Public Abstract
First Name:Harcharan
Middle Name:
Last Name:Singh
Adviser's First Name:Gordon
Adviser's Last Name:Springer
Co-Adviser's First Name:
Co-Adviser's Last Name:
Graduation Term:SS 2011
Department:Computer Science
Degree:MS
Title:FAULT TOLERANT AND HIGHLY AVAILABLE ENTITLEMENT SERVER

Web accessible resources containing research related data and information have been important for researchers for the past 15 years. The sharing of information through the web leverages the research and development process. At present, the web is one of the most popular, fast, and convenient mediums for sharing resources. Originally, all resources made available on the web were accessible to anyone with a web browser. However, this has been found to be unsatisfactory for a variety of reasons and situations. Thus, recent efforts have been made to provide protection of users and resources using the robust capabilities of the web.

The current project is based, in part, on the use of Shibboleth to provide restricted access to resources via the web. Shibboleth consists of the Service Provider and an Identity Provider to authenticate access to the resources. These services and the incorporation of a separate Entitlement Server provide fine-grained access to protected resources. This project incorporates multiple Entitlement Servers to provide a robust authorization environment that can continue to operate in the event of server or network failures in the trusted environment.

The design proposed in this project decentralizes the authorization process by running multiple entitlement server applications in the network. All servers form a logical group, which is used for the authorization process. The project outlines a procedure of interaction between a service provider and the group of entitlement servers for performing the authorization of users. Multiple entitlement servers in the network help in achieving a fault tolerant and highly available authorization process. All entitlement servers in the logical group stay synchronized. The authorization process can proceed when at least one entitlement server is present in the logical group.

Each of the entitlement servers present in the group maintains enough information about the users to make detailed authorization decisions. An information synchronization methodology is utilized such that each of the entitlement servers has consistent data. The scalable architecture of the authorization process allows the addition of an additional entitlement server to the group on the fly. Moreover, the entitlement server can move in the network from one physical machine to another without affecting the authorization process. The design also considers the security risk factors so that any communication message between two entities is encrypted to avoid disclosure of the messages. Similarly, the active servers in the network mutually authenticate each other to avoid having an imposter server attempting to break into the authorization process.