Authorization Federation in Multi-Tenant Multi-Cloud IaaS

Navid Pustchi

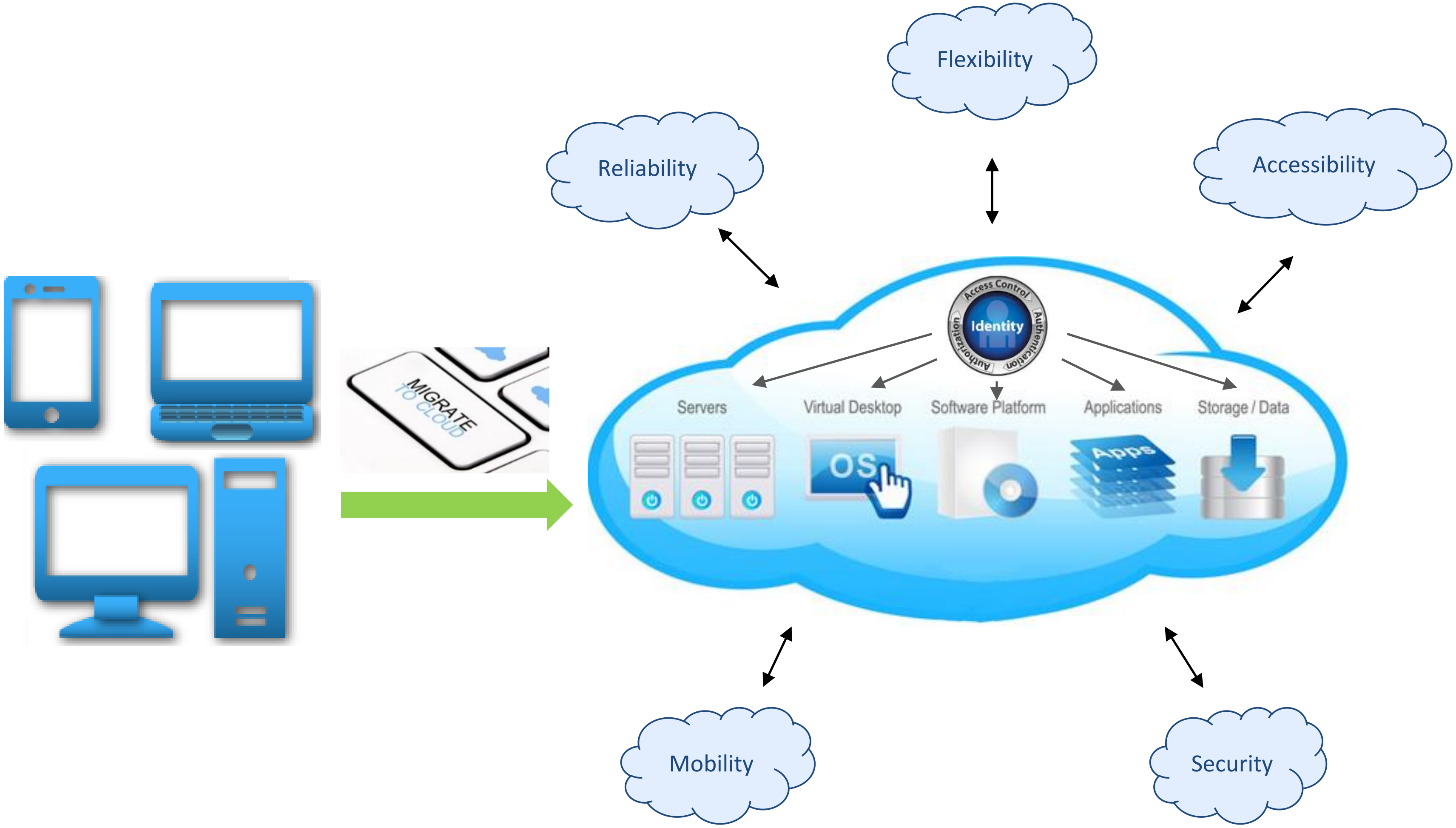
Dissertation Defense

Department of Computer Science

