Table of Contents

List of Figures

List of Tables

Certificate

I hereby certify that the work which is being presented in this thesis entitled **"A Security Policy Framework for Grid Services"**, in partial fulfillment of the requirement for the award of degree of "Doctor of Philosophy" submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Seema Bawa and refers other researchers works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Sarbjeet Singh 16/06/09

(Sarbjeet Singh)
Regn. No. 9040355

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Seema Bawa 16/06/2009

(Dr. Seema Bawa)
Professor & Head
Department of Computer Science & Engineering
Thapar University
Patiala – 147 004
Punjab, INDIA

Acknowledgements

I would like to express my sincere gratitude to Professor Seema Bawa for her valuable advices, direction, and encouragement during my doctoral research endeavor for the past four years. Her observations and comments helped me to remain focused and move forward in the direction of improvement. It was only because of her support and all around help that I am able to complete the thesis in time. I thank her for providing me the opportunity to work with her.

I would like to express my sincere thanks to Doctoral Committee Members – Professor R.S. Kaler and Professor R.K. Sharma, and Dean of Research and Sponsored Projects – Professor Sushil Mittal, for their critical observations and valuable comments which helped enormously in presenting results and shaping this thesis.

I am thankful to Dr. Maninder Singh, Assistant Professor, for their valuable suggestions and help in setting up the environment for framework implementation.

I would like to thank faculty and staff members of Computer Science & Engineering of Thapar University, Patiala for providing and sharing resources that have been utilized in different implementations of the framework.

I am also grateful to colleagues and staff members of University Institute of Engineering and Technology, Panjab University, Chandigarh for their cooperation. They always helped me to spare time for research.

I would like to express special thanks to Anju Sharma (Thapar University), Inderveer Channa (Thapar University) and Bhupinder Singh (Siemens) for making research a wonderful experience for me.

I would like to thank administrative and academic staff members of Thapar University and Panjab University who have been kind enough to advise and help in their respective roles.

I am also grateful to numerous others who have directly or indirectly contributed towards carrying out the research in all aspects during last four years.

Last, but not the least, I would like to dedicate this thesis to my family, my father, my mother, my wife and twin daughters Agampreet and Avneet for their love, patience and understanding. They allowed me to spend most of the time on this thesis.

Sarbjeet Singh 16/06/09

Sarbjeet Singh

Abstract

Grid computing deals with flexible, secure and coordinated sharing of resources that are distributed over wide area networks. With the evolution of this field, the complexity of the distributed systems has increased and therefore the implementation of a secure environment has become difficult. At the same time, grid setups necessarily require a secure environment where users/organizations have access to resources, precisely on the basis of their rights, with proper accountability and control. This thesis work implements a security policy framework to address key security requirements (mainly identified as authentication, privacy, trust and authorization) and provide support to express, evaluate and enforce security policies related to these requirements.

The identified security requirements of grid systems have been categorized mainly into four security disciplines which are authentication, privacy, trust and authorization. Therefore, the framework implements four different models namely authentication model, privacy model, trust model and policy based authorization model. These models address security requirements and policies specific to their respective disciplines.

To achieve the set objectives, a comprehensive literature review of developments related to grid and web services, their method of operation and execution has been done. The similarities and differences between the two have been brought out. A thorough study and analysis of standards and specifications used in grid and web services based systems has also been carried out. Previous work done in the areas of authentication, privacy, trust and policy based authorization in grid systems has been studied, extended in the form of a framework, and reported in detail.

Out of the four models, the authentication model provides support for single sign-on and delegation features using proxy certificates and a credential management service to store, retrieve and update multiple user credentials. The privacy and trust models provide privacy and trust based access to grid services. The privacy model in particular provides support for anonymous access, hidden service access and access to private information based on conformance to privacy policies. The trust model provides support for

calculating direct as well as recommended trust to determine trustworthiness of target services/resources. All these models also describe how the security policies related to them can be expressed and evaluated. The policy based authorization model provides access to grid services based on conformance to various types of security policies. The policy specification, evaluation and enforcement related functionality of authentication, privacy and trust models has been incorporated into policy based authorization model and the resulting model is called the integrated policy based authorization model.

The complete framework has been evaluated by implementing different security related scenarios and through implementations involving enforcement of different types of access control policies. These scenarios and implementations cover different aspects related to authentication, privacy, trust and authorization. The results show that the various implementations are able to meet the identified security requirements. The results clearly demonstrate that the approach is workable and can be effectively used to address key security requirements related to authentication, privacy, trust and authorization, and further to provide policy based access to grid services/resources.