Semantic Based Policy Management for Cloud Computing

Hassan Takabi
hatakabi@sis.pitt.edu

Joint work James Joshi

12-07-2011
Access Control in Cloud

• No single authorization mechanism
• No single policy language
• No single management tool
• Users must use diverse access control solutions
• Composed in incompatible languages
• Maintained separately at every cloud service provider
Access Control in Cloud

- Authorization mechanisms are bound to providers
- No unified policy management system
- No unified policy management tool
- Policies are heterogeneous
• Design an integrated AC system
  – can be used across services from different providers.

• Ideal access control scheme
  – must be able to work with all types of content regardless of where they are stored.
  – Users should not have to manage many copies of their data
  – they should be able to manage access to their data and resources from a central location.
The Unified Framework

Authorization GUI

Global Knowledge Base

Conflict Resolution

Policy Association

Global Policy Base

Authorization API

Global Ontology

Semantic Based Policy Management Server

Cloud Service Providers

Provider Authorization API

Semantic Based PDP

Local Knowledge Base

Local Policy Base

Local Ontology

PEP

LERSAIS @ School of Information Science
The Implementation Architecture

Authorization GUI (WebProtege)

Global Knowledge Base
- Protégé-OWL
  - OWL Files
- SWRLTab
  - SWRL Rules

RESTful Service

RESTful Methods

RESTful Client

Local Knowledge Base
- Protégé-OWL
  - OWL Files
- SWRLTab
  - SWRL Rules

Protege-OWL Reasoner API

Jena

Pellet

Semantic Based Policy Management Server

Cloud Service Providers

LERSAIS @ School of Information Science
Advantages

• Access policy specification is externalized.
• Users use a unified policy management tool.
• Users have a consolidated view
• If resources moved from one application to another, no new policy needed
• Overcomes some limitations of the existing access control systems
Question?