CHAPTER II

LITERATURE SURVEY ON GRID SECURITY MODELS AND MECHANISMS

2.1 Introduction

The previous chapter of this thesis describes various aspects of grid computing environment and the security issues associated with grids. In this chapter, we present a detailed survey of relevant literature in grid computing security. The aim of this survey work is to present current research trends from the point of view of the security models and authorization mechanisms available in the grid computing environment. Efforts have been made to present an up-to-date research information with details of approaches, algorithms and implementation systems that have been developed and used during the last decade of grid computing evolution.

The chapter has been organized as follows. First we review the literature work in the general area of grid computing security. In section 3, we present various schemes in the grid access control. Section 4 discusses the grid authorization attempts. Section 5 presents the research in trust relationships in grid computing. Next, we present the security issues identified as part of this survey. Section 7 discusses the need for grid access control and the characteristics of an ideal grid security mechanism. Finally we summarize the chapter.

2.2 Grid Security

Grid computing is an interesting and a highly potential area for most enterprises [74] of recent times. Security is one of the major impediments in wide-spread grid adoption. By security, we mean the concepts, techniques, technical measures and administrative measures used to protect the information assets from deliberate or
inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss or use. The standardization effort of grid security has led to the design of security standards in grids which is defined under Grid Security Infrastructure (GSI) [135], [190]. Global Grid Forum (GGF), a consortium of researchers and practitioners was set up for exchanging information and defining standards for grid computing. The Open Grid Standards Architecture (OGSA) proposed by Ian Foster and his group, defines web services [33] for different systems to communicate and share the heterogeneous grid resources.

A grid defines the concept of a Virtual Organization (VO). In a VO, different individuals, enterprises, organizations come together to share resources and services under a set of rules or policies guiding and governing the extent and conditions of sharing. VO can be formed across different universities, across different enterprises as well as within an enterprise also. The level of heterogeneity is high in such situations. Thus the main aspect that separates grid systems and its security from other systems are heterogeneity and complex policies [61]. Marty Humphrey, Mary Thompson et.al, in their work on grid security [139] came up with a comprehensive study on the security aspects of grids. According to them, the most significant challenge for grid computing is to develop a comprehensive set of mechanisms and policies for securing grids. Their work presented the state of the art with regard to grid security and identified open issues. This paper grouped the activities in grids that need to be secured into four categories: naming and authentication; secure communication; trust, policy, and authorization; and enforcement of access control. According to them significant challenges remain in cases like privacy management, denial of service, and integrated cross-domain auditing.

“Security for Grid Services” [128], another work in this area by Von Welch et.al, discusses how one must deal with diverse local mechanisms, support dynamic creation of services, and enable dynamic creation of trust domains. They have also described how these issues are addressed in various versions of the Globus Toolkit, a grid middleware. The combination of dynamic policy overlays and dynamically created entities drives the need for three key functions in a grid security model namely, multiple security mechanisms, dynamic creation of services and dynamic
establishment of trust domains. According to this work, security can be implemented as a service. In summary, the work suggests that secure operation in a grid environment requires that applications and services be capable of supporting a variety of security functionality, such as authentication, authorization, credential conversion, revocation [52], auditing and delegation.

Ian Foster et.al, [128] analyzed the unique security requirements of large-scale distributed (grid) computing and developed a security policy and the corresponding security architecture. An implementation of the architecture within the Globus meta-computing toolkit was also discussed. To identify the security requirements in any environment, the primary step is to understand the environment’s distinctive characteristics.

Accordingly the main characteristics of grid are identified as: large and dynamic user population, large and dynamic resource pool, dynamic computation involving group of processes running on different resources and sites, unicast or multicast communication among the processes, resources requiring different authentication and authorization mechanisms. Also individual user may be associated with different local name spaces, credentials, or accounts, at different sites and finally the resources and the users may be located in different countries. Based on these characteristics the following grid security requirements were identified: authentication, access control, integrity, privacy and non-repudiation. Specifically we need to provide authentication and authorization solutions for users, processes and resources of the grid. Subsequent works outline the generic requirements for security in grid systems and the problems often cited with current grid software. The outcome was the possibility of these issues being resolved by a federation of both users and resources. Also a comprehensive set of grid usage scenarios were presented and analyzed by M Humphrey and M R Thompson in the year 2001 [139], with regard to security requirements such as authentication, authorization, integrity, and confidentiality. There were also works which made suggestions for implementing security without much performance degradation in grids.
2.3 Grid Access Control

