Outline

- Overview of Cloud
- Security Challenges in Cloud
- Motivation
- Use case scenario
- Semantic Based Policy Specification
- Semantic Based Policy Management Framework
- Conclusion & Future Work
Overview of Cloud and its features

● 5 Key Characteristics
  – On-demand self-service, ubiquitous network access, location independent recourse pooling, rapid elasticity, measured services

● 3 delivery models
  – IaaS, PaaS, SaaS

● Deployment models
  – Public cloud, private cloud, community cloud, hybrid cloud
Security Implications of Cloud Features

- Outsourcing
- Extensibility and Shared Responsibility
- Virtualization
- Multi-tenancy
- Service Level Agreement
- Heterogeneity
Security Challenges in Cloud

- Authentication and Identity Management
- Access Control
- Policy Integration
- Service Management
- Trust Management
Motivation

- No single authorization/policy language
- Each CSP employs its own access
- Authorization is bound to CSP
- Policies composed in incompatible languages
- CSPs don’t understand each other
- Users must use diverse AC solutions
Challenge

- Design an integrated access control system
  - work with all types of content
  - regardless of where they are stored
  - Manage from a central location.
Use Case Scenarios

- **Individual**
  - Alice a PhD student
  - Dropbox, Google Docs, Amazon S3, Mint

- **Small and Medium Businesses**
  - IaaS: Amazon S3 and FlexiScale
  - PaaS: Google App Engine and LoadStorm
  - SaaS: Zoho, Zuora, Workday, Salesforce, …

- **Collaboration & interoperation is impossible**
Use Case Scenario (Cont.)
Use Case Scenario (Cont.)
Use Case Scenario (Cont.)
Limitations

- Application centric vs. user centric
- Unified policy management system
- Heterogeneity and interoperation
- Privacy preservation
Policy Management Framework

- Cloud-based framework that efficiently delivers policy management services
- Built on the concept of centrally expressing user’s security requirements
- Manage user’s resources scattered across the Cloud
Architecture: Unified Policy Management Framework
PMaaS

- capabilities provided to the customers to manage policies for services and products running on a cloud infrastructure which are accessible through usable interfaces.
- customers do not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application capabilities.
PMaaS: High Level View

- Cloud user
- PMSP
- CSP
- requester
Policy Management as a Service (PMaaS) Framework

[Diagram showing various components of the PMaaS framework, including Policy Editor, Policy Server, Cloud Service Provider, and Requester.]
Policy Management Service Provider (PMSP)

- The Policy Editor
  - policy administration point (PAP)
- The Policy Server
  - policy information point (PIP)
Policy Management Process

- Registering cloud service providers
- resource discovery
- specifying policies
- exporting policies
The Framework Deployment

- PMSP should be able to exchange data with the CSPs.
- PMSP should generate policies in a format that the cloud service provider understands.
- Changes
  - Push strategy
  - Pull strategy
PMaaS: Discussion

- Policy specification is external to CSP
- Unified policy management system
- Consolidated view of the access policies applied to their resources.
- Moving resources from one CSP to another
- Extend functionalities of the existing system
- Concerns
Semantic Based Policy Specification

- Semantic Web and Policy Management
- provide a common understandable semantic basis for policy specification
- semantic based policy specification language (SBPSL)
- Use OWL to model this specification language
Semantic Web and Policy Management

- combination of OWL 2 RL and SWRL with DL-Safe restriction,
  - high expressiveness
  - reasoning using rule-based engines which offer good performance
  - scalable reasoning without sacrificing too much expressive power
  - heterogeneity management and interoperability
  - separation between domain description and policy description
Semantic Based Policy Management Framework
Ontologies

- Subject rdfs:subClassOf owl:Thing
- Role rdfs:subClassOf owl:Thing
- Object rdfs:subClassOf owl:Thing
- Action rdfs:subClassOf owl:Thing
- Attribute rdfs:subClassOf owl:Thing
- Provider rdfs:subClassOf owl:Thing
- Service rdfs:subClassOf owl:Thing
Ontologies

- Subject Ontology
- Object Ontology
- Action Ontology
- Provider Ontology
- Service Ontology
- Attribute Ontology
Subject Ontology

- **Subject**: a user, a user group, a role, a process, a service and so on.
- modeled as an OWL class `Subject`.
- The instances of this class represent the subjects on which the policies are defined.
- The object property and data property of OWL are used to describe attributes of a subject with `hasSubjectAttribute` and `hasSubjectDataAttribute` respectively.
Rule and Rule Set

- [Subject, Object, Action]
- [Provider, Subject, Object, Action, Service]
SBPSL
Knowledge Management

- Authorization knowledge management
- Access request processing
Reasoning & Conflict Analysis

● The Reasoning Process
  – Inference
  – Validation
  – Querying the ontology

● Policy Conflict
  – when two disjoint properties appear simultaneously
  – unauthorizedSubject
Implementation Architecture
Performance evaluation
Performance evaluation
Performance evaluation
Cloud Interoperation
The Architecture

- cloud service provider
  - PAP
  - PEP
- semantic based policy management service
  - semantic based PDP
Access Request Processing
Conclusion and Future Work

- The access control issues particularly heterogeneity and interoperation
- proposed a semantic based policy management framework
- introduced semantic based policy specification language
- Privacy Preservation
Questions?