Information Security in Business Intelligence based on Cloud: A Survey of Key Issues and the Premises of a Proposal

Elena Jaramillo, Manuel Munier, Philippe Aniorte

Information Security in Business Intelligence based on Cloud: A Survey of Key Issues and the Premises of a Proposal

Elena Jaramillo, Manuel Munier, and Philippe Aniorté

LIUPPA, Univ Pau & Pays Adour, France
{gloriaelena.jaramillorojas, manuel.munier,
philippe.aniorte}@univ-pau.fr

Abstract. More sophisticated inter-organizational interactions have generated changes in the way in which organizations make business. Advanced forms of collaborations, such as Business Process as a Service (BPaaS), allow different partners to leverage business intelligence within organizations. However, although it presents powerfull economical and technical benefits, it also arrises some pitfalls about data security, especially when it is mediated by the cloud. In this article[1], current aspects which have been tackled in the literature related to data risks and accountability are presented. In addition, some open issues are also presented from the analysis of the existing methodologies and techniques proposed in the literature. A final point is made by proposing an approach, which aims at preventive, detective and corrective accountability and data risk management, based on usage control policies and model driven engineering.

Keywords: data security, cloud computing, accountability, business intelligence.

1 Introduction

The growing needs of communication and business collaboration, attributed among others to internationalization and free trade agreements, have generated deep changes in the underlying information and communication technologies, thus causing a rapid development in infrastructure and the emergence of new and novel architectures and programming paradigms. Currently, Cloud Computing and Service Oriented Architectures are frenzy and promising technologies, both implemented in order to leverage organizational business goals, by facing complex and rapid enterprise challenges.

The genesis of cloud computing seems to be a natural evolution of IT technologies regarding organizational needs. Beyond an economic decision, delegating the management of the physical machines and processing of application to a cloud provider allow organizations to concentrate on what really matters: their business goals. Thus, cloud computing allows companies an on-demand access to pool resources through the Internet. Moreover, regarding the cloud computing stack, the layer representing the Business

[1] This work is supported by the Conseil Général des Landes (doctoral fellowship to E.J.) http://www.landes.org/enseignement-superieur

Process as a Service (BPaaS) focuses on the outsource of business process services from the cloud, a new interaction mechanisms that entails complex challenges that compel to "rethink" the information system architecture that supports such a communication form. In this context, Service Oriented Architectures show up for allowing system integration.

Taking into account the enterprise advantages of both SOA and the cloud, particularly BPaaS, in the remaining of the article, we discuss the main issues that have been commonly associated to inter-organizational interaction by means the cloud with respect to information security. We present in Section 3 an overview, in which some works related to inter-organizational workflow, quality of service and accountability are described. Next, in Section 4 we propose some clues to better tackle some existing open issues. Additionally, we also present a proposal that aims trustworthiness in the inter-organizational service interaction by means the cloud. Finally, we conclude in Section 5.

2 Business Process as a Service and the Cloud

In order to successfully accomplish cooperation among enterprises through the cloud, two important issues highlight: standards and interoperability. Thus, interaction, outsourcing, data exchange and collaboration are requirements that are becoming more frequent when performing business activities and as we presented in the previous section, BPaaS and SOA are both technical approaches proposed for getting support to those needs. To clarify both concepts, cloud computing uses the Internet to enable interactions (among others in the form of BPaaS) between the cloud service user and cloud service provider. On the other hand, SOA focuses on enterprise integration technologies to exchange information between systems. Although SOA and cloud computing can exist independently, they can be treated as complementary activities thus leveraging business goals in the form of BPaaS.

Considering their main constituents and characteristics, the following are advantages widely reported in the literature of implementing a service oriented architecture:

- **Reuse**: each service should be implemented and deployed having in mind their reutilization in order to develop business functionalities and expose it as a service only once, to then be used several times by different clients.
- **Loosely-coupled**: this characteristic is twofold: services should be independent and service implementation changes should remain transparent for service users.
- **Integration**: services should be able to cooperate (composed services) in order to build more complex business processes.
- **Simplicity and platform independent**: service oriented technologies should rely on standards in order to guarantee interoperability.

