

# Table of Contents

List of Figures .....	vi
List of Tables .....	ix
Certificate.....	x
Acknowledgements.....	xi
Abstract.....	xiii
<b>Chapter 1. Introduction .....</b>	<b>1</b>
1.1 Distributed Computing.....	1
1.2 Grid Computing .....	2
1.2.1 Grid Application Areas .....	3
1.3 Grid and Web Architecture.....	4
1.3.1 Grid Architecture .....	4
1.3.2 Web Services Architecture .....	5
1.4 Grid and Web Services .....	7
1.4.1 OGSA, OGSF and WSRF.....	7
1.4.2 Relationship between Grid and Web services .....	8
1.4.3 Grid and Web Services Invocation .....	9
1.5 Grid Security.....	11
1.6 Building Blocks for Grid Security .....	12
1.6.1 XML, SOAP, WSDL and UDDI .....	13
1.6.2 Web Services Security Specifications .....	14
1.6.3 Security Assertion Markup Language (SAML).....	15
1.6.4 eXtensible Access Control Markup Language (XACML) .....	16
1.7 Organization of the thesis .....	17
<b>Chapter 2. Literature Review .....</b>	<b>19</b>
2.1 Grid Security: The Multidimensional Problem.....	19
2.1.1 Grid Security Requirements.....	20
2.1.2 Grid Security Frameworks.....	24
2.2 Authentication.....	30
2.2.1 Authentication Schemes.....	30
2.2.2 Additional security requirements related to authentication .....	32

2.2.3	Authentication in existing middleware .....	34
2.3	Privacy .....	36
2.3.1	Privacy Issues.....	37
2.3.2	Privacy handling in existing middleware.....	38
2.4	Trust.....	41
2.4.1	Taxonomy of Trust .....	43
2.4.2	Approaches used for managing trust.....	45
2.4.3	Trust management in existing middleware .....	47
2.5	Authorization .....	50
2.5.1	Authorization Issues.....	50
2.5.2	Approaches used for Authorization .....	51
2.5.3	Authorization in existing middleware.....	53
2.6	Problem Formulation .....	59
2.7	Objectives of the thesis .....	59
<b>Chapter 3. Elements identified for the Framework.....</b>		<b>62</b>
<b>Chapter 4. Security Policies Categorization for the Framework .....</b>		<b>70</b>
4.1	Security Policies.....	70
4.1.1	Access Control Policies .....	71
4.1.2	Non Access Control Policies .....	71
4.2	Access Control Policies Categorization.....	72
4.2.1	Authentication Policies (ANPs).....	73
4.2.2	Privacy Policies (PPs).....	74
4.2.3	Trust Policies (TPs).....	74
4.2.4	Authorization Policies (APs) .....	75
4.3	Policy Expression.....	77
<b>Chapter 5. Security Policy Framework .....</b>		<b>83</b>
5.1	Authentication Model .....	83
5.1.1	Single Sign-on and Delegation .....	83
5.1.2	Nonrepudiation, Confidentiality, Integrity and Secure Communication.....	86
5.1.3	Credential Management.....	86
5.1.4	Services defined, implemented and exposed by Authentication Model .....	89
5.2	Privacy Model.....	91

5.2.1	Privacy Infrastructure.....	91
5.2.2	Hidden/Secret Services and Anonymous Access .....	94
5.2.3	Privacy based Access.....	96
5.2.4	Services defined, implemented and exposed by Privacy Model.....	98
5.3	Trust Model.....	99
5.3.1	Trust Relationships .....	100
5.3.2	Trust Evaluation.....	101
5.3.3	Trust Manager Service.....	107
5.3.4	Services defined, implemented and exposed by Trust Model .....	108
5.4	Policy based Authorization Model.....	109
5.4.1	Authorization System.....	109
5.4.2	Policy Based Access System .....	112
5.4.3	High Level View of Implementation .....	115
5.4.4	Services defined, implemented and exposed by Integrated Policy Based Authorization Model.....	116
5.5	Distinguished Features of Models .....	117
	<b>Chapter 6. Implementation Results and Performance Analysis .....</b>	<b>120</b>
6.1	Scenarios Implementation.....	121
6.1.1	Scenarios related to Authentication .....	122
6.1.2	Scenarios related to Privacy.....	123
6.1.3	Scenarios related to Trust.....	125
6.1.4	Scenarios related to Authorization.....	126
6.2	Performance Analysis .....	128
6.2.1	Performance analysis of authentication policies.....	129
6.2.2	Performance analysis of privacy policies .....	133
6.2.3	Performance analysis of trust policies .....	136
6.2.4	Performance analysis of authorization policies .....	139
6.2.5	Comparison of authentication, privacy, trust and authorization policies.....	142
	<b>Chapter 7. Conclusion and Future Scope.....</b>	<b>145</b>
7.1	Conclusion .....	145
7.2	Future Scope .....	148
	<b>References.....</b>	<b>150</b>
	<b>List of Publications .....</b>	<b>164</b>

