CHAPTER VIII

CONCLUSION AND FUTURE SCOPE

In this chapter, we summarize the major contributions of the research work presented in this thesis. We also highlight the future scope and further research directions. This thesis contributes to the modelling of grid security measures along with the development of the implementation mechanisms. This work covers the fundamental aspects of grid security through access control modelling. We use algorithmic representations for the theoretical characterization of the proposed models. The applicative issues have been addressed through implementation of authorization systems. Performed on the standard Globus middleware platform, these implementations help us understand the working of the proposed models.

8.1 Summary of Contributions

Grid Computing is rapidly emerging as the dominant paradigm of wide area distributed computing. Its primary objective is to provide a service-oriented infrastructure that leverages standardized protocols and services to enable pervasive access and coordinated sharing of geographically distributed hardware, software and information sources. Grid applications are distinguished from traditional client-server applications by their simultaneous use of large number of resources, dynamic resource requirements, use of resources from multiple administrative domains, complex communication structures and stringent performance requirements among others. While scalability, performance and heterogeneity are the desirable goals for any distributed system, the characteristics of grids lead to security problems that are not addressed by existing security technologies for distributed systems. Many of the present grid security solutions are based on user identity rather than user’s access rights. In the present set up, the resource access is coarse-grained. Further more, the dynamic nature of a grid can make it impossible to establish trust relationships between sites prior to application execution. Also, the
diverse intra-domain access control solutions should interoperate with the inter-domain security technologies.

In this thesis, we have proposed new techniques that overcome many of the cited difficulties. We presented access control models that address requirements for direct authorization, indirect authorization (delegation), inter-operability with local policies (across the multiple administrative domains) and dynamically varying resource requirements. We also presented an implementation mechanism for the models with a case study on “Garuda”, the National Grid Computing Initiative of India. In summary, this thesis makes four major contributions towards the advancement of grid computing security, supported by implementation and case study. The details are as below:

- **Role-Based Direct Authorization:** We provide architectural frameworks for representation of scalable access control and authorization mechanism built on the standard RBAC which uses the concept of role as the unit of authorization. First, we propose a single-domain authorization mechanism by treating the grid as a single logical enterprise. Then we extend this framework for cross-domain authorization for a grid envisaged as a global enterprise comprising diverse physical domains. The first step for cross-domain authorization, is to map the role of a given domain to its equivalent role in another domain. The classical Role Based Access Control, though an effective access control standard for single enterprise, does not address the issue of resolving a local role into a global role. So, we suggested a role-mapping architecture, to establish role equivalence among the domains by mapping a local domain role to its equivalent global role. We use the approach of weighted role-ranking for the same. The authorization decision is then made based on the mapped global role ranking and also the resource access policies.

- **Role-Based Grid Delegation:** We proposed the use of delegation as the primary form of authorization in grids. As credential-based delegation has its own limitations in a dynamic grid environment, a new conceptual model is required to effectively formulate the grid delegation requirements. Here, we present a framework called Role-Based Grid Delegation Model (RB-GDM) for
delegating access rights in a single grid enterprise. The basic unit of delegation in this model is role. Derived from the standard RBAC formalisms, this framework explores various approaches for indirect authorization through delegation. We present the RB-GDM interconnection framework for various scenarios like intra-domain and inter-domain delegation (both peer-to-peer as well as master/slave topologies). We suggest various algorithms and show how the components of these interconnection frameworks work. As the users have the choice of delegating their sub roles (junior roles), this enforces one of the basic principles of security: “The Principle of Least Privilege”.

As revocation of rights is as important as delegation, we present mechanisms by which one can revoke the delegated rights. The revocation methods include grant-dependent, grant-independent as well as timeout revocation. We then extend this technique for cross-domain delegation through roles. We implemented these frameworks on the Globus platform with two academic organizations being used as illustrative domains.

- **Trust-Based Dynamic Delegation Model:** Here, we propose a Fuzzy Trust and Delegation Model (FTDM) to address the dynamic access control requirements of grids. As the grid resources are distributed in space and time, we need to have authorization mechanisms implemented in dynamic context. Also, trust relationships are central to the implementation of security in the dynamic and ever evolving communities like grids. The model comprises a two-stage fuzzy inference process wherein the first stage computes and quantifies the trust values of the sites involved in resource access based on certain criteria and the second stage determines the degree of delegation based on the trust values obtained from the first stage of fuzzy process. Use of fuzzy inference systems to make access decision is a relatively new approach in grids. This methodology suits the dynamic grid environment as fuzziness or uncertainty is typical to dynamic contexts. The rule design used in this model ensures formulation of an efficient dynamic delegation policy in grids.

