

Security Issues in Collaborative Computing

(Abstract of Keynote Talk)

Mikhail J. Atallah

Department of Computer Science
Purdue University
CERIAS, Recitation Bldg, West Lafayette, IN 47907, USA
mja@cs.purdue.edu

Even though collaborative computing can yield substantial economic, social, and scientific benefits, a serious impediment to fully achieving that potential is a reluctance to share data, for fear of losing control over its subsequent dissemination and usage. An organization's most valuable and useful data is often proprietary/confidential, or the law may forbid its disclosure or regulate the form of that disclosure. We survey security technologies that mitigate this problem, and discuss research directions towards enforcing the data owner's approved purposes on the data used in collaborative computing. These include techniques for cooperatively computing answers without revealing any private data, even though the computed answers depend on all the participants' private data. They also include computational outsourcing, where computationally weak entities use computationally powerful entities to carry out intensive computing tasks without revealing to them either their inputs or the computed outputs.