# List of Figures

Figure 1.1: The layered Grid architecture and its relationship to the Internet protocol architecture [2] .....	5
Figure 1.2: Web Services Architecture Stack [14] .....	6
Figure 1.3: Schematic showing (a) Stateless web service (b) Stateful web service (c) Grid service. ....	9
Figure 1.4: A typical web service invocation scenario .....	10
Figure 2.1: A Computational Grid Security Architecture [24] .....	25
Figure 2.2: Web Services Security Specifications .....	27
Figure 2.3: Components of Grid Security Model [43] .....	28
Figure 2.4: Authorization Push Sequence .....	52
Figure 2.5: Authorization Pull Sequence .....	52
Figure 2.6: Authorization Agent Sequence .....	53
Figure 3.1: Schematic showing Grid Environment consisting of three domains along with other elements of the security framework .....	66
Figure 4.1: Schematic showing authentication, privacy, trust and authorization policies among different entities in a grid environment .....	72
Figure 4.2: Interrelationship among different types of policies .....	76
Figure 4.3: XACML policy language model .....	77
Figure 4.4: Skeleton of policy written in XACML format .....	79
Figure 4.5: Skeleton of policy representing purpose and context attributes in XACML format .....	80
Figure 4.6: Skeleton of policy file associated with a service/resource .....	81
Figure 5.1: Proxy creation and action .....	84
Figure 5.2: Credential Retrieval using Credential Manager Service .....	88
Figure 5.3: Usage of Credential Manager Service .....	89
Figure 5.4: Schematic representing grid environment consisting of three domains showing how privacy requirements among subjects and services of different domains are handled .....	92
Figure 5.5: Schematic showing how anonymous access to a Service is provided .....	96
Figure 5.6: Trust Model architecture for trust based access .....	107
Figure 5.7: Schematic showing the use of Filter-In and Filter-Out components .....	110

Figure 5.8: Integrated Policy Based Authorization Model .....	114
Figure 5.9: Schematic showing high level view of the implementation.....	115
Figure 6.1: Schematic showing Single Sign-On.....	122
Figure 6.2: Schematic showing Delegation and Single Sign-On.....	122
Figure 6.3: Schematic showing access of private information based on established privacy policies and relationships.....	123
Figure 6.4: Schematic showing anonymous access of a service.....	124
Figure 6.5: Schematic showing access of a hidden service .....	124
Figure 6.6: Schematic showing determining direct trust with a service .....	125
Figure 6.7: Schematic showing determining direct and recommended trust with a service .....	125
Figure 6.8: Schematic showing access based on conformance to service's policies.....	126
Figure 6.9: Schematic showing scenario related to distributed authorization .....	127
Figure 6.10: Schematic showing scenario related to federation of security services .....	127
Figure 6.11: PIP time to evaluate individual authentication policy .....	130
Figure 6.12: PDP time to evaluate individual authentication policy .....	130
Figure 6.13: PEP time to evaluate individual authentication policy.....	131
Figure 6.14: PIP time to evaluate authentication policy file of different sizes.....	131
Figure 6.15: PDP time to evaluate authentication policy file of different sizes .....	132
Figure 6.16: PEP time to evaluate authentication policy file of different sizes.....	132
Figure 6.17: PIP time to evaluate individual privacy policy .....	133
Figure 6.18: PDP time to evaluate individual privacy policy .....	134
Figure 6.19: PEP time to evaluate individual privacy policy .....	134
Figure 6.20: PIP time to evaluate privacy policy file of different sizes .....	135
Figure 6.21: PDP time to evaluate privacy policy file of different sizes.....	135
Figure 6.22: PEP time to evaluate privacy policy file of different sizes .....	135
Figure 6.23: PIP time to evaluate individual trust policy .....	136
Figure 6.24: PDP time to evaluate individual trust policy.....	137
Figure 6.25: PEP time to evaluate individual trust policy .....	137
Figure 6.26: PIP time to evaluate trust policy file of different sizes .....	138
Figure 6.27: PDP time to evaluate trust policy file of different sizes.....	138
Figure 6.28: PEP time to evaluate trust policy file of different sizes .....	139
Figure 6.29: PIP time to evaluate individual authorization policy .....	140
Figure 6.30: PDP time to evaluate individual authorization policy.....	140

Figure 6.31: PEP time to evaluate individual authorization policy .....	140
Figure 6.32: PIP time to evaluate authorization policy file of different sizes .....	141
Figure 6.33: PDP time to evaluate authorization policy file of different sizes.....	141
Figure 6.34: PEP time to evaluate authorization policy file of different sizes .....	142
Figure 6.35: Comparison of PEP time to evaluate individual authentication, privacy, trust and authorization policies .....	143
Figure 6.36: Comparison of PEP time to evaluate authentication, privacy, trust and authorization policy files of different sizes.....	143

# List of Tables

Table 2.1: Comparison of existing middleware in terms of their support in the areas of authentication, privacy, trust and authorization. ....	58
Table 3.1: Privacy Index levels and their meaning.....	64
Table 5.1: Sequence of steps for proxy certificate creation and usage.....	85
Table 5.2: Sequence of steps representing how a subject retrieves credentials using CMS .....	88
Table 5.3: Services defined, implemented and exposed by authentication model .....	90
Table 5.4: Sequence of steps for privacy based access to grid services/resources .....	97
Table 5.5: Services defined, implemented and exposed by privacy model.....	99
Table 5.6: Levels of trust with $\alpha = 0.5$ and $\beta = 0.5$ .....	102
Table 5.7: Pseudo code to calculate trust value .....	104
Table 5.8: Pseudo code to calculate direct trust.....	104
Table 5.9: Pseudo code to calculate recommended trust .....	105
Table 5.10: Services defined, implemented and exposed by trust model.....	109
Table 5.11: Sequence of steps for policy based access to grid services/resources .....	113
Table 5.12: Services defined, implemented and exposed by integrated policy based authorization model .....	117
Table 6.1: Average time taken by PIP, PEP and PDP components to evaluate authentication, privacy, trust and authorization policies. ....	142

## 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.

*Sarbjeeet Singh*  
(Sarbjeeet Singh) 16/06/09  
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*  
(Dr. Seema Bawa) 16/06/2009  
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.

Sarbjeeet Singh  
16/06/09

Sarbjeeet 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.