University of Texas San Antonio

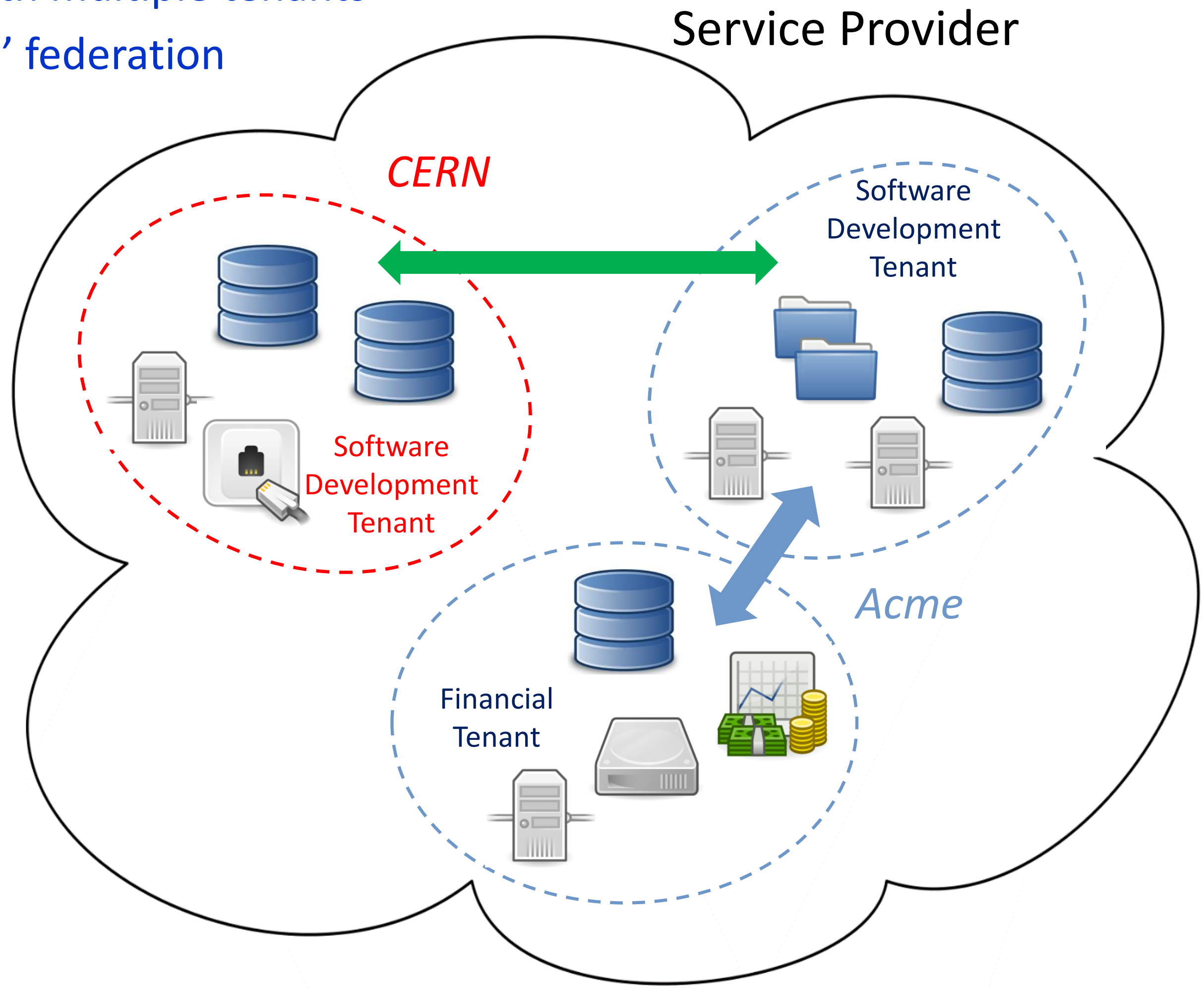
Advisor: Dr. Ravi Sandhu
Co-Advisor: Dr. Ram Krishnan
Dr. Gregory B. White
Dr. Matthew Gibson
Dr. Palden Lama