There have been some attempts at providing security to the resources of a grid environment through access control. Here we discuss some of such attempts. Kevin Kane and James C. Browne, in their research paper [92], presented a classification of implementations of access control systems based on a lattice taxonomy. Pietro Mazzoleni et.al [186] discussed ways to provide fine-grained access control in large scale grid services. They developed a novel resource broker service for grids that integrates access control with resource scheduling. Weizhong Qiang et.al [202], proposed a general authorization and access control architecture, RB-GACA, for grid environment. It is based on the classical access control mechanism - Role Based Access Control (RBAC). The architecture provides convenient policy evaluation and decision making approach. They provided a framework for access control management that treats the whole grid as a series of independent, interrelated, dynamic domains. Though this approach introduced RBAC in grids, it did not address many issues like delegation, scalability and trust relationships. Also, no provision for cross-domain authorization was made.

Xinwen Zhang et.al [201], in their work, “A Usage-based Authorization Framework for Collaborative Computing Systems”, proposed a usage control (UCON) based authorization framework for collaborative applications. Usage control policies are defined using subject and object attributes [11], along with system attributes as conditions. Earnesto Damiani et.al [69], in their work titled “New Paradigms for Access Control in Open Systems” suggested ways of providing access control in open distributed systems. They surveyed the current state of this research area and came up with the possible future trends in open system access control. There are a few new access control paradigms like the attribute-based models and the semantics-based access control [21] which outline some research and development challenges that should be addressed in this field. “XACML Policy Integration Algorithms”, a work done by P. Mazzoleni et.al [100], suggested the use of XACML, an OASIS [1] standard language for the specification of authorization and entitlement policies. Works like [76] by Gabriel Kuper and [103] by Nathan N Vuong discuss the use of markup languages to present generalized
security views. In [107], Rafae Bhatti et.al proposed an XML-based policy specification framework and architecture for enterprise-wide access control. Virtual enterprises are usually built through collaboration of several autonomous subjects sharing their resources. Their requirements have been addressed by industrial outfits like the IBM [36], [38]. James B.D.Joshi et.al proposed an access control language for multi-domain environments in [47]. Weizhong et.al [118] proposed a VO-based access control model for grids.

2.4 Grid Authorization Systems

In the literature on grid security research, the focus has been on authentication. Here, we discuss some of the research works and also the publications in the area of grid authorization. Access control in any computing environment involves three phases ‘Authentication’, ‘Authorization’ and ‘Accountability and auditing’. These three phases are called the three As of access control. Though authentication forms the foundation for most of the grid security solutions, authorization also has evolved as an important stage of access control [148]. Lorch et.al PRIMA [95], proposes a Policy-Reduced Integrity Measurement Architecture (PRIMA) for grids. They proved how a remote party can verify the integrity properties using PRIMA. R. Alferi and R.Ceccini [12], discussed the evolution of grid authorization from grid map file to Virtual Organization Membership Service (VOMS). A simple authorization implementation, based on a direct user registration on the resources, is not sufficient for large scale environments like grids. According to the authors, VOMS allows fine grained control of the use of the resources both to the users’ organizations and to the resource owners. But the drawback of this approach is that through a membership in VOMS the user gets access to the resources without any fine-grained control. Mary Thompson et.al [99] presented a mechanism called Akenti, for authorization in grids. But, it does not directly address the determination of rights to be granted.

Attribute-based authorization schemes have also been suggested for grid access which can streamline and broaden access control by allowing authorization decisions to be made based not only on user identity, but also user attributes and roles. Community Authorization Service or CAS proposed by Laura Pearlman et.al [196]
is an authorization system built on the Grid Security Infrastructure (GSI). CAS allows resource providers to specify course-grained access control policies in terms of communities as a whole, delegating fine-grained access control policy management to the community itself. The drawbacks of CAS are, it completely removes access control from local resource or service, which is in violation of one of the main properties of grid namely “site autonomy”. CAS also has scalability issues because of central management. In addition, the approach of limiting the group’s privileges [60], through restrictions, to generate a subset of privileges applicable to an individual community member presents a subtractive security mechanism and violates the “least privilege principle” [17]. Authorization and account management in Open Science Grid has been discussed in [98]. Some authentication and authorization mechanisms for multi-domain environments have been discussed in [94].