However, despite the optimistic growth and undeniable advantages of both cloud computing and SOA, recent studies have shown a strong fear of companies and a feeling of insecurity when delivering their information to a third party (cloud service provider). In this way, their attracting advantages have been compensated by several issues that have thus restrained the widely adoption of these models, namely:

- Due to the fact that business processes are orchestrated through several domains and/or cloud providers, it is difficult to detect faults and data breaches, and, in turn, it is difficult to establish a chain of accountability.
- The cloud user has no direct control over the process and data.
- Legal aspects and possible conflicts get involved in case of transborder data.
- The lack of standards between service providers can hamper interoperability.
- Cloud user's fear that the data may be manipulated by another cloud user sharing resources from the same provider.

In addition, traditional risks presented in distributed environments also appear: availability, integrity and confidentiality. In general terms, issues related to data privacy, data security and accountability, as evident in the aforementioned pitfalls, need several interrelated study areas in order to create a solid framework. For that purpose, in this article we consider some insights that show the strong relation among information security policies, and their social impacts, the changes in the organizational culture, the legislation and the technical aspects that reflects all those features.

Relating to the legislation, in the interaction between cloud service users and cloud service providers, public legislation is presented as a regulatory framework dealing with national security policies that restrict and regulate data processing. Currently, two major aspects continue to be interesting research topic by the community. The first one is linked to jurisdictional laws applicable in data transfers and accountability about data protection and data lost . Recognizing the importance of protecting personal information along the entire value chain, different countries have implemented policies to ensure and protect business operations as well as gain trust in their information technologies. Within the European Union, Directive 95/46/EC, Directive 2010/87/EC, Sopot Memorandum and the legislation documents issued by Article 29 of the Data Protection Working Party [1,2,3,4,5] have been proposed in order to define the responsibilities of each entity participating in the interaction process. Alternatively, in the US legislation[6], the government plays an important role in data exchange, which grants the right of accessing personal and commercial information. The second aspect, related to legislation is the real implementation of the public politics inside an organization or an information system. The cases of ChoicePoint Inc.[2], Google[3] and SONY BMG[4] are some examples in which heavy fines were got by incorrect use to user's private information, in particular, those practices related to confidentility.

On the other hand, as stated in [7], technology built without taking into consideration a human impact is bound to fail. Decisions made from the whole information gathering from different cloud sources, affect people in a direct or indirect way. Especially, now that the increase of social networks has changed the way in which people expose personal information. Although it is an interesting research line that covers technological strategies as well as preventive, detective and corrective regulations associated to data protection, especially, personal data protection, it is out of the scope of our work because it is not directly related to the technical aspects of the BPaaS model. However, interesting thoughts can be found in [8,9,10].

[2] http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf
[3] http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf
[4] http://www.ftc.gov/os/caselist/0823071/081211cmp0823071.pdf

In the next section, we focus on the technological aspects such as architectures and interaction models proposed in the literature aimed at data risks and trustworthiness.

3 Litterature Review

In this section we present different architectural models and technical solutions reported in the literature to tackle data risks and trustworthiness. Due to the fact that those topics are actively researched and they can be studied in several domains from different perspectives, we narrowed our survey to those covering aspects of BPaaS, namely: interorganizational workflows through orchestration and choreographies, quality of service and accountability.

3.1 Interorganizational Workflows

In [11] an interorganizational workflow is defined as a cooperation of several, autonomous and heterogeneous business processes, in order to achieve a common goal. From a design perspective, workflows represent the coordination of several tasks to accomplish a business process. From an organizational point of view, it is an attracting approach which enables to integrate services exposed in the cloud, to accomplish their own business process, creating temporary Virtual Enterprises (VE)[5] [12]. However, from a technological point of view it is hard to integrate workflows from different organizations since several issues emerge related to security and autonomy of each partner, as well as managing of the VE.

