Sécurité de l'Information dans les Environnements Inter-Organisationnels

Elena Jaramillo (gloriaelena.jaramillorojas@univ-pau.fr)*
Manuel Munier (manuel.munier@univ-pau.fr)*
Philippe Aniorté (philippe.aniorte@univ-pau.fr)*

Résumé :
Actuellement, les dynamiques du commerce mondial imposent aux entreprises de disposer de systèmes d'information qui facilitent l'intégration de services, la communication, et l'accès. Les architectures orientées services et les processus d'entreprise sous forme de services ont été proposés comme solutions technologiques pour répondre à telles exigences, ce qui permet de créer des services composés à travers le cloud. Cependant, malgré les prévisions de croissance positives dans l'utilisation de ces technologies, il y a encore des problèmes de sécurité qui doivent être résolus avant que ces technologies soient largement utilisées. Dans cet article[a], nous proposons un panorama de la gestion des risques (liés à la sécurité des données) et de la gestion des responsabilités. Compte tenu des questions ouvertes identifiées, nous proposons une approche basée sur des mécanismes de contrôle d'usage.

[a] Ce travail est soutenu par le Conseil Général des Landes (bourse de doctorat à E.J)
http://www.landes.org/enseignement-superieur

Mots Clés : sécurité de l'information, gestion des risques, gestion des responsabilités, environnements inter-organisationnels.

1 Introduction

Il est nécessaire aux entreprises de pouvoir adapter rapidement leurs systèmes d'information aux changements permanents imposés pour la dynamique des entreprises. Ces nouveaux besoins ont conduit à l'émergence de nouveaux paradigmes architecturaux. En particulier , les architectures orientées services, mieux connues sous leur sigle anglais SOA[1], ont permis aux organisations de créer des nouveaux moyens de communication, en termes de collaboration à la fois intra et inter-organisationnelle. SOA se réfère à un nouveau paradigme d'intégration des technologies (services) afin d'échanger des informations. Dans la littérature, plusieurs avantages ont été attribués aux SOA en matière de réutilisation, de couplage lâche, de facilité d'intégration et d'indépendance vis-à-vis de la plate-forme utilisée.

Les entreprises ont d'ailleurs bien perçu le potentiel d'intégration des systèmes de communication qu'offre l'informatique en nuage ou *Cloud Computing*. La mise en œuvre de ce nouveau paradigme permet au service informatique de déléguer la gestion de

* LIUPPA, Université de Pau et des Pays de l'Adour, France
[1] SOA: *Service Oriented Architecture*

l'infrastructure et/ou des applications vers un fournisseur de services, lui permettant ainsi de se concentrer sur les objectifs métier de l'entreprise. En plus des avantages d'une architecture orientées services, le cloud permet de réduire les coûts associés à l'infrastructure, d'optimiser les ressources en les augmentant ou en les réduisant en fonction des besoins du consommateur, de fournir un accès plus facile depuis n'importe quel endroit, d'améliorer l'expérience utilisateur, de faciliter les interactions entre les organisations, ou encore de fournir un réseau d'accès ubiquitaire. Dans un tel scénario, il n'est pas surprenant que la firme de recherche Gartner indique qu'en 2012, en ce qui concerne l'utilisation des services offerts par le cloud, 52% des entreprises utilisaient le cloud pour les processus d'entreprise sous forme de services (BPaaS), couche technique de la pile du cloud qui représente la collaboration entre les différents processus métier considérés comme services.

Toutefois, malgré les perspectives optimistes à la fois pour les BPaaS et les SOA, des études récentes révèlent un sentiment de méfiance de certaines entreprises quant à fournir des informations sensibles sur la logique interne de l'organisation à des tiers (fournisseurs de services), de sorte que les avantages attractifs du cloud sont masqués par des questions de sécurité qui ont freiné l'adoption de ce modèle à large échelle, à savoir :

- Du fait que les processus de l'entreprise sont orchestrés par divers fournisseurs de services, il se crée des chaînes complexes de processus qui rendent difficile la détection de défauts ou de violations de données. Par conséquent, il est difficile d'établir une chaîne de responsabilité.
- Le client n'a pas le contrôle direct sur les processus et les données qu'il confie.
- Dans le cas où les données sont hébergées dans un autre pays, il peut y avoir des conflits entre les politiques de sécurité et les réglementations en vigueur.
- Afin d'optimiser ses ressources dans les infrastructures, un fournisseur de services peut partager ses ressources physiques entre plusieurs domaines (chacun représentant différentes organisations), ce qui peut faire craindre à certains clients que leurs données puissent être manipulées ou accédées par un autre client de ce fournisseur.