“Moving” to Cloud



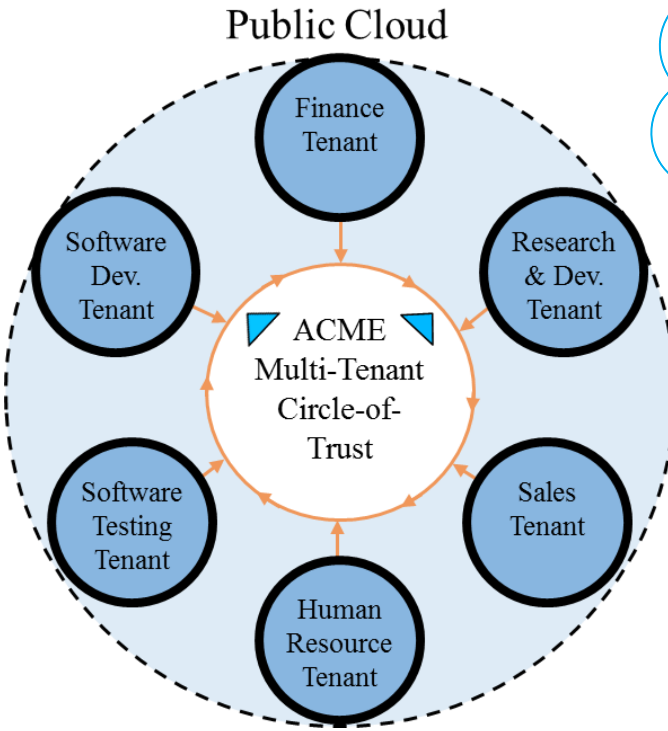
Why Federation ?

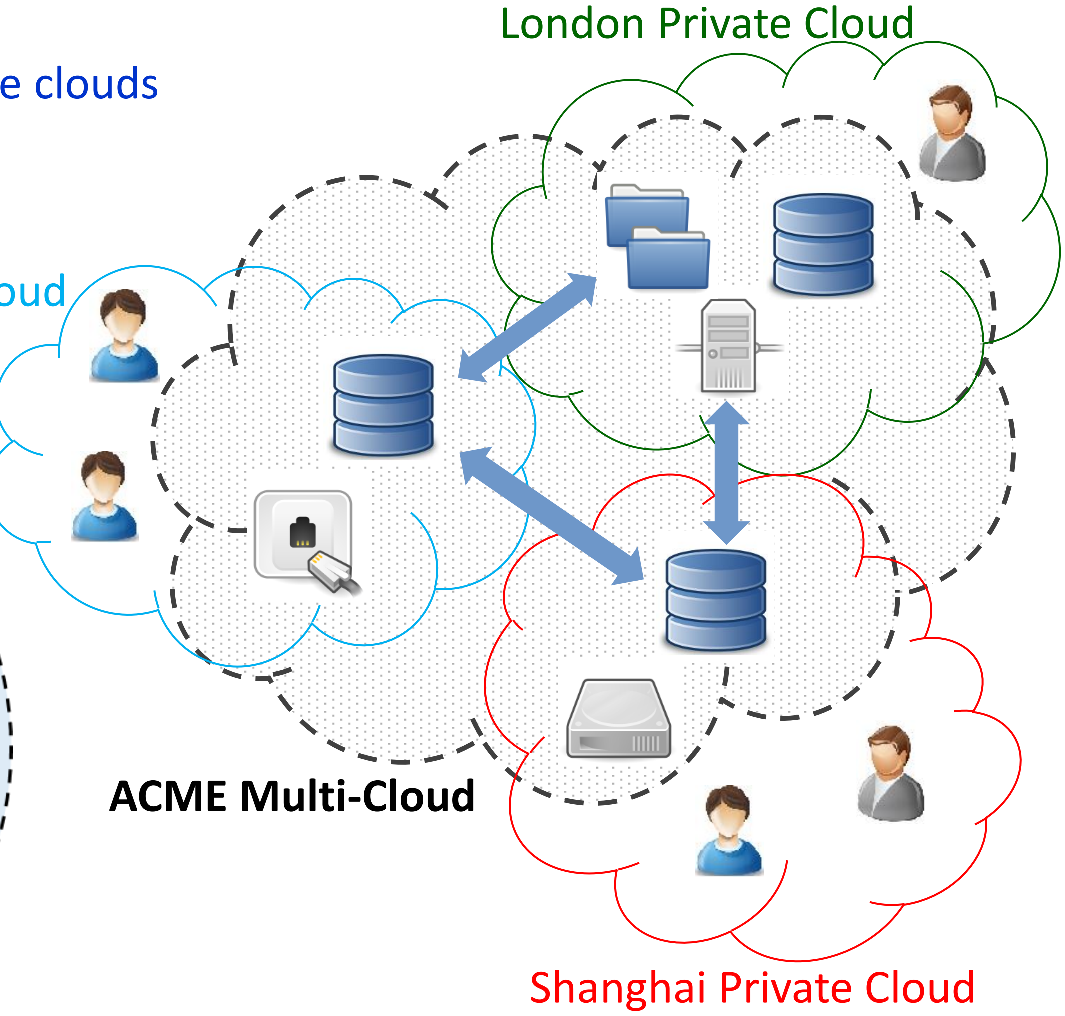
- Large organization with multiple tenants
- Distinct organizations' federation



Why Multi-Cloud?

