Securing Loosely-coupled Collaborations in a SaaS Cloud through Risk Estimation and Access Conflict Mediation

by

Nirnay Ghosh

Research Scholar, Department of Computer Science and Engineering, IIT Kharagpur

PhD Thesis Abstract

In recent times, collaborations among multiple autonomous organizations (public-public, public-private, and private-private) have become essential as they allow these domains to easily connect with partners, customers, and employees from remote locations. As a particular stakeholder may not have all the data and services, sharing information through collaboration has become a natural choice. Such initiatives become very useful during emergency situations, where information has to be fetched quickly as well as accurately. Online collaboration is one of the popular services offered by Software-as-a-Service (SaaS) clouds. The nature of such collaborations is loosely-coupled, where collaborating agents share their resources dynamically, and do not have any predefined global policies to govern the interoperations. This thesis attempts to address both security and availability requirements of such cloud-centric collaborations.

Some of the present day SaaS clouds, providing online collaboration, have not been found to deliver consistent service level agreement (SLA) guarantees. As cloud SLAs contains non-standard clauses and unclear technical specifications, it becomes a challenge for customers to select an appropriate service provider to ensure guaranteed service quality. In a service outsourcing environment, like cloud, quality of service levels are of prime importance to any customer, as the latter uses the third-party cloud services to store and process their clients' data. This work focuses on selection of an appropriate collaboration service provider, which is both trustworthy as well as competent enough to fulfill the negotiated guarantees. Trustworthiness is computed from personal experiences gained through direct interactions or from feedbacks related to reputations of vendors. Competence is assessed based on *transparency* in provider's SLA guarantees. Experimental results validate the practicability of the proposed estimating mechanisms.

A major challenge in loosely-coupled collaborations is authorizing access requests from remote users, since the participating domains have only web-based token information the requester and do not know either the latter's security clearance level or the credential information, essential for giving accesses to local resources. Inspite of that, access requests need to be granted so that inter-domain collaborations are not affected. Thus, access risk and security uncertainty related to the requests need to be evaluated before giving accesses. In recent years, researchers have proposed *risk-based access control (RAC)* to address such limitations. To address the issue, this dissertation proposes a customized RAC framework using fuzzy inferences. The framework incorporates soft security mechanism (e.g., reputation) to determine the level of risk involved in providing access to remote user. Further, to choose “better quality” requests for securing collaborations, an optimization problem with the parameters (i) access risk and (ii) security uncertainty, have been formulated. The objective of the optimization problem is to minimize both the parameters. A multi-objective request selection (MORS) algorithm has been proposed to solve the optimization problem and generate a set of requests. Simulation-based analysis and performance evaluation has been presented for validation and demonstrate that the selected requests, if authorized, render more secure collaborations than the existing risk-based access control mechanisms.

The authorized permissions are now required to be mapped to a set of roles which are to be activated by the requester to access the local resources. Mapping the requested permissions into appropriate roles is non-trivial

and is termed in the literature as the *inter-domain role mapping (IDRM)* problem. Two variants of the IDRM problem, viz., the *IDRM-safety* and the *IDRM-availability* address the security and fairness issues in collaborations, respectively. In this thesis, a distributed role mapping framework has been proposed, which implements a novel heuristic to solve the IDRM-availability problem. Results establish efficacy of the proposed approach in comparison to the reported ones. The proposed framework is also observed to be efficient in terms of response time, thus, addressing the scalability requirement of cloud-based services.

Activation of several local roles during a particular user's session may introduce cyclic conflicts which violate the principle of security. In this thesis, two types of conflicts have been considered: (i) *cyclic inheritance*, and (ii) *violation of SoD constraints*. To address this issue, a distributed security framework has been proposed, which dynamically detects and removes these conflicts, thus ensuring that the collaboration is secure, and the requested objects are available. Two features of the proposed framework are: (i) it requires only local information, and (ii) it detects and removes conflicts on-the-fly. Formal proofs have been provided to establish correctness of this approach. Experimental results and qualitative comparison with related work demonstrate the efficacy of the approach in terms of response time.