Chapter 7

Conclusion and Future Scope

7.1 Conclusion

The thesis addresses important security requirements mainly identified as authentication, privacy, trust and authorization and implements a security policy framework. The security policy framework has four models namely authentication model, privacy model, trust model and policy based authorization model. These models address security requirements and policies specific to authentication, privacy, trust and authorization. The policy specification, evaluation and enforcement related functionality of authentication, privacy and trust models have been incorporated into policy based authorization model and the resulting model is called the integrated policy based authorization model. The integrated model is capable of providing access to grid services based on conformance to different types of security policies and also allow us to treat the policy involving different combinations of authentication, privacy, trust and authorization related aspects as a single unit.

To achieve the set objectives, a comprehensive review of development related to grid and web services has been done. A thorough study of standards and specifications used in grid and web services based systems is also carried out. Work done in the areas of authentication, privacy, trust and authorization in grid systems has been studied and reported in detail. Following paragraphs describe the characteristics and important features provided by individual authentication, privacy, trust and integrated policy based authorization model.

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 features provided by the authentication model are:

- ✓ It provides credential repository and a service to manage multiple user credentials.
- ✓ It is based on Web Services Security specifications like WS-Security, WS-SecureConversation etc.
- ✓ It supports the storage of multiple types of tokens/credentials. (e.g. X.509, Kerberos, Custom Security Token etc.)
- ✓ It can be used for grid as well as web services.
- ✓ CMS is distributed over different domains, therefore removes the drawbacks of central storage.
- ✓ It provides support for single sign-on and delegation through proxy certificates.
- ✓ It provides a mechanism to express, evaluate and enforce authentication policies.

The privacy model provides support for anonymous access, hidden service access and access to private information based on conformance to privacy policies. Following features have been provided by the privacy model:

- ✓ It supports purpose based access to private information/resources.
- ✓ It supports hidden service access through custom security tokens.
- ✓ It supports anonymous access through the concept of anonymous security tokens.
- ✓ It provides mechanisms to handle privacy requirements of both, the service requesters as well as service providers.
- ✓ It provides mechanisms to express, evaluate and enforce privacy policies between service providers and requesters.
- ✓ It describes the integration of privacy based access with authorization framework.
- ✓ It uses XACML to express access control privacy policies which is OASIS standard.

The trust model provides support for calculating direct as well as recommended trust to determine trustworthiness of target service to enable trust based access. Following features have been provided by the trust model:

- ✓ It can deal with identity as well as behavior trust.
- ✓ It provides support to calculate direct as well as recommended trust.
- ✓ It provides mechanisms to express, evaluate, and enforce trust policies.
- ✓ It describes the integration of trust based access with authorization framework.

- ✓ It also supports updation and management of trust relationships.

Integrated policy based authorization framework provides policy based access to grid services and integrates privacy and trust models by implementing trust and privacy based access. It provides support to express, evaluate and enforce different types of security policies (authentication, privacy, trust and authorization policies). It enables us to treat and specify the policy involving combination of authentication, privacy, trust and authorization related aspects as a single unit. The framework is flexible, scalable, supports fine grained access to services/resources and is able to express and enforce VO wide and other access control security policies. Following are the features provided by the authorization model:

- ✓ It supports fine grained and context based access to grid services/resources.
- ✓ Policy expression is platform independent.
- ✓ It is able to express and enforce VO wide and service wide access control policies.
- ✓ It introduces Filter components which make it flexible and scalable.
- ✓ It extends basic authorization mechanism to include trust and privacy based access to grid services.
- ✓ It supports multiple security policies and provides facilities to integrate different authorization mechanisms.

The security policy framework has been evaluated by implementing various security related scenarios and through implementations that involve enforcement of different types of access control policies. The implementation has been done in .NET environment with the support of WSE 3.0 toolkit.

From scenario implementations it is clear that the framework can be used to implement single sign-on and delegation features in grid systems. It can also be used to address privacy and trust related issues among service providers and service requesters. It provides support for purpose based access and anonymous access to grid services/resources. It can also be used to determine direct and recommended trust on a target service/resource. The framework is also capable of implementing policy based access to grid services and supports distributed authorization and federation of security services.

From experimental results, it is observed that total time required to evaluate different policies increases linearly with the increase in number of policies and does not become an overhead for the authorization framework. Increasing the number of policies attached with a service does not adversely affect the performance of the authorization framework. Authentication policies takes less time and trust policies takes more time to evaluate compared to evaluation of privacy and authorization policies. The performance can be a concern if the number of trust policies attached with a service / resource are more. For trust policies, the total evaluation time increases more assertively compared to other policies. This is because determination of trust value of target involves calculations and access to history of past interactions taken place between source and target which are time consuming. The time taken by privacy and authorization models in evaluating policies is close to each other. This is because both involve almost similar type of access to subject, resource, environment and other attributes. Authentication policies take less time to execute as they require little access to resource, environment and other attributes compared to other policies and almost all the information required to evaluate authentication policy is available in the access request itself.

The implementations carried out and results obtained demonstrate that the identified objectives have been achieved and the approach is workable. The framework can be used to address key security requirements related to authentication, privacy, trust and authorization, and to provide policy based access to grid services.

7.2 Future Scope

For the implementation of the framework, the necessary functionality has been developed and used wherever required, no XACML and SAML specifications implementation tools have been used. The certificates and other credentials used in the implementation have been generated through tools available in .NET environment. In future, the framework can be implemented using third party tools that provide specific implementation of many technologies and specifications. This will make the implementation and management of the framework more flexible.

The authentication model can be extended to include more types of security tokens. Work in the area of securing CMS can be started. CMS can be extended to include support for credential expiry notifications. Privacy model makes use of anonymous security token and custom security token to provide anonymous access and hidden service access. Work on standardizing these security tokens can be started. Trust model can be extended to incorporate other attributes like honesty, accuracy, risk, time *etc*. Policy based authorization model can be extended by implementing more types of authorization mechanisms and integrating them. Work in the area of identifying and resolving conflict policies can also be started. Currently the framework provides support to express, evaluate and enforce access control policies but in future can be extended to include non access control policies like resource usage and business policies. Work can be initiated on defining and implementing an accounting and audit model. Study can be started on anti virus, intrusion detection and intrusion protection mechanisms also. Thesis has not touched the attacks that can be possible on the implemented security policy framework. A detailed analysis of different kinds of attacks and their protection mechanisms can be taken as a future work. As security is a multi dimensional problem, a lot many areas for future work exist and can be carried out.