Proposition de recherche doctorale

Policy Definition and Enforcement for Accountable Services in Cloud Computing

Mots clés :

- Directeur de thèse : yves ROUDIER
- 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)

The research performed by Alexandr Garaga will contribute to the definition of an interoperable policy language for handling and managing accountability concerns. This language should enable the expression of service contracts, security objectives, and regulatory requirements of cloud infrastructures and map these descriptions to the mechanisms implemented. Secondly, the student will investigate policy enforcement mechanisms, possibly involving distributed aspect-oriented design and programming frameworks [15, 16] in order to trace chains of accountability and to provide feedback if they are violated. More specifically, the student will focus on the following objectives: * Establish suitable machine-readable policy representations and techniques for mapping policies at different abstraction levels (application, platform, infrastructure). * Devise policy enforcement mechanisms and conformance testing approaches for ensuring that those policies are effectively applied in the cloud stack. * Document recommended practices to ensure an optimal enforcement and accountability of security policies. * Develop mechanisms for enforcing data protection in order to ensure the compliance of the cloud computing service. * Provide reliable accountability mechanisms, resistant to tampering and other kinds of attacks. * Provide tools to help cloud providers to enforce privacy preferences when handling private data. * Integrate tools and services to facilitate the execution of obligations, incident handling, and the generation of evidence at different levels in the cloud. The research work will follow an agile approach to acquisition of requirements for enforceable policies in conjunction with the work packages of the A4Cloud project. Mr. Garaga will first define ways of representing accountability policies, drawing on existing practices and languages as much as possible, and then develop the capability of enforcing those policies across the cloud eco-system. He will establish the extent to which policy enforcement is achievable using combinations of automated tools in conjunction with regulatory/contractual mechanisms in order to obtain a level of assurance in the use cases as required by the risk assessment process. Automation requires a machine-readable, and machine-understandable, representation of policies for accountability such as a declarative language. The research work performed with the student will embrace existing standards, languages and methodologies as much possible. One of the challenges to be addressed is the heterogeneous nature of the cloud environment with policies relating to the infrastructure, the platform, and software applications. Furthermore, those policies might also be addressing legal, financial, business, or performance issues. Finally, they might emanate from regulatory, organizational, or personal decisions. It is consequently important to define which limitations apply to policy enforceability and auditability in such diverse situations. On the policy enforcement side, investigations will aim at identifying or defining appropriate methodologies and then identifying the tools and interfaces needed for implementing them. In order to improve the acceptance of the new accountability language, it will likely be necessary to provide compatibility with existing frameworks for access control, usage control, and private data handling. Tools and services to support the policy enforcement methodologies identified previously and interfaces for their integration into the cloud stack will have to be defined. The outcome expected from this PhD thesis proposal relates to the improvement of the acceptability of cloud-based infrastructures: the absence of any control on how to secure data is perceived to be a major risk in this framework. Policies and tools will be created that will make it possible to establish responsibilities while striking a balance between transparency and privacy, and to determine issues and constraints for regulators, corporate and institutional service providers, cloud resource consumers, and their end-users. We expect in particular the following results: * Policy language design: identify and address the limitations of existing policy languages such as PPL, XACML and USDL in their ability to accurately represent the concepts of accountability and security for cloud computing. * Policy enforcement: methodologies, software and protocol design approaches, and best practices to achieve compliance with specific accountability policies. * Feasibility study of supporting the methodologies identified previously, and specification of supporting tool/service interface. * Accountability and privacy enforcement tools that can be verified and audited. * New trust models and risk analysis techniques adapted to the cloud.