ABSTRACT

The term “grid” (in the context of computing systems) refers to systems and applications that integrate and manage sharing of resources and services distributed across multiple administrative domains. Performance with scalability, optimum utilization of resources, efficient management and reliability and virtualization are some of the advantages of grid-enabled applications. Most of the existing research on grid security is focussed on authentication. Access control and authorization is a relatively less explored area, although very important for grid security. The potential of access control as a security mechanism in grids is one of the major motivating factors behind this work.

Design and development of new models for access control and authorization, specific to grid environment and its security requirements forms the core of this thesis work. The thesis proposes models for representing various access control components of grid security and suggests algorithms to show the association between these components. Our study on the access control and authorization requirements of grid systems helped us to identify the core grid security issues as grid-wide access control and authorization, indirect authorization for the geographically spread users and resources, dynamic authorization and fine-grained access control of the grid resources.

Since a grid-wide mechanism to secure the grid resources does not exist, we proposed an RBAC (Role-Based Access Control)-oriented grid authorization model for the same. This framework includes single-domain (or intra-domain) and cross-domain (or inter-domain) authorization architectures. To facilitate cross-domain authorization, we need to map the role of a given domain to its equivalent role in another domain. A role-mapping architecture is thus proposed. Role-ranking algorithms govern the working of this architecture. We implemented the grid authorization model for single-domain and cross-domain enforcement of access control. Lightweight Directory Access Protocol (LDAP) was used to represent additional user attributes apart from roles. We proposed a Role-Based Grid Delegation Model (RB-GDM) for enforcing indirect authorization based on the user’s role. RB-GDM includes frameworks for delegation within a domain as well as across the domains. To enable the grid users to perform dynamic authorization, we proposed a fuzzy-based scheme called Fuzzy Trust and Delegation Model (FTDM). Finally, a fine-grained authorization framework was presented to introduce finer access control aspects in grid resource access. We implemented the models using programming techniques and fuzzy inference mechanisms.