Proposition de recherche doctorale

La sécurité dans le cloud computing

Mots clés :

- **Directeur de thèse** : salima BENBERNOU
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'Informatique PAris DEscartes
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

Le Cloud Computing est entrain de révolutionner le monde informatique. Il consiste en l'externalisation des infrastructures informatiques vers des prestataires spécialisés. Les utilisateurs du Cloud Computing gagnent en autonomie, en ergonomie et en simplicité. Aussi, la composition d'applications sur le "cloud" ouvrira des possibilités de travail collaboratif encore imprévisible. Les offres SaaS, pour Software as a Service, en Cloud Computing permettent un paiement selon l'utilisation du service offert [1], d'ou la réduction de la consommation d'énergie vue la mutualisation des ressources entre plusieurs entreprises. Très important pour la sauvegarde de notre planète, en connaissant les efforts consentis dans ce sens et les contraintes environnementales actuelles. L'une des principales caractéristiques du cloud computing est la Multi-tenancy [6], soit le fait que plusieurs tenants/utilisateurs exécutent simultanément la même instance d'une application ou processus métier déployé sur un serveur distant ou datacenter. La Multi-tenancy permet une réutilisation de fragments de processus métiers par les différents tenants. Cette réutilisation contribuera à optimiser le temps de service. Néanmoins, les entreprises acceptent d'externaliser seulement leurs applications non stratégiques par peur sur la sécurité et la vie privée de leurs données. Le but de la thèse est la proposition de framework pour la préservation des données sensibles lors de l'externalisation des données pour un SssS.

Résumé du projet de recherche (Langue 2)

D’un coté, des travaux [2,3] ont été menés dans le cadre des Mashup de bases de données. Et des algorithmes d’anonymisations [4,5] ont été proposés. En effet, si une entité ne sait pas à qui elle a affaire, elle ne pourra pas obtenir d'informations personnelles sur son interlocuteur. Il existe pourtant d'autres façons de protéger la vie privée des utilisateurs et l'une des composantes possible est le chiffrement. En effet, si l'entité ne sait pas quelle donnée est manipulée, alors elle n'obtiendra pas d'informations personnelles sur son interlocuteur (même si, cette fois-ci, elle sait qui il est). D’un autre coté, des travaux sont menés actuellement au sein du LIPADE ayant pour objectif la définition de méthodes formelles pour la fragmentation d’un processus métier dans le but de permettre la réutilisation de ces fragments dans une plateforme SaaS. Le fait de réutiliser des fragments déjà calculés par d'autres tenants peut amener des processus métiers malicieux déployés par des tenants malveillants, de vouloir récupérer des données sensibles seulement en réutilisant ces fragments. Nous souhaitons proposer des méthodes formelles d’anonymisation des fragments de processus métiers afin de protéger la vie privée des tenants lors des réutilisations de fragments, puis implémenter ces méthodes et les tester sur des plateformes SaaS opérationnelles. 1. Tim Kraska, Martin Hentschel, Gustavo Alonso, and Donald Kossman. Consistency Rationing in the cloud: pay only when it matters. In VLDB09, pages 253_264, 2009 2. Noman Mohammed, Benjamin C. M. Fung, Ke Wang, and Patrick C. K. Hung. Privacy- preserving data mashup. In EDBT, pages 228_239, 2009. 3. Thomas Trojer, Benjamin C. M. Fung, and Patrick C. K. Hung. Service-oriented architecture for privacy-preserving data mashup. In ICWS, pages 767_774, 2009. 4. Latanya Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5):571_588, 2002. 5. Latanya Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5):557_570, 2002. 6. Cor-Paul Bezemer and Andy Zaidman. Challenges of reengineering into multi-tenant saas applications. Technical report, Delft University of Technology, 2010.

Informations complémentaires (Langue 1)

Le sujet proposé a une grande portée Européenne et internationale, étant donné la préoccupation internationale quand aux données sensibles manipulées lors l'utilisation d'un Sass à la demande.

Informations complémentaires (Langue 2)

Financement sous forme d’une Convention CIFRE avec une PME Francilienne. Cette collaboration permettra l’implémentation des solutions proposées et leurs tests sur des plateformes SaaS pour évaluer leurs efficacités