Proposition de recherche doctorale

Sécurité des services de Stockage de Données dans le Cloud Computing

Mots clés :

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

Résumé du projet de recherche (Langue 1)

Grâce aux économies de gestion et de maintenance qu'il offre, le « cloud computing » connaît un essor important dans le déploiement des services informatiques. D'après le principe d'infogérance étendue qui est à la base du cloud computing, la plupart des traitements informatiques sont mis en œuvre par des tierces parties en utilisant des équipements situés à distance tout en assurant une qualité de service et un temps de réponse comparables à ceux obtenus sur des équipements locaux. Le service de stockage de données ou Storage as a Service (StaaS) fait partie des services les plus populaires du cloud computing et permet de stocker d'une façon fiable des volumes importants de données. En contrepartie des avantages en terme de coût et de facilité de gestion, le StaaS pose de nouveaux problèmes liés à la sécurité des données et des traitements effectués sur ces données pendant le stockage en raison du stockage des données à distance et au-delà des périmètres des usagers et de l'implication d'une ou plusieurs tierces parties comme fournisseurs de service ou d'infrastructure. Les exigences de sécurité concernant le service de stockage varient de la confidentialité des données et de leur intégrité à des garanties sur leur disponibilité. Les mécanismes classiques de sécurité comme le chiffrement et les méthodes d'intégrité ne répondent que partiellement à ces exigences d'une part à cause des nouvelles vulnérabilités dues au traitement à distance et aux intrusions possibles par le canal de transmission et en raison de la malveillance potentielle d'une des entités assurant le service d'autre part. La mise en œuvre des solutions classiques devient encore plus difficile quand on tient compte des exigences spécifiques du cloud computing qui sont liées à la qualité de service et au temps de réponse en présence de très gros volume de données. Des techniques d'optimisation propres au cloud computing comme la parallélisation massive par des algorithmes distribués ou la dé-duplication pour réduire la redondance sont des exemples de méthodes spécifiques qui sont incompatibles avec les solutions classiques de sécurité. Des offres commerciales comme le chiffrement des données dans Amazon S3 commencent à apparaître en réponse aux besoins de sécurité dans le StaaS mais elles reposent pour le moment sur le principe d'un fournisseur de service fiable et non malveillant. Des problèmes spécifiques au StaaS comme les attaques provenenant de la multiplicité des fournisseurs ou les difficultés liées à la dé-duplication (http://usenix.org/events/sec11/tech/slides/mulazzani.pdf) sont de plus en plus abordés dans les milieux de la recherche et des approches nouvelles pour répondre aux besoins de sécurité spécifiques au StaaS comme des techniques de chiffrement homomorphes proposées par le startup Porticor (www.porticor.com) ou la méthode de confidentialité de données sans chiffrement proposée par Cleversafe (www.cleversafe.com) montrent l'intérêt porté aux problèmes de sécurité dans le StaaS et à leur solution. Le but de cette thèse est de concevoir de nouveaux mécanismes de sécurité qui sont compatibles avec les exigences de StaaS. Ces mécanismes devront prendre en compte l'aspect massivement distribué des unités de stockage sans dégrader la qualité du service et le temps de réponse. Pour une partie des scénarios, le fournisseurs de service sera considéré potentiellement malveillant et dans ces cas, les mécanismes de sécurité correspondant devront permettre à l'usager du service de vérifier la cohérence des opérations effectuées par le fournisseur et la confidentialité des données vis-à-vis du fournisseur. Les nouveaux mécanismes de sécurité pour le StaaS seront développés en utilisant une combinaison d'algorithmes massivement parallèles et des systèmes cryptographiques. La prise en compte du fournisseur potentiellement malveillant nécessitera l'intégration des techniques homomorphes afin de permettre l'exécution d'opération sur des données chiffrées. Le plan prévisionnel du travail comprend les étapes suivantes : -Analyse des besoins de sécurité dans les services StaaS existants -Etat de l'art sur la recherche en cours dans le domaine de la sécurité du cloud computing, tout particulièrement en ce qui concerne le chiffrement homomorphe, le chiffrement à base d'identité, private information retrieval et la garantie de récupération (proof of retrievability) -Définition de modèles d'attaques pour le StaaS -Conception de mécanismes répondant aux besoins, preuves de leur sécurité dans les modèles d'attaques et étude de leur performance -Prototypage des mécanismes dans le cadre d'un système de StaaS.