Another issue is scalable authorization. The work by David Cordes et.al [35] addressed the authorization problem in grid system environments. They came up with a solution for authorization within the Globus system. The authorization approach is based on distributed authorization servers and extensions to Globus Metacomputing Directory Service (MDS). “A Rule-Based Framework for Role-Based Delegation and Revocation” [200], though a contribution not specific to grids, focuses on user-to-user delegation, where a user delegates his/her role to another user. The authors proposed a rule-based framework for role-based delegation. A rule-based system is one where all behaviors are governed by a set of explicit rules. The major requirements of role-based delegation were identified as support for multi-step delegation, support for different revocation schemes, support for constraints and support for partial delegation. But this work was a general framework meant for enterprises. Issues specific to grids were not addressed in this paper.

James B.D.Joshi et.al [183] suggested an integer programming (IP) approach for secure inter-operation involving RBAC policies. But their work also does not reflect the distinct characteristics and requirements of grid authorization. Another proposed approach is user-credential based role-mapping where by a user’s credentials associated with the role form the basis for role-mapping [146]. As the
fundamental unit of RBAC is a role and since one user can be mapped to multiple roles, we cannot use the user’s credentials as the sole criteria for role mapping. Liang Chen et.al [30], proposed an inter-domain role mapping technique based on the principle of least privilege. They suggested a minimal cardinality for a role within a domain to avoid misuse of access. But this constraint may work against the dynamic and heterogeneous access requirements of grids.

Some of the existing grid authorization mechanisms are Permis [67], [28], Akenti [99], Shibboleth [181], VOMS [12] and CAS [196]. Though Permis, Akenti and CAS introduce the concept of roles in a grid environment, they are not role-based access control implementations like the standard RBAC. Also they lack the flexibility of RBAC and are static in nature. CAS is primarily a community based authorization service, it allows resource providers to specify course-grained access control policies in terms of communities as a whole, delegating fine-grained access control policy management to the community itself. The major drawback is the lack of scalability and denial of basic right for every node to decide its users.

"A Multi-policy Authorization Framework for Grid Security", a work by Bo Long et.al [55], suggested a framework for authorization in a grid system based on multiple policies across the domains. The grid environment needs to be flexible and scalable to support multiple security policies. The absence of a standard role-mapping mechanism to address the grid authorization and access control issues combined with the fact that the present form of RBAC for single enterprises does not support grid access control motivated us to develop a new architecture which can truly reflect a multi-domain grid access environment.

2.5 Trust in Grid Systems

Significant amount of research has been done in the area of trust relationships in distributed systems in general and grid environment in particular. Woodas et.al [169], proposed trust models for distributed systems and suggested that distributed trust models assume asymmetrical trust. They also talked about combining trust values of different applications. Snelling et.al, [188] suggested the use of explicit trust relationships for providing security in dynamic grids. Farag Azzedin
et.al [13], proposed a trust-aware resource management mechanism for grids. Resource optimization in grids has been another area where the concept of trust has been suggested [140]. Liu et.al [156], et.al proposed a mission-aware trust model for grid computing systems. Internet applications also extensively use the concept of trust [132], [133], [134]. The usefulness of trust in ubiquitous computing has been highlighted in [184]. Jeffrey Dwoskin et.al [85], in their research work, defined three generic grid security scenarios: mutual trust, partial trust (distrusted user) and mutual distrust. According to them, decreasing levels of trust enable one to expose new vulnerabilities and show the increasing levels of security support required.

2.6 Shortcomings of the Existing Solutions

The existing approaches to grid security fail to provide a holistic solution to grid security. Primarily, authentication has been in use for providing security in grids. Authorization has proven to be a successful alternative or addition to authentication in providing security to today’s enterprise applications. Also, security in dynamic context is another aspect which we need to consider. Building trust relationships between the organizations in a grid can contribute to grid security. Fine-grained access control of the resources is another important requirement in grids. Providing security to the geographically spread resources is a real challenge, which, many of the existing solutions seem to neglect. We need to come up with solutions for grid computing security keeping in mind its characteristics. i.e, We need to provide a specific security mechanism for grids in place of the existing generic approaches. As a first step in this regard, we identified various security issues in grids, which led us to the need for access control in grids. From the findings of the literature survey we have arrived at the characteristics of an ideal grid access control mechanism which we explain in the following section. These characteristics govern the design of the authorization models which we have proposed through this thesis.
2.7 Security Issues Identified in Grids

Based on the extensive literature survey conducted with regard to grid computing environment in general and grid security and authorization in particular, we have come up with some observations, which guide us through the design and development of a grid access control mechanism. We first identified the security issues in grids, the need for access control in grid systems and finally came up with the desirable features of a grid access control and authorization mechanism. As grids are decentralized, dynamic and distributed in nature, they require security mechanisms that allow seamless access to resources to the users of different organizations [58]. The most significant challenge for grid computing is to develop a comprehensive set of mechanisms and policies for securing the Grid. The security constraints resulting from the distinctive characteristics of grid computing environment include:

- Large and dynamic user population which belong to many physical organizations and which may change frequently
- Large and dynamic resource pool contributed by different physical organizations which can change rapidly.
- The possibility that a computation may acquire, start processes on, and release resources dynamically during its execution. In other words, throughout its lifetime, a computation is composed of a dynamic group of processes running on different resources and sites
- Resources may require diverse authentication and authorization mechanisms and policies
- Resources and users may be located in different locations

Other security issues derived from the characteristics of the grid environment include [141]:

1. **Single sign-on**: A user should be able to authenticate once and initiate computations that require resources, use resources, release resources without further authentication of the user
2. **Delegation:** A user must be able to endow to a program/user the ability to run on that user’s behalf, so that the program/user is able to access the resources on which the user is authorized. The program/user should also be able to further delegate to another program/user.

3. **Inter-operability with local security solutions:** While the security solutions may provide inter-domain access mechanisms, access to local resources will typically be determined by a local security policy that is enforced by a local security mechanism.

4. **Naming:** Users in the grid must be identified unambiguously and globally which means that a user needs a distinguished name which is unique throughout the grid. The X.500 naming structure is an attempt to define enough components that people can be named uniquely and meaningfully. X.509 names, derived from the X.500 standard, are commonly used in grids to provide global names for users and hosts.

### 2.8 Need for Access Control in Grids

Access Control is the secure evaluation of whether an established identity can have access to a particular resource, also referred to as an object. The following grid characteristics point to the need for enforcing access control in grids.

1. The resources in a grid environment are owned by multiple institutions. Each individual institution may give preference to local users (belongs to the same institution) than users of other domains.

2. The service providers restrict the access to their resource.

3. At the organization level users of higher authority may get more preference than users with lower authority.

4. Resources in the grid environment are valuable, confidential and need different levels of authorization.

5. Resources have their own restrictions to take into account before providing services to the requests [37] (for example, a server may consider availability of its free memory, CPU load etc before accepting the request).
2.8.1 Characteristics of An Ideal Grid Access Control Mechanism

As discussed in section 2.2, a grid is a virtual organization which consists of a set of institutions. Therefore, an efficient grid access control system should meet the following requirements:

- **Suitability for the Organization’s Needs:** Each organization, in real world consists of hierarchy of users and different set of permissions associated for the respective users.

- **Scalability:** Grids consist of large and dynamic users. So, the access control mechanism must be able to deal with large number of users.

- **Maintainability:** User populations and resources are often large and unstable in a grid system environment. Access control information between users and resources may be adjusted and changed at any time. The grid authorization service must ensure that the associated administration and maintenance work is able to keep pace with the dynamic nature of the grid system.

- **Variety of security policies:** The authorization scheme must be able to express a variety of security policies. Since each organization unit and resource may have different ways of specifying its own security policy, this flexibility is essential.

2.9 Chapter Summary

This chapter focuses on the related research which has taken place over the past few years in the area of grid computing security. The last decade has seen tremendous development with regard to grid technology. We carried out an extensive literature survey, on the research work done in the grid computing area in general and grid security and access control in particular. The chapter starts with a brief introduction to grid technology. In the later sections, we discuss the research work which has taken place in grid computing security, followed by research on grid access control and grid authorization. We explain in detail, various research papers published in this area, the major contributions and their drawbacks. Various
authorization attempts in grid security implementation have been discussed thoroughly. We also discussed the importance of trust relationships in grids and implementing security based on trust values across domains. We presented a summary of major security issues in grids, the need for access control in a grid environment and also the desirable features of a grid access control mechanism.

The literature survey on related work motivated us to take up the following research directions. In Chapter III, we come up with a role-based grid authorization model which is the resultant of our study on Role Based Access Control. In Chapter IV, we have suggested a delegation model for grids. It is the outcome of the study and survey we conducted on the delegation requirements in grids. Our research on the dynamic delegation requirements in grids motivated us to propose a trust-based dynamic delegation model for grids. This is explained in Chapter V of the thesis. To facilitate a fine-grained access mechanism for grid resource access we have created a framework as shown in Chapter VI. During the course of the literature survey we felt the lack of sufficient work as well as survey material in the area of implementation of grid security. To fill the gaps and also to test our models, we prepared an implementation set up, the details of which are explained in Chapter VII of this thesis.