タイトル、所属、見出し　Helvetica Bold
本文、問合せ　Helvetica Regular

A Grid-aware Access Control and Data Filtering Mechanism

Cybermedia Center, Osaka University, Japan

Recently, the Grid has increasingly gathered the attention and interest of scientists and researchers as a building block technology for computational infrastructure. In reality, however, the Grid is not utilized well in today's actual scientific research areas because of security problems. Generally, in a Grid environment, many users with various user attributes are supposed to utilize a diversity of computational and data resources. For this reason, an access control solution that forces users to access such resources properly depending on the users' attributes is essential.

Architecture of our Grid-aware Access Control and Data Filtering Mechanism

In general, access control is performed through the two operations of authentication and authorization. Authentication is an operation of verifying the identity of the individuals, and authorization is an operation that determines what kind of actions can be permitted to the identified individuals.

Our Grid-aware access control and data filtering mechanism takes advantage of the synergy of Grid Security Infrastructure (GSI) and MyProxy as authentication technologies, Privilege and Role Management Infrastructure Standards (PERMIS) as an authorization technology, and XSLT (XML Stylesheet Language Transformations) as an filtering technology. Our Grid-aware access control allows users to access data of their interest based on Role-based Access Control (RBAC) using digital certificates.

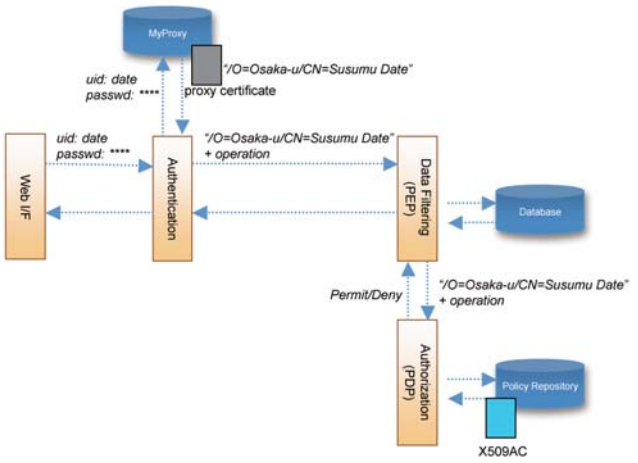

Fig.1: Access Control and Data Filtering Mechanism in Action

The mechanism is composed of Authentication, Authorization, and Data Filtering modules. Authentication module uses MyProxy, an on-line credential repository for retrieving users' proxy certificates registered in advance. The Authorization module as a policy decision point contacts the Policy Repository to retrieve an attribute certificate corresponding to the users' role. The Data filtering mechanism filters XML data retrieved from the Database to appropriate XML data to the users' role.

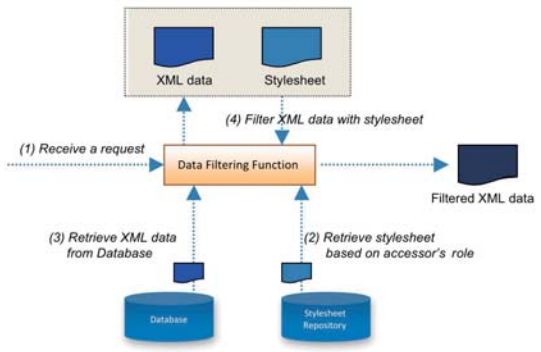

Fig.2: Data Filtering Module (PEP) in Action

The XML data retrieved from the Database is filtered with a stylesheet appropriate to the accessing user's role. The stylesheet is written in XSL.

Application Example: A Clinical Database for Parkinson's Disease Research and Diagnosis

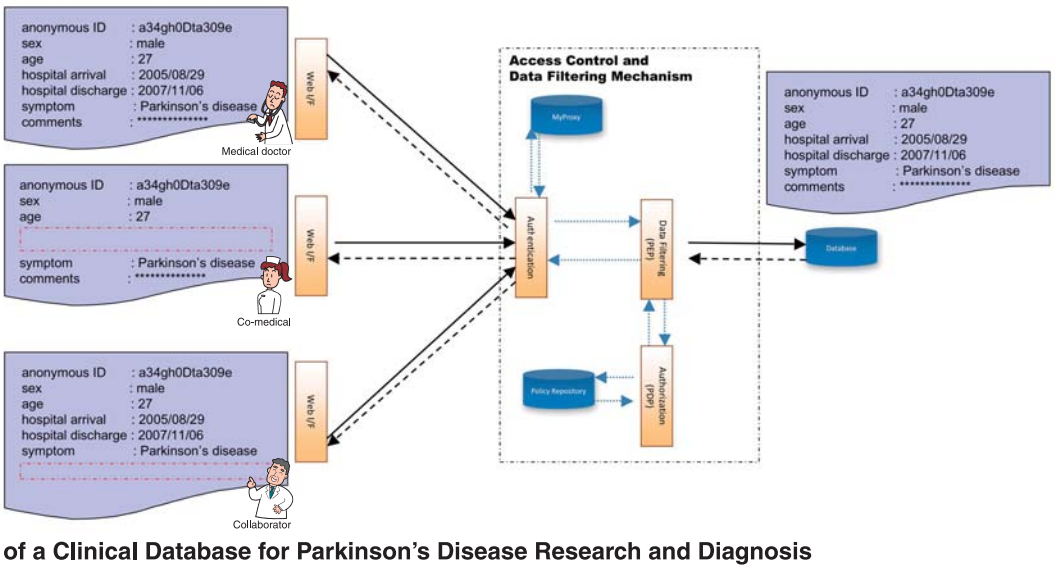

Fig.3: Architecture of a Clinical Database for Parkinson's Disease Research and Diagnosis

The clinical data pertaining to Parkinson's disease is filtered on an XML element level based on the accessing users' role, i.e., medical doctor, co-medical, and/or collaborator and is then delivered to the users. The clinical data is written in Medical Markup Language (MML), which conforms to Health Level 7 (HL7).

Contact : Susumu Date, Ph.D
E-mail : date@ime.cmc.osaka-u.ac.jp