Comme nous pouvons le constater, la sécurité et la confidentialité des données, de même que la notion de responsabilité, deviennent des facteurs clés dans l'interaction entre les différentes organisations via le cloud. Si dans ce document nous nous concentrons sur les aspects techniques, nous sommes conscients qu'aborder les facteurs précédemment cités nécessite une approche multidisciplinaire où les techniques et méthodes utilisées intègrent les aspects juridiques qui régissent l'interaction entre les différents acteurs ainsi que les changements sociaux et organisationnels qu'ils génèrent. Sans ignorer que de nombreux efforts ont été faits pour aborder ces sujets individuellement, il y a encore des questions à résoudre. En ce qui concerne les aspects juridiques, il est nécessaire de considérer à la fois les lois qui s'appliquent au transfert des données en dehors du pays d'origine [Eur10, Sta01] ainsi que leur application effective à l'intérieur d'une organisation ou dans un système d'information. D'autre part, nous devons aussi considérer que manipuler et exposer des informations privées dans le cloud peut avoir un impact sur les vies personnelles des utilisateurs d'un système, ce qui nécessite, d'un point de vue de l'entreprise, la mise en œuvre de politiques de sécurité dans l'organisation et la formation des employés de sorte que cette mise en œuvre soit efficace. Il ne s'agit là que de quelques idées de la façon

dont les aspects juridiques, sociaux et organisationnels sont liés à la mise en œuvre d'une politique de gestion des risques.

Dans la suite de l'article, nous présentons les principaux paradigmes actuels qui ont été proposés dans la littérature pour aborder ces questions d'un point de vue technique et architectural. Dans la section 2, nous passons en revue certains paradigmes actuels qui portent sur la sécurité, la confidentialité des données et la gestion des responsabilités, en particulier dans les scénarios inter-organisationnels. La section 3 présente les principaux aspects qui sont encore du domaine de la recherche pour la communauté scientifique et les entreprises. À la fin de cette section, nous présentons aussi une proposition qui vise à compléter les approches existantes en offrant des solutions à certains des problèmes identifiés. Enfin, nous concluons dans la section 4.

2 État de l'Art

L'interaction entre de multiples organisations au travers du cloud est étudiée activement tant par la communauté scientifique que par les entreprises. Cette question a donc été abordée par de nombreuses approches, chacune apportant des éléments d'amélioration à ce paradigme. Y figurent les aspects sécurité issus de la vision traditionnelle de la confidentialité, l'intégrité et la disponibilité, la sécurité au niveau des nouveaux risques introduits par les protocoles de communication dans les architectures orientées services, la formalisation de modèles de communication pour améliorer la collaboration entre plusieurs organisations... Dans cet article, la taxonomie proposée regroupe la revue de la littérature en trois catégories, à savoir : les workflows inter-organisationnels au travers de l'orchestration et de la chorégraphie, la qualité du service et la confiance via la gestion des responsabilités.

2.1 Workflows Inter-Organisationnels

Les workflows inter-organisationnels ont été définis dans [LCO06] comme la coopération entre différents processus autonomes et hétérogènes afin d'accomplir un objectif commun. Dans la littérature, deux architectures principales ont été proposées pour représenter l'interaction entre plusieurs entités (organisations): des architectures distribuées et des architectures centralisées. La première catégorie correspond à un processus de chorégraphie dans lequel chaque entité est responsable de sa performance et chacune connaît ses relations et ses dépendances avec les autres entités. D'autre part, dans une approche centralisée, une entité nommée orchestrateur est chargée de coordonner les activités entre tous les participants du workflow. Du point de vue de la modélisation, WS-CDL a été proposé comme un langage standard pour représenter un workflow basé sur la chorégraphie. Ce langage n'est cependant pas exécutable. Par contre, le standard BPEL utilise un moteur d'orchestration pour exécuter la coordination entre les différentes entités. Étant donné qu'ils sont tous les deux des standards bien connus pour la communauté, plusieurs approches, basées principalement sur la transformation de BPEL, ont été proposées pour combler le fossé entre le modèle abstrait et sa mise en œuvre [MH05].

