Abstract

The purpose of security in ad hoc grid environments is to support secure execution of tasks on shared resources and to protect the resources from malicious user actions. The mechanisms of authentication and authorization commonly used in traditional grid environments are not sufficient to cover all security requirements arising from the decentralized nature of the ad hoc grid. However, the concept of trust management is capable to solve the security issues by incorporating trust into the process of decision making whether or not to execute a user’s task on a selected resource. The quality of made decisions is dependent on a correct assessment and representation of trustworthiness assigned to the potentially collaborating parties. In most cases the value of trustworthiness is derived at least from direct trust and recommendations, but other factors as risk, uncertainty, context dependant information and attributes characterizing the task and the shared resource should be included in the derived value as well. This paper presents an overview of the trust evaluation process and provides a specification of parameters relevant for an accurate trust evaluation.
References


Index Terms

Computer Science Information Sciences

Keywords

Grid entity trust evaluation, trust value parameters, parameters classification