterprise collaborations, particularly in open service ecosystems. In order to achieve objectivity, misbehaviour must be defined in the contracts that are negotiated and signed at the beginning of each collaboration. In closed collaboration environments, the transfer of control from the subcontractors to the contractor may extend to allowing the hub actor both monitor access to the entire collaboration, and to replace partners with a one-sided decision. Strongly centralized decision-making is not a viable solution for an open service ecosystem, however.

4 Implications of architecture choice

We summarize the differences between open and closed architectures in Table 1.

	Closed collaboration environment (e.g. subcontracting)	**Open service ecosystem** (e.g. networked business)
Partner selection	Fixed strategic network	Opportunistic; many options
Trust decisions	Verification of out-of-band authorization (e.g. certificates); updates made externally	Risks vs. incentives, based on reputation data; self-adjusting authorization
Trust evolution	Outsourced, replicates pre-existing trust relationships	New experiences are encoded into reputation
Monitoring, governance	Centralized around hub actor acting as "judge and jury"	Distributed and contract-based, no all-seeing observer
Collaboration support	Single collaboration format, repeatable, no evolution	Repositories of different collaboration types, versioning
Role of infrastructure	Minor: ad hoc integration, simple one-time solutions	Necessity: model-based interoperability, reusability

Table 1. Comparison of closed collaboration environments of low maturity and open service ecosystems.

From the point of view of service ecosystem maturity models, a closed collaboration environment built around a single collaboration represents an early stage ecosystem. It has a reasonably low setup cost, which consists mostly of integration effort between the actors. The solution is inflexible,

however, and provides poor support for collaboration evolution or partner changes.

A more flexible and sustainable service ecosystem requires additional infrastructure, and is therefore more costly to set up: its collaboration models should be reusable between different sets of services, and key support activities such as monitoring cannot depend on all actors in the ecosystem trusting a specific third party. The open service ecosystem benefits from economies of scale, instead: the cost of setting up any given collaboration is considerably lower than for a specialized solution, where the cost is repeated whenever the collaboration model or collaborators change.

In addition, the distributed governance model that does not depend on centralized control leaves the actors with more autonomy on their own choices, which we find to be a key factor in the acceptability of the ecosystem. The tightly-knit contractor-subcontractor connection can easily become too symbiotic to be viable in the long term, as smaller subcontractor businesses can grow overly dependent on the contractor enterprise; this is not beneficial to the contractor either. Loose coupling between collaborating services in the ecosystem and model-based interoperability provides more space for the market to evolve in response to changes in the business environment.

Finally, as the model-based infrastructure aligns business-level goals and concepts with technical-level solutions, it provides a solid basis for automation of routine activities, such as repeated trust decisions during the collaboration when the reputation information has not seen major changes. This reduces operation and setup costs further. While increased automation is theoretically possible for closed environments as well, setting up the models to support it becomes costly: it is more difficult for a closed environment to collect a critical mass of the by necessity mutually trusted actors to benefit from economies of scale to an equal degree. Instead, to implement more technologically flexible but still selective breeding environments between members of a strategic network, it would seem to be more advantageous to set up virtually closed collaboration environments within an established open service ecosystem, and reuse the models available there.

When we consider how the two approaches can be supported by infrastructure in a cloud computing platform, we find two obvious targets for service provision in the context of trust management. In a closed collaboration environment, the gatekeeper making decisions on who is allowed to enter the environment essentially provides trust decisions as a service; decision-making is outsourced to it by the participants. For an open service ecosystem, decision-making remains distributed to each autonomous service, while reputation systems to disseminate experience information could be packaged into a form of reputation as a service. For inter-enterprise collaborations that span over multiple cloud platforms, we will need mechanisms that can handle such distribution; while the dissemination and collection of reputation information from different sources is a service that can be provided independently on different cloud platforms, the perimeter defense established for closed environments becomes unwieldy for collaborations that cross cloud borders, considering e.g. that any distributed decision-making points must all agree in their decisions.