Du point de vue de la logique de l'entreprise, utiliser des services publiés dans le cloud est une alternative attirante pour réduire les coûts et se concentrer sur les objectifs de l'entreprise; cependant, du point de vue technique, il s'agit d'un grand défi, car il implique la création temporaire d'entreprises virtuelles [LaM07] pour permettre une coopération efficace mais sans compromettre la sécurité et l'indépendance de chaque entité. Par con-

séquent, plusieurs questions doivent être considérées, à savoir: Comment atteindre une coopération efficace sans compromettre l'autonomie de chaque organisation ? La sécurité de chaque organisation est-elle compromise ? Qui est chargé de réglementer le bon fonctionnement de l'organisation virtuelle ?

Dans [PT06], un modèle d'architecture basé sur une entité central nommée «smart UDDI[2]» est proposé pour assembler et gèrer un réseau hétérogène de SOAs. Dans la proposition citée, l'intégrité et la confidentialité des données est garantie par la mise en œuvre d'une entité qui intercepte les messages entre le consommateur et le fournisseur. Dans cette même ligne de recherche, plusieurs travaux ont été rapportés dans la littérature qui proposent dans leur configuration une architecture basée sur une entité centrale. Dans [LaM07], la gestion et la supervision du workflow inter-organisationnel est réalisée par un agent intelligent avec la capacité de récupérer des exceptions survenues au cours de l'exécution en adaptant le réseau de Pétri qui définit le workflow.

Tous les travaux de cette catégorie ont l'avantage principal d'avoir une vision globale du processus et une compréhension unifiée de l'état du système. Cependant, cette approche pose certaines questions qu'il faut analyser et résoudre tant par rapport à la préservation de l'autonomie de chaque entité qu'à la gestion cette l'entité centrale. À cet égard, le travail de Van Der Aalst sur les workflows organisationnels [VDA03] traite de l'autonomie locale des différentes entités impliquées dans le processus de l'organisation virtuelle. La base de son travail est de permettre à chaque organisation de modifier ses processus internes sans affecter le fonctionnement du processus inter-organisationnel. De même, en partant du principe que les organisations ne veulent pas offrir une vue publique de leurs processus internes pour construire un workflow inter-organisationnel, il est proposé dans [EKK+11] la mise en place de vues (*views*) selon lesquelles chaque entité de l'organisation virtuelle fournit une vue publique qui ne contient que ses processus susceptibles d'être utilisés dans le workflow d'une autre organisation.

2.2 Qualité du Service

Comme preuve de la relation établie entre un consommateur et un fournisseur, différentes formes de contrat privé peuvent être utilisées : licences, accords de service, contrats en ligne (principalement représentés par les contrats connus comme *«click-and-accept»*). Cependant, les travaux qui seront présentés ci-dessous abordent des contrats qui permettent une négociation ou un accord sur les termes du contrat, car cela impose des restrictions supplémentaires à l'interaction, ce qui nécessite un rôle actif des deux parties.

Par rapport à leur modélisation, il est proposé dans [VDA03] une formalisation basée sur la phase de négociation compte tenu de la relation contractuelle entre de multiples services au travers de multiples participants. De même, dans [BPRA+11] il est proposé une approche méthodologique pour définir le cycle de vie des accords au niveau du service (SLA[3]). Dans ce travail, le cycle de vie comprend cinq étapes: la définition du contrat, la publication et la découverte, la négociation, l'opérationnalisation et l'échéance du contrat. En ce qui concerne la sécurité et la confidentialité des données, il faut établir dans la phase d'échéance du contrat des politiques claires concernant à l'élimination sûre des données et/ou leur transfert au contrôleur.

---

2 UDDI: *Universal, Description, Discovery and Integration*

3 SLA: *Service Level Agreement*

D'autres travaux, tel que celui présenté dans [CSM02], intègrent les exigences de Qualité de Service (QoS) dans le workflow. Dans cet article, les auteurs ont analysé les aspects quantitatifs et qualitatifs de la qualité du service, en proposant des mesures de qualité telles que la fidélité, la fiabilité, le temps de réponse (temps de retard et temps de traitement) et le coût associé à l'exécution workflow, tous représentés quantitativement.

