Authorization Federation in Multi-Tenant Multi-Cloud IaaS

Navid Pustchi

Advisor: Prof. Ravi Sandhu
“Moving” to Cloud

World-Leading Research with Real-World Impact!
Why Collaboration?

- Large Organization with multiple tenants
- Distinct Organizations’ Collaborative tasks

World-Leading Research with Real-World Impact!
Why Multi Cloud?

World-Leading Research with Real-World Impact!
Cloud Federation

- Collaboration of cloud service providers and identity providers in order to share their services and resources based on trust agreements.

Multi-Cloud

- Collaboration of multiple cloud service providers (public or private) within different administrative domains (Cloud and Domain) to provide complex services at specified service model (Infrastructure, Platform and Software).

---

**World-Leading Research with Real-World Impact!**
Multi Cloud Collaboration

Cloud Federation

- **Service (IaaS, PaaS, SaaS)**
  - Heterogeneous: Google account (Open ID 2.0) Heterogeneous within google.
  - Homogeneous: Eduroam federated network access.

- **Platform**
  - Heterogeneous: OpenStack federation with AWS.
  - Homogeneous: Keystone to Keystone federation.

- **Trust**
  - Circle-of-Trust: Alliance of institutions for sharing scientific data such as CERN.
  - Peer-to-Peer: Best Buy federating with Rackspace.

- **Coupling**
  - Identity Federation: SAML, OAuth, OpenID, SSO.
Problem Statement

Current access control models provided by cloud platforms are not sufficient to cultivate efficient peer-to-peer and circle-of-trust collaboration between tenants in a cloud or across multiple cloud platforms. Prior role-based and attribute-based access control models in distributed systems are not effectively applicable to cloud IaaS.

Thesis Statement

The problem of authorization federation in multi-tenant cloud IaaS can be partially solved by integrating multiple types of peer-to-peer and circle-of-trust relations between tenants in single-cloud and multi-cloud environments into role-based and attribute based models.
Scope of Contribution

Cloud Federation

- Service
  - SaaS
  - PaaS
  - IaaS

- Platform
  - Homogenous
  - Heterogeneous

- Trust
  - Circle-of-Trust
  - Peer-to-Peer

- Coupling
  - Authentication Federation
  - Authorization Federation
Scope of Contribution

Cloud Federation

Service
- SaaS
- PaaS
- IaaS

Platform
- Homogenous
- Heterogeneous

Trust
- Circle-of-Trust
- Peer-to-Peer

Coupling
- Authentication Federation
- Authorization Federation

World-Leading Research with Real-World Impact!
A collaboration group of clouds, relationships are established by a set of contracts defining obligations and access rights of participating clouds.

Member clouds have access to a set of shared services and resources.

Joining the circle of trust requires agreement of member clouds.
Collaboration of clouds, relationships established between each two participating clouds.

Clouds share resources and services upon trust relationship between trustor and trustee clouds.

Joining a new relationship requires establishing trust with other clouds.
Identity (Authentication) Federation:
- Authenticating users (services and applications) in a cloud service provider other than their registered identity provider based on trust between collaborating clouds.

Authorization Federation:
- Granting access to authenticated users by assigning roles in cloud service provider based on trust agreements between two clouds.

Authorization federation is dependent on identity federation to authenticate users.
Contribution

Infrastructure-as-a-Service

Multi-Tenant Multi-Cloud

- Peer-to-Peer
  - MT – RBAC

Multi-Tenant Cloud

- Circle-of-Trust
  - Heterogeneous
    - MT – RABACc

- Homogeneous
  - MT – RBACc

- Peer-to-Peer
  - MT – ABAC
Peer-to-Peer Trust

Initiation

Direction

Transitivity

Bilateral

Unilateral

Bidirectional

Unidirectional

Transitive

Non-transitive

World-Leading Research with Real-World Impact!
Administrative Realms

Service Ownership → Clouds

Domain Ownership → Domains

Role Ownership → Clouds

Project Ownership → Users

User Assignment → Projects

Service Assignment → Projects

Project-Role-Pair (PRP) → Projects

Service Instance → Services

Service Insantiation → Services

Cloud Trust

Domain Trust
Two trust scopes based on administrative realms in cloud:

- **Cross Cloud Trust**
  - Sharing cloud infrastructure resources, such as services.

- **Cross Domain Trust**
  - Sharing domain resources such as projects.
Type $\alpha$:

- If $\text{domain}_A \leq_\alpha \text{domain}_B$, $A$ is authorized to assign $B$'s users to its resources. $A$ controls trust relation and inter-cloud assignments.

- For example, cloud $B$ acts as an identity provider to access $A$’s resources.

![Diagram showing domain trust relationships](image-url)
Type $\beta$:

- If $\text{domain}_A \preceq_\beta \text{domain}_B$, $B$ is authorized to assign $A$'s users to its resources. $A$ controls trust relation and $B$ controls inter-cloud assignments.

- When access to shared resources is controlled by resource owner.
Domain Trust

➢ **Type — $\gamma$:**
  
  - If $\text{domain}_A \leq_{\gamma} \text{domain}_B$, $B$ is authorized to assign its users to $A$'s resources. $A$ controls trust relation and $B$ controls inter-cloud assignments.
  
  - Sharing resources with group of clouds.

![Diagram of domain trust relationship](image-url)
Type — $\delta$:

- If $\text{domain}_A \preceq_\delta \text{domain}_B$, B is authorized to assign A's users to A's resources. A controls trust relation and B controls intra-cloud assignments.