5 Conclusion

We have discussed the possibilities and implications of choosing a closed or open trust management architecture in an environment where services from independent providers join together to implement a business model. We have established that closed collaboration environments with low infrastructure investments are suitable for some collaboration patterns, but that the open service ecosystem provides a more flexible and sustainable approach, particularly when considering potential changes in the business situation for a single enterprise or a market domain.

The open service ecosystem is based on infrastructure that must be trusted to fulfil its function similarly to how other participants in the collaboration are trusted to provide a service. In the

meanwhile, actors are not forced to trust neither the infrastructure nor other collaboration participants to make decisions for them: the final policies are set by and specific to a given service. These policies may even disagree with the collaboration contract, if the compensation process represents a smaller cost to the service provider than fulfilling the contract would.

We claim that the independence of decision-making ensured by the open service ecosystem makes it more acceptable for businesses, and that the peer-based control provided by reputation systems helps it scale in size even in the presence of misbehaving actors. The loose coupling between collaborators and the model-based interoperability approach leaves space for model evolution, which allows the ecosystem as a whole to evolve based on the market situation. This improves its long-term viability in comparison to specialized collaboration environments.

The cost of infrastructure establishment for open service ecosystems is a key reason why simpler ad hoc solutions appear more attractive when studied in the short term, while the flexibility gained from establishing this kind of infrastructure and viable business models for operating it pays itself back over a longer period. Where specialized solutions must be rebuilt from scratch repeatedly, the open service ecosystem infrastructure evolves through reconfiguration.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. A view of cloud computing. Communications of the ACM 53 (Apr. 2010), 50–58.
2. Gollmann, D. From access control to trust management, and back — a petition. In Trust Management V; 5th IFIP WG 11.11 International Conference, IFIPTM 2011; Proceedings (Copenhagen, Denmark, June/July 2011), vol. 358 of IFIP AICT, Springer, pp. 1–8.
3. Kutvonen, L., Metso, J., and Ruohomaa, S. From trading to eCommunity management: Responding to social and contractual challenges. Information Systems Frontiers (ISF) - Special Issue on Enterprise Services Computing: Evolution and Challenges 9, 2–3 (July 2007), 181–194.
4. Kutvonen, L., Ruokolainen, T., and Metso, J. Interoperability middleware for federated business services in web-Pilarcos. International Journal of Enterprise Information Systems, Special issue on Interoperability of Enterprise Systems and Applications 3, 1 (Jan. 2007), 1–21.
5. Li, Q., Martin, K. M., and Zhang, J. Design of a multiagent-based e-marketplace to secure service trading on the Internet. In Proceedings of the 13th International Conference on Electronic Commerce (Liverpool, UK, Aug. 2011).
6. Papazoglou, M. P., and van den Heuvel, W.-J. Blueprinting the cloud. IEEE Internet Computing 15, 6 (2011), 74–79.
7. Ruohomaa, S., and Kutvonen, L. Trust and distrust in adaptive inter-enterprise collaboration management. Journal of Theoretical and Applied Electronic Commerce Research 5, 2 (Aug. 2010), 118–136.
8. Ruohomaa, S., and Kutvonen, L. From subjective reputation to verifiable experiences - augmenting peer-control mechanisms for open service ecosystems. In Proceedings of the 6th IFIP WG 11.11 International Conference on trust Management (IFIPTM 2012) (Surat, India, May 2012). To appear.
9. Yao, Y., Ruohomaa, S., and Xu, F. Addressing common vulnerabilities of reputation systems for electronic commerce. Journal of Theoretical and Applied Electronic Commerce Research 7 (Apr. 2012), 1–15. To appear.
10. Zhang, Q., Cheng, L., and Boutaba, R. Cloud computing: state-of-the-art and research challenges. Journal of Internet services and applications 1, 1 (Apr. 2010), 7–18.