An Approach to Managing Policy Heterogeneity in Cloud Computing Environments

Hassan Takabi and James Joshi {hatakabi, jjoshi}@sis.pitt.edu, LERSAIS, University of Pittsburgh

Policy Management in Cloud

Motivation
Centralized policy management
- Better view of access policies applied to resources
- Allows users to centralize management of access control policies
- Find errors or inconsistencies

Case Study
- We developed a unified framework to accommodate policy management in one central place.
- *Amazon S3, DropBox, LinkedIn, Twitter, Flickr*

Limitations of Existing Policy Management Systems
- **Authorization mechanisms are bound to service providers**
- **There is no unified policy management system**
- **There is no unified policy management tool**
- **Access control policies are not interoperable**
- **Access control policies are heterogeneous**

Our Proposed Solution
Semantic Web
- We use combination of OWL 2 and SWRL
- High expressiveness
- Reasoning
- Scalable reasoning without sacrificing too much expressive power
- Separation between domain description and policy description
- Heterogeneity management and interoperability

Implementation

Implementation Architecture
- Java-based
- SBPMS & CSPs
- The *authorization API* and the *provider authorization API* are published through RESTful Web service technology
- A RESTful Web service is implemented in the SBPMS side and the CSPs are implemented as RESTful clients.
- Authentication of the provider and server is done using Oauth
- We use Protégé-OWL
- SWRLTab
- In order to reason, we use Jena and Pellet
- Authorization GUI: WebProtege
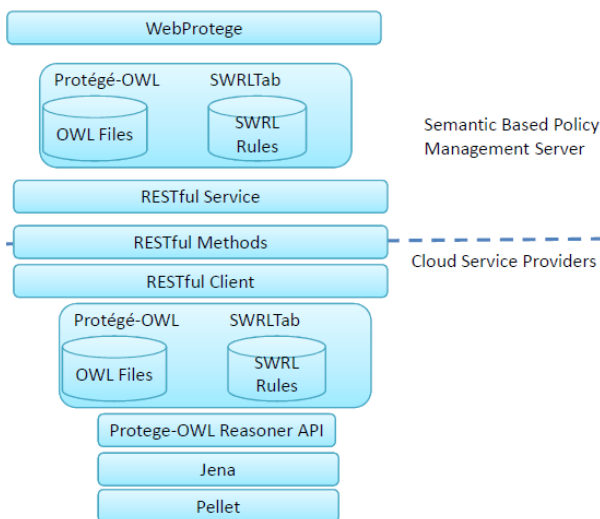
The Cloud Based Policy Management Framework

Cloud Service Provider (CSP)
- Local Ontology
- Local Policy Base
- PEP
- Semantic based PDP
- Provider authorization API

Semantic Based Policy Management Service (SBPMS)
- Global Ontology
- Global Policy Base
- Provides authorization services and interfaces for cloud users
- Detects and resolves possible conflicts among access policies
- Separates the policies related to each cloud service provider
- Exports them into the associated CSP via the provider authorization API
- Authorization GUI
- Access Request Processing
- The Reasoning Process
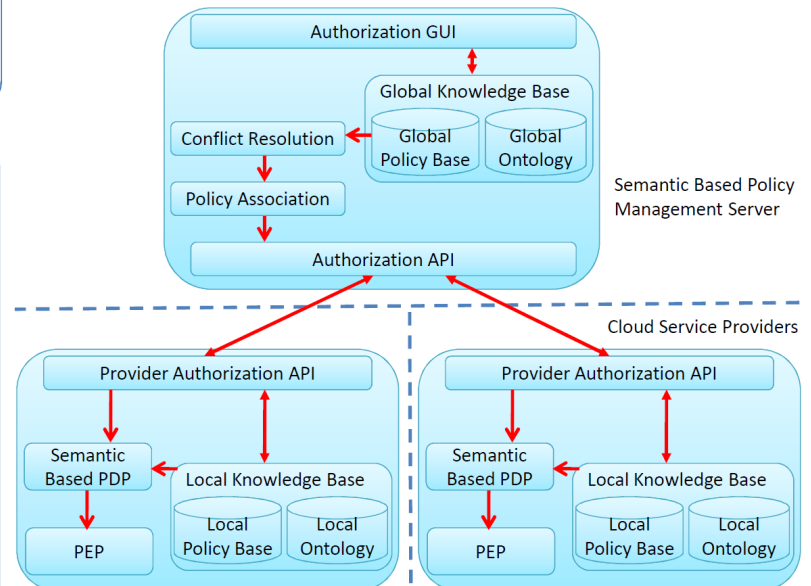
Conclusion & Future Work

Conclusion
- Lessons we learned from a case study implementation
- Limitations of existing approaches
- Developed Semantic based policy management framework
- Proof of concept implementation
- Performance Evaluation

Future Work
- Performance of reasoning process
- Design a usable GUI
- Perform user studies

Publication
Policy Management as a Service: An Approach to Manage Policy Heterogeneity in Cloud Computing Environments, In Proc. 45th HICSS, January 2012.
Semantic Based Policy Management for Cloud Computing Environments, International Journal of Cloud Computing (To Appear)