In [13] an architectural model based on a "smart" UDDI (Universal, Description, Discovery and Integration) is proposed to assemble heterogeneous SOA networks. This central entity plays the role of a SOA network manager being able to know everything about each service and the whole process by using information such as transport protocol rules, network routing rules, security information, QoS and SLA rules, and changes in the management status. In that approach, privacy and data integrity is guaranteed by implementing a message interceptor between the service user and the service provider. Several works have been proposed in the same research line, which have some central entity in their architecture. In [12] an interorganizational workflow management agent takes responsibility for the creation and supervision of the workflow, and recovering from exceptions. All those works are interesting approaches that present as main advantage having a general and unified knowledge of the state of the overall system but two major concerns also arise; the first relates on how to keep organizational autonomy of each party, and the second, and possibly more important, there is no agreed knowledge about who is in charge of the management of the central entity.

Van Der Aalst's work about inter-organizational workflows [14] tackles local autonomy of the different parties but allowing high levels of interaction. The basis of his work is to allow individual parties to change their internal workflows without affecting the cross-organizational process behavior. In order to do so, he proposes a three-step

[5] A virtual enterprise is a temporary alliance of enterprises that come together to share skills or core competencies and resources in order to better respond tobusiness opportunities, and whose cooperation is supported by computer networks.

methodology which consists in creating a public workflow (contract) which in a second step is split up among the different domains (business partners) and in a final step all the public parts are replaced for private workflows. Similarly, based on the principle that partners do not want to grant a public view on their internal processes, in [15] an architecture that tackles control flow and data flow for web services orchestration and choreography is proposed. It proposes the implementation of a workflow view in which each partner offers different public views only exposing those elements of their internals that are useful for another entity workflow.

Finally, the standard ISO 27010 [16] is a complete guide that covers methods, policies, processes and controls that have to be considered in inter-organizational data sharing in complex scenarios. It aims to fulfill legal and contractual agreements.

3.2 Quality of Service

In the relation between the cloud service provider and the cloud service user, contracts are the evidence which describe the terms of the interaction. Particularly, private contracts should contain the responsibilities of the entities involved in the process, the public law concerns, but also technical details about data protection, data security, and functional and nonfunctional characteristics of the service. In [17] a methodological approach that defines the Service Level Agreement (SLA) life-cycle is proposed. In that work the five-step SLA life cycle comprises: contract definition, publishing and discovering, negotiation, operationalization, and de-commissioning. In terms of data protection, it is important to highlight that in the decommissioning step, transfer and erasure of the service user's data is an issue that needs to be clarified in the contract. In [18] Quality of Service (QoS) metrics are incorporated into business workflows. In that work, authors analyze both qualitative and quantitative metrics and propose as quality of service metrics: fidelity, reliability, task response time (delay time and process time) and the cost associated to the workflow execution; all represented in a quantifiable form. In [19] another approach based on a contracting workflow for multiple services is proposed. That work focuses in particular on the negotiation process by proposing eight negotiation patterns, which cover from a simple "implicit-accept" interaction to alternating binding counter offer patterns, which, in theory, could include the negotiation of SLA terms. However, the inclusion of QoS in the patterns are left for future work.

Due mainly to an important characteristic of SLO: measurability, most of, or almost all of the SLA only include infrastructure QoS metrics in the agreements, which gather [17]: hardware availability, power availability, data center network availability, backbone network availability, service credit for unavailability, outage notification guarantee, Internet latency guarantee, packet loss guarantee, service level parameter metric, function, measurement directive, SLO and penalties.

On the other hand, in order to facilitate the evaluation of the compliance of SLA by implementing machine-readable contracts, several agreement modeling have been proposed in the literature, i.e., SLANG, WSLA, WSOL and WS-Agreement.

For further information, [20] presents a comprehensive survey about agreements in cross-organizational enterprises considering several evalution criteria: does it covers a multiple architectural layer or a single layer, dependencies techniques, the life cycle it covers and the specification language used.

3.3 Accountability

Beyond legal aspects regarding the compliance and penalties of the contract, accountability aims for the compliance in terms of workflow executions and trustworthiness of the entities which interact in the achievement of a composite business process. Several authors [21,22] agree to define that a system is accountable if faults can be reliably detected and each fault can be undeniably linked to one or more nodes. In this way, an entity is trustworthy if accountability is guaranteed. Also, it can be established that for accomplishing the two named characteristics, every particular action has to be associated to a node in the process. In turn, this implies that accountability involves aspects such as knowing where information crosses, possible data transformation, and the reason and purpose of the processing. For that purpose, techniques as logging, monitoring and auditing have been proposed.