- Federation consist of multiple clouds or multiple tenants.





Problem & Thesis Statement

- Problem Statement

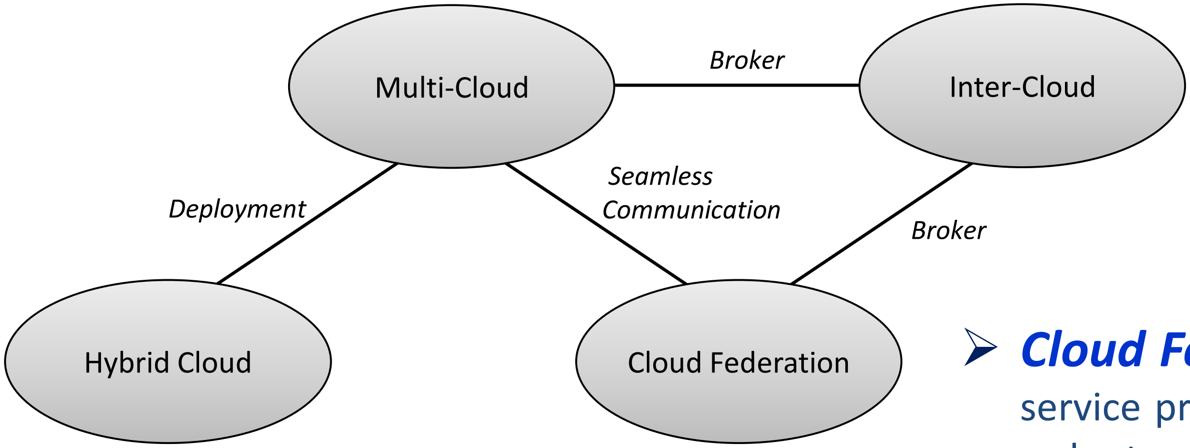
Current access control models provided by cloud platforms are not sufficient to cultivate effective peer-to-peer and circle-of-trust federation between tenants in a cloud or across multiple cloud platforms. Prior role-based and attribute-based access control models in distributed systems are not effectively 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 cloud and multi-cloud environments into role-based and attribute-based access control models.

What is Cloud Federation?

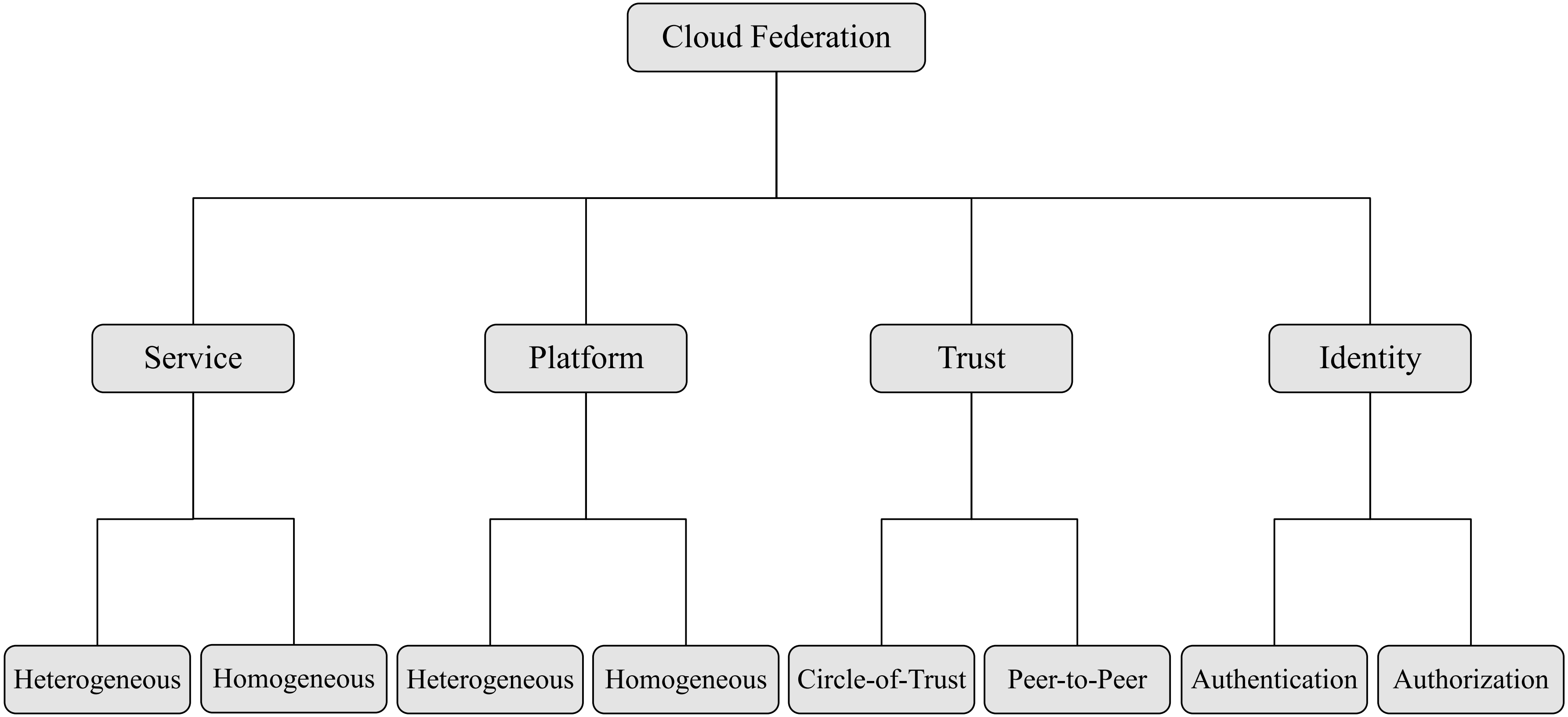
- ***Multi-Cloud*****,** Federation of multiple cloud service providers (public or private) within different administrative domains (Cloud and Domain) to provide complex services at specified service model (Infrastructure, Platform and Software).