Un élément important des Objectifs de Niveau de Service (SLO[4]) est la mesurabilité. De ce fait, toutes les études que nous avons passées en revue au moment de la rédaction du présent article ne considèrent que la qualité de service associée à l'infrastructure. Citons par exemple [BPRA+11] : la disponibilité du matériel informatique, la disponibilité de l'alimentation, la disponibilité du réseau interne au datacenter, la disponibilité des connexions réseau, le crédit de service en cas d'indisponibilité, la garantie de notification de panne, la garantie de latence d'Internet, la garantie de perte de paquets, les métriques quant aux paramètres de niveau de service, le fonctionnement, la supervision, les SLO et les pénalités.

À noter que pour faciliter l'évaluation de l'accomplissement des SLA au travers de contrats lisibles par la machine, plusieurs langages de spécification ont été proposés dans la littérature. Parmi ceux-ci on trouve SLANG, WSLA, WSOL et WS-Agreement. Certains auteurs s'accordent à dire que ce dernier est aujourd'hui le plus utilisé.

Pour plus d'informations, nous recommandons au lecteur de se référer à [GCFJ12] qui présente une étude détaillée sur les contrats dans des environnements inter-organisationnels en considérant plusieurs critères d'évaluation : le nombre de couches de l'architectures qu'ils comprennent, leur dépendances techniques, les étapes du cycle de vie qu'ils prennent en compte, ainsi que le langage de spécification utilisé.

2.3 Gestion des Responsabilités

Dans ce document, nous utilisons le terme gestion des responsabilités dans le même sens que le terme anglais *«accountability»*. En ce sens, la gestion des responsabilités concerne la mise en œuvre des obligations entre le fournisseur et le consommateur, au-delà des relations contractuelles, mais en se concentrant sur les aspects de la responsabilité et de l'exécution du workflow. Dans la littérature, plusieurs auteurs [Hae10, YCW+10] s'accordent pour définir qu'un système met en œuvre la gestion des responsabilités si les défauts peuvent être détectés de manière précise et peuvent être associés à un ou plusieurs nœuds dans le workflow. Pour répondre à ces caractéristiques, chaque action du workflow doit être associée à un nœud, ce qui nécessite de connaître les points par lesquels passe l'information, la possible transformation des données ainsi que la raison et le but du traitement. Ainsi, une entité est considérée comme fiable s'il est possible d'assurer la gestion des responsabilités. Pour assurer la fiabilité des entités impliquées dans le processus inter-organisationnel, plusieurs techniques telles que les journaux d'événements, le suivi et l'audit ont été proposées.

Le travail de Rengelstein [RS07] traite du suivi des politiques concertées dans les workflows distribués, en recueillant des informations au sujet de qui, pourquoi et comment les données sont traitées. La base de son travail est d'ajouter des logs à toutes les instances de données qui sont traitées et transmises dans les messages SOAP. Dans [YCW+10] il est proposé le terme de gestion forte de la responsabilité comme un élément important de

[4] SLO: *Service Level Objectives*

la conception du système TSOA[5]. Dans cette proposition, il est possible d'identifier une mauvaise exécution, l'entité qui en est responsable ainsi que des preuves de la défaillance. La conception de TSOA considère la gestion des responsabilités comme un service qui est inclus dans l'architecture et la mise en œuvre du système. Dans ce travail, le log est réalisé en modifiant le document BPEL représentant l'orchestration entre les différentes entités, de manière à insérer des étiquettes XML qui font appel au service de gestion des responsabilités avant et/ou après la transmission des données à une entité du processus. Ainsi, l'entité responsable du service de la gestion des responsabilités enregistre des informations sur le script BPEL, le SLA et le WSDL pour effectuer les activités d'audit et de suivi dans le système. À l'inverse, [Hae10] propose une approche où le log n'est pas centralisé sur une seule entité, mais réparti entre les différents participants, où chaque nœud du processus enregistre des informations sur les messages d'entrée et de sortie.