Ringelstein's work [23] tackles monitor agreed-upon policies in distributed workflows by retrieving information about who, why and how the data is processed. The proposal consists of attaching logs, specified by RDF-based semantic formalism, to all data instances in SOAP messages. That kind of metadata includes data type specification for entity identification (who process the data), action activity (how to process the data) and it includes an ontology to define the purpose of the processing (why process the data). In [22] strong accountability is implemented in the design of the TSOA (Trustworthy Service Oriented Architecture) system, which is able to identify misbehavior, the entity responsible for the fault and the evidence of the guilty party. The logging in the cited work is done by modifying the original BPEL document by inserting XML invoke messages before or after the data is transmitted to any entity, in this way, it is possible to trace the data. Additionally, time information is included in order to check QoS compliance. In the architecture of the system, a single accountability service entity contains the BPEL script, SLA and WSDL for accomplishing monitoring and auditing. A different approach in which every node maintains its own log to detect incorrect executions is presented in [21]. In this approach logs contain information about input and output messages by implemented tamper-evident logs, in addition, trusted timestamping are also added, allowing SLA check compliance.

Accountability as seen from a holistic point of view, covering legal, socioeconomic, regulatory and technical aspects is presented in [24]. That European project named A4Cloud aims at four objects which tackles accountability developing tools that:

i enable cloud service providers to give their users appropriate control and transparency over how their data is used,

ii enable cloud end users to make choices about how cloud service provider may be use,

iii monitor and check compliance with user's expectation, business policies and regulations,

iv develop recommendations and guidelines for how to achieve accountability for the use of data by cloud services.

Although, the project is in its early stages and not many publications are reported, it seems to be a promising approach that tackles preventive, detective and corrective control which allow to achieve accountability.

Despite not presenting a technical approach, several authors have also remarked the relevance of trust and auditing data in the cloud [7,25], especially taking into account the natural fluid property of data.

4 Discussion and Open Issues

In light of the above literature review, it is not difficult to see that accountability encompasses the other two aforementioned technical areas. Trust in a partner entity for data transfer as an intermediate step in the building of a composed service in the cloud, does not only attach importance to the technical aspects, it involves to know the use other entities will give to that data, the purposes of the processing, the traceability of the data, and the quality of the result data as well as the overall service. Additionally, all of these issues imply to take into account legislation that governs data transfer, duties of parties involved in the process, business goals and the social impact that creates the making decision process in the case of incorrect results. By performing reverse engineering to the previous section, we get back to the three technical aspects presented in the previous section beginning at accountability and relating it to the other areas, but this time by highlighting some issues that need to be considered to achieve trustworthiness both in the partners and the data.

With regards to trustworthiness (including data and partners), monitoring every step of the process workflow and data workflow is a critical activity. According to the literature review, three major approaches can be identified, monitoring the action of every partner (user-centric), monitoring the process, by for example, monitoring the workflow (process-centric) or monitoring the data flow itself (data-centric). Each of these approaches has its advantages and drawbacks, however the logging seems to be a common denominator. Regardless the approach implemented, several issues need to be considered:

i taking into account that penalties may be imputed to faulty entities, some of them could prefer to hide their misperforming. Thus, checking that reliable information is recorded in the log and insuring that the log is not modified, become a non-trivial issue,

ii keeping privacy in the log is a relevant matter that affects the customers and the entities business logic. This means, that not every single activity has to be record in the log - due to the fact that some relevant business logic could be compromised, which is crucial especially when the log is shared among all the participants,

iii based on a final log feedback, careful attention needs to be paid to penalties especially in critical activities,

iv improved assessment tools need to be implemented to detect, based on the expected results, in which specific node the data was corrupted,

v special security measures need to be implemented for logging by considering for example if the log format is readable for humans or not, and in the case of sharing log security, measures also need to be implemented to the entity that housed it, in order to restrict that unauthorized users access the log. In this latter, access control models offer an important support.