- ***Cloud Federation*****,** Federation of cloud service providers and identity providers in order to share their services and resources based on trust agreements.

- ***Hybrid Cloud*****, "**A composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities. **"**

Federation in Cloud

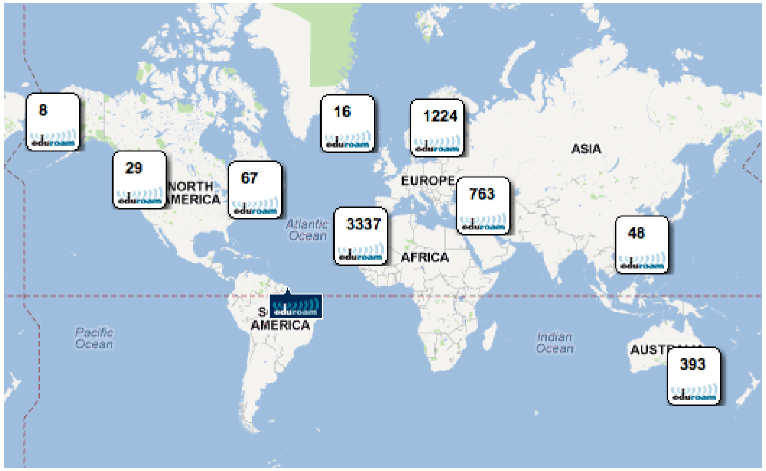


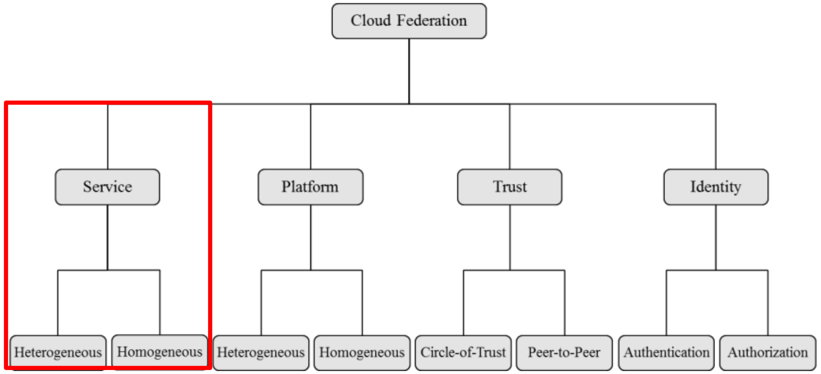
Service in Cloud Federation

- **_Service_**
  - Heterogeneous
    - Google account (Open ID 2.0) Heterogeneous within google.
  - Homogeneous
    - Eduroam federated network access.
    - OpenStack Federation.