Finalement, un point de vue similaire à celui présenté ici est proposé dans [PTC+12] où la gestion des responsabilités est traitée à partir d'une approche juridique, socio-économique, réglementaire et technique. Ce travail fait référence au projet européen A4Cloud dont le principal objectif est le développement d'outils pour i) permettre aux consommateurs de services un meilleur contrôle et une plus grande transparence par rapport à la gestion des données par les fournisseurs, ii) faciliter au contrôleur le choix d'un prestataire de services, iii) surveiller et vérifier l'accomplissement des attentes des consommateurs ainsi que des politiques de l'entreprise et des règlements, iv) formuler des recommandations et des lignes directrices sur la gestion des responsabilités quant à l'utilisation des données dans le cloud. Bien que le projet soit à ses débuts et que peu de publications aient été rapportées, ce projet semble très prometteur car il aborde la gestion des responsabilités avec une approche de prévention, de détection et de correction.

3 Discussion et Proposition

Considérant les travaux présentés dans la section précédente, il faut établir que les questions juridiques, sociales et organisationnelles doivent être analysées et conceptualisées dans une approche technologique qui permettrait d'assurer la confiance dans les entités participant aux processus inter-organisationnels, en particulier au travers de la gestion des responsabilités. Cependant, il faut également connaître l'utilisation qui sera faite des données à l'intérieur et à l'extérieur du workflow, la finalité du traitement, leur traçabilité et la qualité des résultats, ainsi que le processus de traitement lui-même. Cette section a pour but de lister les aspects technologiques présentés précédemment en soulignant certains éléments qui restent encore des questions ouvertes.

En ce qui concerne la confiance (dans les entités et dans les données), le suivi de chaque processus et des données au travers du workflow est une activité essentielle. Selon les travaux publiés dans la littérature, il est possible d'identifier trois approches principales: suivre les actions individuelles de chaque entité (approche centrée sur les entités), suivre les processus, par exemple en suivant le workflow (approche centrée sur les processus), ou suivre le flux de données (approche centrée sur les données). Chacune présente des avantages et des inconvénients, soit dans sa mise en œuvre soit en termes de gestion des risques sur les données. Cependant, quelle que soit l'approche adoptée, le log, vu comme

[5] TSOA: *Trustworthy Service Oriented Architecture*

une preuve de l'interaction entre les multiples entités impliquées dans le processus, semble être un dénominateur commun pour lequel plusieurs analyses doivent être effectuées:

i Considérant qu'il y a des sanctions envers les entités qui, en quelque sorte, ne respectent pas les termes du contrat, certaines entités pourraient être tentées de masquer un mauvais fonctionnement; il faut donc s'assurer que l'information enregistrée dans le log est fiable et qu'elle ne peut pas être modifiée.

ii Restreindre l'accès au log aux seules entités autorisées implique la mise en œuvre de politiques de confidentialité. D'abord, toutes les activités individuelles ne nécessitent pas forcément d'être enregistrées dans le log, ceci afin de ne pas compromettre la logique interne des organisations impliquées dans la création d'un service composé. Ensuite, il faut avoir des politiques de sécurité particulières pour le log et pour l'entité qui l'héberge. Des aspects tels que le stockage du log (chiffré ou en clair) doivent être pris en considération. En ce sens, les modèles de contrôle d'accès existants offrent une excellente alternative.

iii À l'échéance du contrat (et du workflow) une rétroaction et une analyse rigoureuse devraient être effectuées pour déterminer d'éventuelles sanctions envers des entités, en particulier pour celles responsables des activités critiques des processus de l'entreprise.

iv Finalement, un travail conséquent est nécessaire en termes d'outils d'évaluation pour déterminer, en fonction de la réponse attendue, dans quel nœud en particulier les données ont été corrompues.