- Administration federation within an organization with multiple clouds.
Attributes are *name:*value pairs
- Represents user and resource properties

Associated with
- Users
- Objects
- Tenants
- Contexts

Converted to rights by authorization policies
- In-time
- Entity attributes
- Set of actions
Why Another Model

➢ ABAC
  ❖ RBAC shortcomings needs custom extension
    ▪ For example real time environmental parameters.
  ❖ ABAC is more flexible
    ▪ Accommodate environmental parameters.

➢ MT-ABAC
  ❖ Multi-tenancy
  ❖ Collaboration consistent with trust
ABAC_0 Model Structure
MT — $ABAC_0$ Model Structure

Association  Access Decision  Many-to-one  Many-to-many
           atomic-valued function  set-valued function
Tenant-trust type-$\alpha$

- If $T_A \leq \alpha T_B$, tenant $T_A$ is authorized to assign values for $T_A$'s user attributes to tenant $T_B$'s users. Tenant $T_A$ controls tenant-trust existence and cross-tenant attribute assignments.
Tenant-trust type-\( \beta \)

- If \( T_A \preceq_{\beta} T_B \), tenant \( T_B \) is authorized to assign values for \( T_B \)'s user attributes to tenant \( T_A \)'s users. Tenant \( T_A \) controls tenant-trust existence while \( T_B \) controls cross-tenant attribute assignments.
Tenant-trust type-γ

- If $T_A \leq_{γ} T_B$, tenant $T_B$ is authorized to assign values for $T_A$'s user attributes to tenant $T_B$'s users. Tenant $T_A$ controls tenant-trust existence while $T_B$ controls cross-tenant attribute assignments.
P2P vs. CoT

Acme Univ. Cloud

- User: Mark, David
  - Role: Prof., Post Doc.
  - Project: Condense Matter

Zenith Univ. Cloud

- User: Andrew, John, Bob
  - Role: Admin, Post Doc., Prof.
  - Project: Compound, Molecular, Materials, Nuclear

Public Cloud


ACME Multi-Tenant Circle-of-Trust

World-Leading Research with Real-World Impact!
Trust in Circle-of-trust

- **Entity Coupling**
  - Heterogeneous
  - Homogenous
- **Initiation**
  - Unilateral
  - Multilateral
- **Direction**
  - Unidirectional
  - Bidirectional
- **Transitivity**
  - Non-Transitive
  - Transitive
Four trust types:

- **Type – $\varepsilon$:**
  - If $T_A \preceq_\varepsilon T_B$, then tenant $T_A$ is authorized to assign its users to $T_B$’s roles. Tenant $T_A$ controls user assignments.

- **Type – $\zeta$:**
  - If $T_A \preceq_\zeta T_B$, then tenant $T_B$ is authorized to assign $T_A$’s users to its roles. Tenant $T_B$ controls user assignments.
Many-to-one relation  Many-to-many relation
MT – RBAC\(_c\) Role Hierarchy

- **Public Role\(_{TB}1\)**
  - **Private Role\(_{TB}2\)**
  - **Private Role\(_{TB}4\)**
  - **Private Role\(_{TA}5\)**
  - **Private Role\(_{TA}7\)**
- **Public Role\(_{TA}3\)**
  - **Private Role\(_{TB}4\)**
  - **Private Role\(_{TA}5\)**
  - **Public Role\(_{TA}6\)**

*World-Leading Research with Real-World Impact!*
World-Leading Research with Real-World Impact!
Many-to-one relation

Many-to-many relation

Association

atomic-valued function

Many-to-one

Roles

U

UATT

TATT

uattOwner

T

oattOwner

OATT

RO

UO

UA

R_{priv}

R_{pub}

PRMS

OBS

OPS

RH

PA
Adding Identity federation to OpenStack cloud, multiple identity providers can federate their users to an OpenStack cloud.

1. Request for a service.
2. Determine user’s IdP.
5. IdP redirects user’s attributes.
6. User access to service is granted.

Keystone Mapping Engine

- Takes SAML assertion as input, and as output OpenStack Token.
- OpenStack cloud admin creates a set of *mapping rules* which determines how to map SAML attributes to groups and users.

![Diagram showing Keystone Mapping Engine](image)

- Identity Provider
- Mapping Engine
- Service Provider

**SAML Attributes:**
- Groups: IBM Regular Employees Canada, SWG Canada
- User: Allen

**Keystone Attributes:**
- Groups: Regular_Employees_Canada, SWG_Canada
- User: Allen

---

Keystone SAML Generator

- Takes as input: an OpenStack Token, and the service provider the user wants to use.
- Outputs a SAML Assertion that can be forwarded to the Service Provider.
- Assuming service provider has the Identity Provider created, the Private Cloud user should get a token that is valid at the Service Provider.

Keystone to Keystone Federation

1. Ask for SAML Assertion
2. Return SAML Assertion
3. Present SAML Assertion
4. Return a Keystone token that can be used on Public Cloud

A. Add public cloud as service provider
B. Add Private Cloud as Identity Provider

World-Leading Research with Real-World Impact!

Coarse-grained and fine-grained trust models in cloud.
- Multi-Tenant Cloud.
- Multi-Tenant Multi-Cloud.

Peer-to-Peer Policy
- Multi-cloud role-based model.
- Multi-tenant attribute-based model.

Circle-of-Trust Policy
- Multi-tenant role-based access control model.
- Multi-tenant role-centric attribute-based access control model.

Implementation
- Single-cloud tenant trust.
- Federated-cloud tenant trust.