Heterogeneous Service Federation

Homogeneous Service Federation

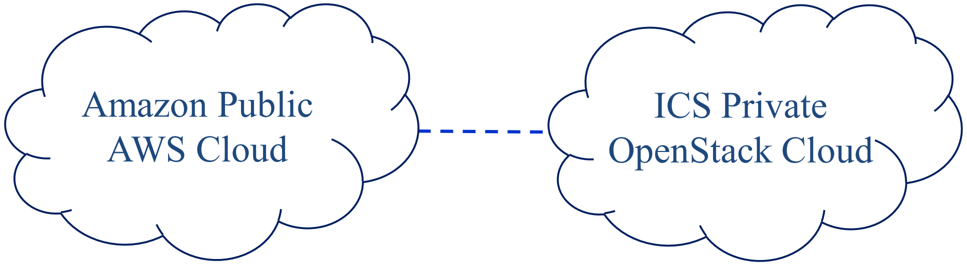




World-Leading Research with Real-World Impact!

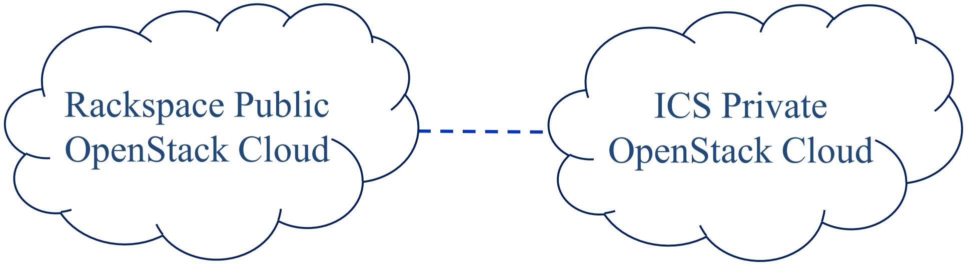
Platform in Cloud Federation

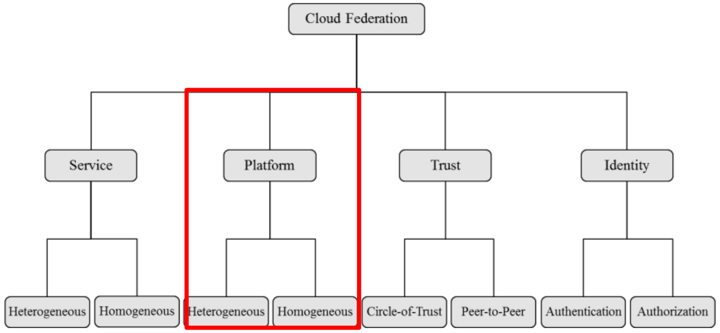
Heterogeneous Platform Federation



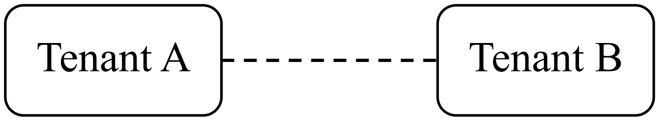
- ***Platform***
  - Heterogeneous
    - OpenStack federation with AWS.
  - Homogeneous
    - Keystone to Keystone federation.