En plus de la notion de preuve (via le log), un deuxième élément à analyser concerne l'accomplissement des niveaux de service. Comme cela est indiqué dans [YCW+10], disperser les processus de l'entreprise entre plusieurs domaines administratifs ajoute une complexité significative à la détection de défauts car chacun d'eux a ses propres intérêts et priorités. Par rapport aux niveaux de service dans l'interaction entre les différentes organisations, il faut considérer que :

i Comme il a été mentionné précédemment, la plupart des travaux publiés jusqu'à présent en termes de qualité de service se concentrent sur les aspects de l'infrastructure, en laissant de côté les accords au niveau de l'entreprise (BLA), les accords au niveau des services de l'entreprise (BSLA) et les contrats de sous-traitance (UC[6]) [GCFJ12]. Ces approches et ces techniques pour formaliser ces contrats dans un langage compréhensible par la machine pourraient aider à concilier les objectifs des entreprises en termes de processus inter-organisationnels.

ii Comme affirmé dans [GCFJ12], beaucoup d'efforts sont encore nécessaires pour créer des outils qui puissent supporter l'interdépendance entre les différents objectifs de qualité, ce qui permettrait d'ailleurs de mieux spécifier ces objectifs.

iii Les modèles de contrôle d'accès mentionnés dans le paragraphe précédent devraient être étendus pour intégrer les SLA.

iv En dernier lieu, mais néanmoins important, il faut définir ce que signifie réellement la *Qualité de Service* dans le cadre d'un service composé inter-organisationnel.

6 UC: *Underpinning Contract*

Puisque avoir confiance sur des données après qu'elles aient été traitées par différents tiers implique le workflow global, les processus et les flux de données, la conception de ce workflow conditionne l'évaluation de la gestion des responsabilités et de la qualité du service. Les implications d'une décision, au niveau de la conception, de mettre en œuvre une architecture centralisée ou distribuée pour piloter le workflow sont bien connues. D'une part, dans une approche centralisée, il est possible d'avoir une vision plus complète et cohérente de l'état du système. Cependant, il est aussi plus sensible aux attaques ou aux défauts de disponibilité de l'entité centrale, et donc poser des problèmes de sécurité et de confidentialité tant pour les entités qui participent à l'organisation virtuelle que pour les données. D'un autre côté, la mise en œuvre d'une architecture distribuée peut aboutir à des incohérences quant à l'état du système, et la gestion des responsabilités peut être chaotique. De plus, en cas de sanctions prises à la suite d'un manquement au contrat, le workflow doit pouvoir s'adapter pour éliminer ou intégrer de nouvelles entités partenaires au sein de l'organisation virtuelle. C'est un aspect de la conception qui doit être soigneusement réfléchi.

Nous proposons de développer une approche qui tienne compte de certains éléments d'améliorations présentés dans cette section comme des questions ouvertes. Bien évidemment, une solution qui répondrait et résoudrait tous les risques et violations à la gestion des responsabilités ainsi que les problèmes de confidentialité et de sécurité des données serait une approche multidisciplinaire ambitieuse et complexe. Nous concentrons donc nos travaux sur la gestion des responsabilités et sur la gestion des risques (sécurité de l'information) en suivant une approche orientée contrôle d'usage. Celle-ci propose la définition de conditions, de restrictions et d'obligations qui doivent être exécutées par le fournisseur de services et le consommateur avant, pendant et après le processus d'interaction. Dans ce contexte, le soutien de modèles existants comme OrBAC [ECCB10] est extrêmement utile. L'usage d'OrBAC dans des environnements inter-organisationnels n'est pas nouveau. Dans [ACBC09] les auteurs proposent de mettre en œuvre ce modèle tant dans des architectures distribuées que centralisées pour définir des politiques de contrôle d'accès et de contrôle de flux en appliquant des restrictions statiques et dynamiques. Cependant, à notre connaissance, peu de travaux utilisent ce modèle de contrôle d'usage dans de tels environnements avec comme objectif d'assurer la gestion des responsabilités et la gestion des risques. Dans nos travaux, la qualité du service sera définie en termes de politiques de sécurité qui doivent être respectées pour atteindre les objectifs de sécurité de l'organisation virtuelle.

En plus du modèle de contrôle d'usage, nous suivons une approche d'Ingénierie Dirigée par les Modèles (IDM) pour définir trois types de modèles, à savoir: un modèle d'interaction, un modèle de sécurité et un modèle de supervision. Compte tenu de la base de travail décrite ci-dessus, deux avantages peuvent être soulignés. Le premier, associé à la traçabilité des données, est la vérification de l'accomplissement des règles de sécurité par les participants du processus. Ceci en considérant qu'il est possible de faire des changements dans le workflow pour accomplir les processus d'entreprise, auquel cas des preuves, sous la forme de métadonnées, seront enregistrés pour expliquer ces changements. Le deuxième est lié à l'utilisation de l'IDM avec pour avantage bien connu de pouvoir réaliser des traitements automatiques sur les différents modèles.