In the second place, as it was shown in some works presented previously, trust in a partner also implies to be sure about its performance in such way that the service level agreement is respected. As stated in [22], spreading business processes among several administrative domains adds complexity to the process of failure detection, due to the fact that each domain may have its own interests and priorities. Four major concerns arise in this point:

i most of the existing works on service agreements focus on infrastructure quality of service and service level agreements, thus leaving aside Business Level Agreements (BLA), Business Service Level Agreements (BSLA) and Underpinning Contract (UC) in the overall process [20]. The inclusion of that kind of approaches along with machine readable techniques could help to agree organizational goals with interorganizational processes.

ii a second aspect that has been already reported in [20] is the lack of a tool to support dependence on service quality objectives, therefore few works consider that a parameter could be expressed in terms of measuring one or more characteristics.

iii as mentioned in the previous paragraph, the implementation of an access model should be included in the SLA and should not be left it aside, and

iv lastly, but probably more important, it is necessary to clearly define what Quality of Service means in light of an interorganizational composed service.

Finally, due to the fact that data trustworthiness involves the overall data flow, the design of the workflow affects the assessment of the accountability process as well as the quality of service. The implications of an architectural decision about implementing a centralized or distributed architecture for governing the workflow are tightly obvious. In a centralized approach, it is possible to have a more complete and uniform view of the system. However, it is also more susceptible to attacks, lack of availability of the central entity, and compromises the internal logic of the different partner entities. On the other hand, the implementation of a distributed architecture could emerge in a weak information about the state of the system and the management of the interaction process becomes more difficult. Additionally, as a result of the penalties imposed by the breach of the contract, the workflow should be able to adapt in order to remove and include partners in the workflow process.

Although a solution which enables to cover all of the previous aspects is an ambitious multidisciplinary approach, we aim to tackle accountability in composed services in the cloud by implementing an usage control approach, which defines conditions, restrictions and obligations that have to be performed by both the cloud provider and the cloud user before, during and after the interaction process. In this context, the support in existing models such as OrBAC [26], which merges both an access control model and an usage control model, will be extremly helpful. In the proposed approach quality of service is defined in terms of security policies that have to be fulfilled in order to guarantee security goals. By using a MDE (Model Driven Engineering) approach three different models will be defined, i.e., an interaction model, a security model and a supervision model. The target pursued by our approach is twofold, it allows to exploit the well-known advantages of MDE approaches mainly automatic operations with models such as transformation, waving and merging, but also auditing the traceability of the

data in order to verify if participants of the process have respected the security policies or determinate if changes could be made in order to accomplish the business goals, if so, metadata will be recorded for proper explanations.

5 Conclusion

In this article a survey of the aspects related to data risk in business processes composed through the cloud was presented. Although in the literature several data risk in the cloud have been identified, such as availability, integrity, confidentiality, transparency, isolation, intervenability, portability, insecure data deletion, insufficient audit trails and accountability, we particularly focus on thrustworthiness, both in partners and data, both gained by an acoutability process. Enhancing the importance of providing more transparency and control to processes mediated by the cloud and taking into account that data is dynamic due to the complex responsibility chains, we thus propose an approach based on preventive, detective and corrective accountability methods. Although this work does not present relevant results, it offers a significant analysis about issues that have to be addressed when considering a solution based on cloud for composed business processes, which we expect could be used as a basis for further discussions.

References

1. European Parliament and the Council of the European Union: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union **L 281** (1995) 0031–0050
2. European Parliament and the Council of the European Union: Directive 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Union **L 318** (2010) 0032–0035
3. European Parliament and the Council of the European Union: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal of the European Union **L 201** (2002) 0037–0047
4. International Working Group on Data Protection in Telecommunications: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - . 51st Meeting, 23-24 April 2012, Sopot (Poland) (2012)
5. Lacey, D.: Inventing the future - the vision of the jericho forum. Inf. Secur. Tech. Rep. **10** (2005) 186–188
6. States, U.: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. U.S. Government Printing Office (2001)
7. Morrow, S.: Data Security in the Cloud. John Wiley & Sons, Inc. (2011)
8. Leimbach, Timo; Friedewald, Michael; Nentwich, Michael; Strauß, Stefan; Weber, Arnd; Koenig, Rene; Hennen, Leonhard ;Skødt, Jakob Nielsen: Cloud computing – european perspectives on impacts and potentials of cloud computing and social network sites (interim report – phase i). Deliverable No.1; im Auftrag von: Science and Technology Options Assessment (STOA), European Parliament (2012)