Homogeneous Platform Federation



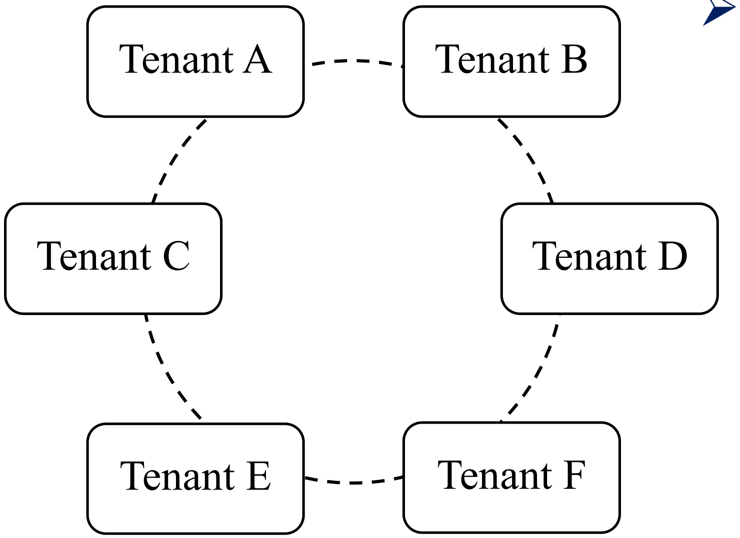


Peer-to-Peer vs Circle-of-Trust



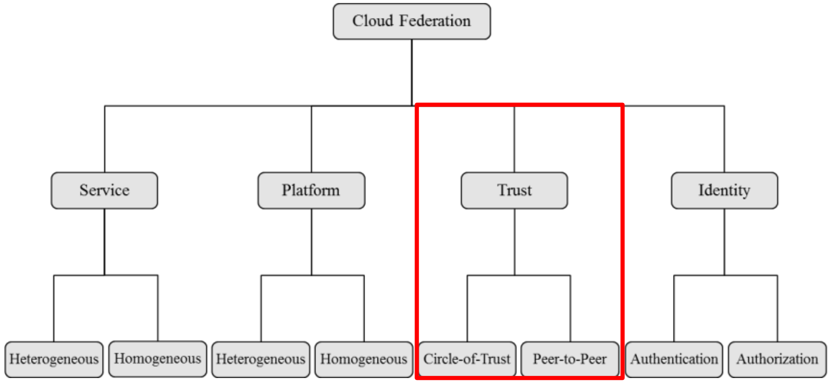
Peer-to-Peer Federation

- Trust between a pair of tenants.
- Specific set of actions between tenants.
- Only trusted tenant.



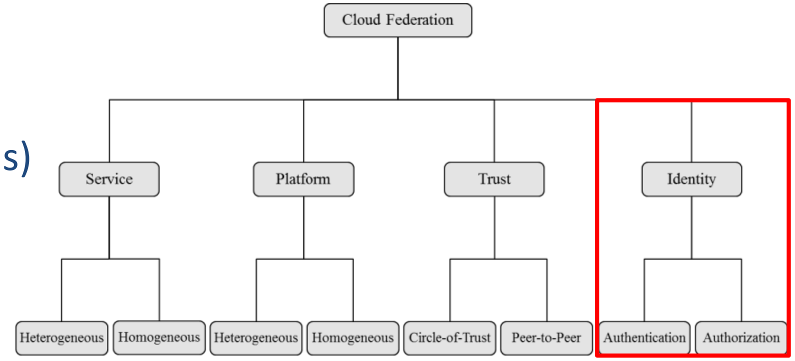
Circle-of-Trust Federation

- Trust between a group of tenants.
- Similar policies and rules.
- Acceptance of all tenants in the circle.