4 Conclusion

Dans cet article, nous avons présenté une vue d'ensemble des questions liées à la gestion des risques dans des environnements inter-organisationnels, à savoir, la confidentialité et la sécurité des données, ceci dans le cadre de services composés à travers le cloud. De même, compte tenu de la nécessité de fournir des outils et des techniques qui permettent un plus haut niveau de transparence et de responsabilité dans le processus, la dernière section a présenté une approche basée sur le contrôle de l'usage pour accomplir la gestion de responsabilité, la prévention, la détection, la correction et l'évolution du workflow tout au long de son cycle de vie. Bien que cet article ne présente pas, à proprement parler, de nouveaux résultats dans le domaine de la gestion des responsabilités et de la gestion des risques, nous avons présenté une analyse intéressante concernant les processus d'entreprise sous forme de services impliquant diverses entités qui, nous l'espérons, pourra être utilisé comme une base pour de futures discussions.

References

[ACBC09] Samiha Ayed, Nora Cuppens-Boulahia, and Frédéric Cuppens. Secure workflow deployment in multi-organizational environments. In ., page ., Luchon, France, 2009. Publibook. 8813 8813.

[BPRA+11] Sumit Bose, Anjaneyulu Pasala, Dheepak Ramanujam A, Sridhar Murthy, and Ganesan Malaiyandisamy. *SLA Management in Cloud Computing: A Service Provider's Perspective*, pages 413–436. John Wiley & Sons, Inc., 2011.

[CSM02] Jorge Cardoso, Amit Sheth, and John Miller. Workflow quality of service, 2002.

[ECCB10] Yehia Elrakaiby, Frédéric Cuppens, and Nora Cuppens-Boulahia. From contextual permission to dynamic pre-obligation: An integrated approach. In *ARES*, pages 70–78, 2010.

[EKK+11] Johann Eder, Nico Kerschbaumer, Julius Köpke, Horst Pichler, and Amirreza Tahamtan. View-based interorganizational workflows. In *Proceedings of the 12th International Conference on Computer Systems and Technologies*, CompSysTech '11, pages 1–10, New York, NY, USA, 2011. ACM.

[Eur10] 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 318:0032–0035, 2010.

[GCFJ12] Ikbel Guidara, Tarak Chaari, Kaouthar Fakhfakh, and Mohamed Jmaiel. 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, pages 411–416, Washington, DC, USA, 2012. IEEE Computer Society.

[Hae10] Andreas Haeberlen. A case for the accountable cloud. *SIGOPS Oper. Syst. Rev.*, 44(2):52–57, April 2010.

[LaM07] Paulo Leitão and João Mendes. 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, pages 71–80, Berlin, Heidelberg, 2007. Springer-Verlag.

[LCO06] Paulo Lopes Cardoso, Henrique; Leitão and Eugenio Oliveira. 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.

[MH05] Jan Mendling and Michael Hafner. From inter-organizational workflows to process execution: Generating bpel from ws-cdl. In Robert Meersman, Zahir Tari, and Pilar Herrero, editors, *On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops*, volume 3762 of *Lecture Notes in Computer Science*, pages 506–515. Springer Berlin Heidelberg, 2005.

[PT06] E. Pulier and H. Taylor. *Understanding enterprise SOA*. Manning Pubs Co Series. Manning, 2006.

[PTC+12] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M.G. Jaatun, R. Leenes, Chunming Rong, and J. Lopez. Accountability for cloud and other future internet services. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 629–632, 2012.

[RS07] Christoph Ringelstein and Steffen Staab. Logging in distributed workflows. In *PEAS*, 2007.

[Sta01] United States. *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.

[VDA03] W. M. P. Van Der Aalst. Inheritance of interorganizational workflows: How to agree to disagree without loosing control? *Inf. Technol. and Management*, 4(4):345–389, October 2003.

[YCW+10] Jinhui Yao, Shiping Chen, Chen Wang, D. Levy, and J. Zic. Accountability as a service for the cloud. In *Services Computing (SCC), 2010 IEEE International Conference on*, pages 81–88, 2010.