9. Timmermans, J., Ikonen, V., Stahl, B., Bozdag, E.: The ethics of cloud computing: A conceptual review. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. (2010) 614–620
10. Esteves, R., Rong, C.: Social impact of privacy in cloud computing. In: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. (2010) 593–596
11. Lopes Cardoso, Henrique; Leitão, P., Oliveira, E.: An approach to inter-organizational workflow management in an electronic institution. In: Proceedings of the 11th IFAC Symposium on Information Control Problems in Manufacturing. (2006)
12. Leitão, P., Mendes, J.a.: Agent-based inter-organizational workflow management system. In: Proceedings of the 3rd international conference on Industrial Applications of Holonic and Multi-Agent Systems: Holonic and Multi-Agent Systems for Manufacturing. HoloMAS '07, Berlin, Heidelberg, Springer-Verlag (2007) 71–80
13. Pulier, E., Taylor, H.: Understanding enterprise SOA. Manning Pubs Co Series. Manning (2006)
14. Van Der Aalst, W.M.P.: Inheritance of interorganizational workflows: How to agree to disagree without loosing control? Inf. Technol. and Management **4** (2003) 345–389
15. Eder, J., Kerschbaumer, N., Köpke, J., Pichler, H., Tahamtan, A.: View-based interorganizational workflows. In: Proceedings of the 12th International Conference on Computer Systems and Technologies. CompSysTech '11, New York, NY, USA, ACM (2011) 1–10
16. ISO: ISO/IEC 27010:2012: Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications. Published, International Organization for Standardization (ISO), Geneva, Switzerland (2012)
17. Bose, S., Pasala, A., Ramanujam A, D., Murthy, S., Malaiyandisamy, G. In: SLA Management in Cloud Computing: A Service Provider's Perspective. John Wiley & Sons, Inc. (2011) 413–436
18. Cardoso, J., Sheth, A., Miller, J.: Workflow quality of service (2002)
19. Van Dijk, A.: Contracting workflows and protocol patterns. In: Proceedings of the 2003 international conference on Business process management. BPM'03, Berlin, Heidelberg, Springer-Verlag (2003) 152–167
20. Guidara, I., Chaari, T., Fakhfakh, K., Jmaiel, M.: A comprehensive survey on intra and inter organizational agreements. In: Proceedings of the 2012 IEEE 21st International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. WETICE '12, Washington, DC, USA, IEEE Computer Society (2012) 411–416
21. Haeberlen, A.: A case for the accountable cloud. SIGOPS Oper. Syst. Rev. **44** (2010) 52–57
22. Yao, J., Chen, S., Wang, C., Levy, D., Zic, J.: Accountability as a service for the cloud. In: Services Computing (SCC), 2010 IEEE International Conference on. (2010) 81–88
23. Ringelstein, C., Staab, S.: Logging in distributed workflows. In: PEAS. (2007)
24. Pearson, S., Tountopoulos, V., Catteddu, D., Sudholt, M., Molva, R., Reich, C., Fischer-Hubner, S., Millard, C., Lotz, V., Jaatun, M., Leenes, R., Rong, C., Lopez, J.: Accountability for cloud and other future internet services. In: Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. (2012) 629–632
25. Rochwerger, B., Vázquez, C., Breitgand, D., Hadas, D., Villari, M., Massonet, P., Levy, E., Galis, A., Llorente, I.M., Montero, R.S., Wolfsthal, Y., Nagin, K., Larsson, L., Galán, F. In: An Architecture for Federated Cloud Computing. John Wiley & Sons, Inc. (2011) 391–411
26. Elrakaiby, Y., Cuppens, F., Cuppens-Boulahia, N.: From contextual permission to dynamic pre-obligation: An integrated approach. In: ARES. (2010) 70–78