- **Fine-Grained Access Control Framework for Grid Resources:** We provide a flexible, trust-aware fine-grained access framework for grid access control
from the context of access permissions and resources allocation. Presently grid security mechanisms maintain confidentiality and integrity of resource access through coarse-grained grant/deny permissions to known entities. In the proposed framework, the access policy (grant/deny or partial grant), is governed by the trust relationships among the grid domains. We quantify various categories of trust namely direct trust, transitive trust and asymmetric trust using fuzzy inference process and map these values to access control decisions. We consider varying degrees of access like full access, partial access (fine grained) or access denial (no access). The quantification of trustworthiness of a resource site is done using fuzzy inference systems. This framework can be incorporated with legacy access control mechanisms.

A framework is useful only if it is proven that it works well for that environment. We implemented the authorization models proposed through this thesis on the Globus platform. The implementation proves that these models suit the requirements of grid security. Many of the major issues of grid security have been addressed through these models. We also conducted a case study on the security requirements of “Garuda”, India’s grid initiative and suggested ways to incorporate some of the models to improve “Garuda” security. Though Lightweight Directory Access Protocol (LDAP) has been the basis for GRIP (Grid Resource Information Protocol) of the Globus Toolkit, its use in our work for the storage and retrieval of additional user attributes in the form of a directory structure, is an innovation. We used the eXtensible Access Control Markup Language (XACML) to specify policies which, being platform independent, adds value for inter-operability.

8.2 Conclusion

We have proposed a set of architectural solutions for grid access control and authorization. The models presented in this work support direct access control, delegation, dynamic authorization and trusted computing. The contributions made in this thesis can thus enhance the grid computing security.


8.3 Future Work

In Chapter III of this thesis, we have proposed a grid authorization model which supports inter-domain authorization. To make the design simple, we have considered two sample administrative domains of the same type (academic domain). Where as in real applications, the resource access could be across heterogeneous domains which makes role-mapping even more complex. So, our future work could incorporate heterogeneity in the access control mechanism.

The implementation details which we described in Chapter VII of this thesis advocates the use of XACML for policy representation. But the presence of diverse administrative domains makes a grid characteristically different. Services in grids may use different resources, held by different individuals or organizations. Thus, there is a lot of scope to extend this research work to study the feasibility of using XACML policy integration algorithms in grids. Another extension could be the use of XACML-RBAC, a recent development in XACML which comes integrated with RBAC elements and tags and defines a rich policy format for the generic RBAC and also for the simple Request/Response messages format used for PEP-PDP communication.

Our models provide inter-domain access mechanisms. However, a separate policy communication module between organizations and VOs, could be implemented. This is very essential in the context of ensuring inter-operability with local security solutions. As the fundamental rule of grid security is to have “local control over own resources”, it is impractical to modify every local resource to accommodate inter-domain access. Though there are proposals for formulating a multi-policy framework for grids at the VO level, implementation efforts in this direction have been minimal.

Another possible improvement is regarding the use of LDAP in the grid environment. We have used LDAP to make access control policies more strict by considering additional attributes of the user/resource in the request. There are practical difficulties regarding integration of LDAP with the grid implementation due to the difference in data models. We have used mysql as the back-end database where as the OPEN LDAP implementation supports BERKELEY database. We have to
develop mechanisms by which we can interface LDAP with all database distributions.

In Chapter III of the thesis, we have proposed a role-mapping architecture based on weighted roles to map a role of one administrative domain to another domain. We can improvise this architecture by suggesting a complete and robust algorithm to rank the roles across domains and also to rank the domains in a virtual organization setup. This should be based on the behavioral patterns of the clients and the service providers.

We implemented the models on the Globus platform. But, we believe that security policies or models should not dictate a specific implementation technology. Rather, it should be possible to implement the models with a range of security technologies. Our proposal to implement the authorization models on Garuda Grid is a step in this direction. Implementation of the proposed models on other middleware platforms like the Gridbus, could also be considered.

Although we have incorporated the access control and authorization mechanism as part of the grid service itself, we can make this mechanism generic, if we could separate it as a service itself. This will enable us to implement a common access control interface for a set of varied services.