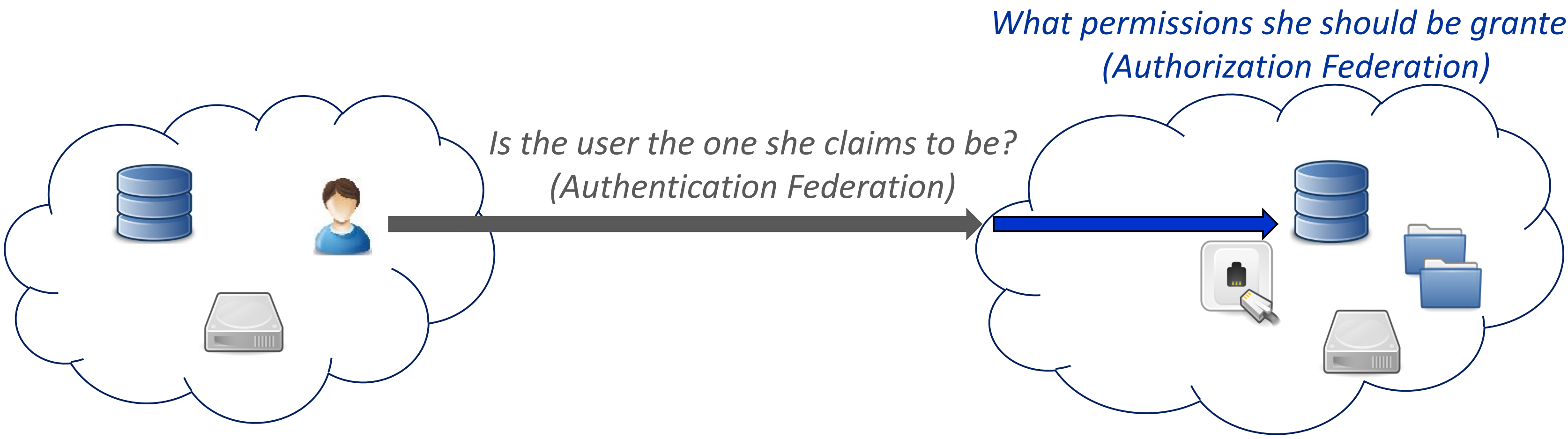


Authentication vs Authorization

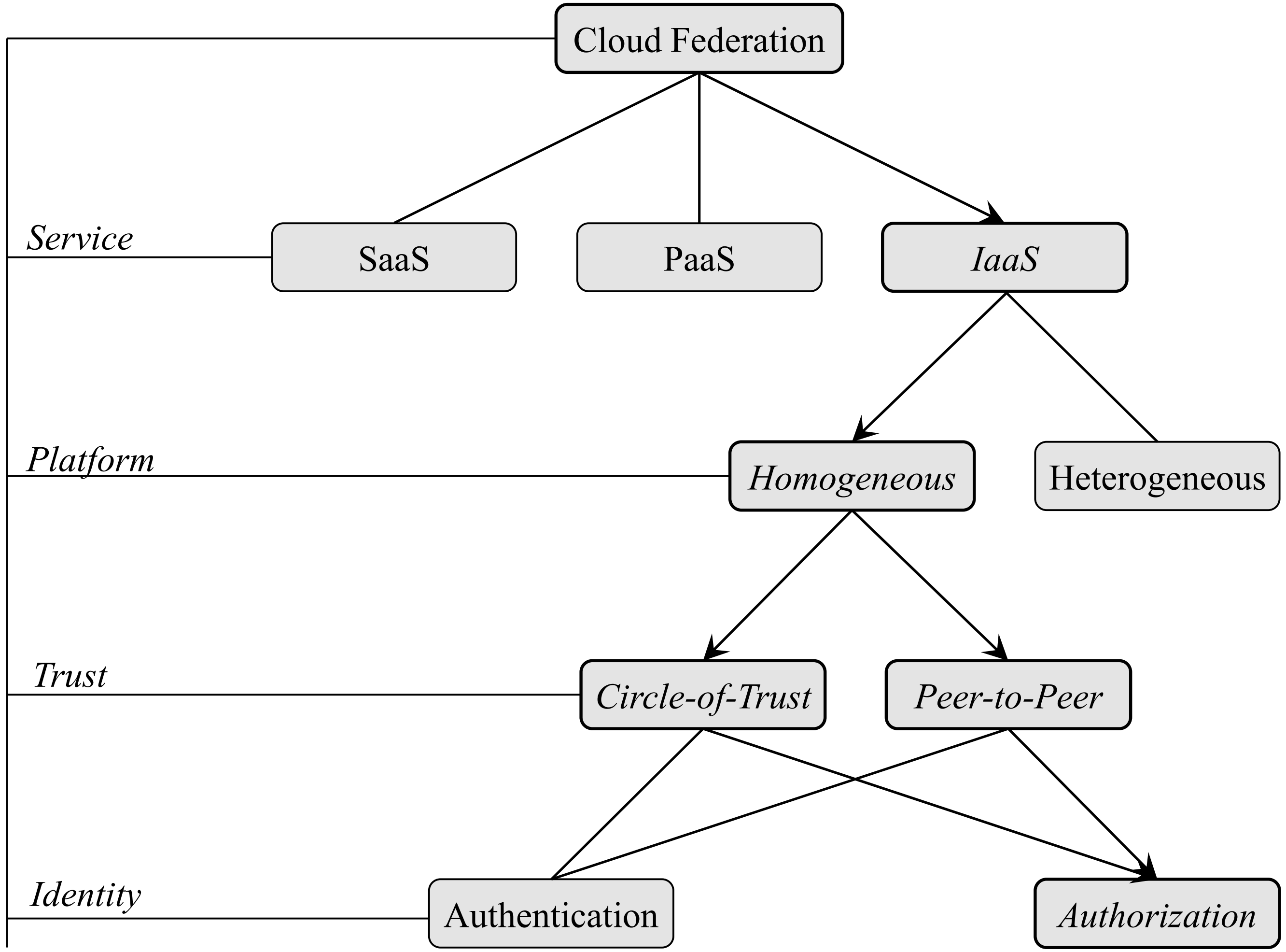
- Authentication Federation
  - Authenticating users (services and applications) in a cloud service provider other than their registered identity provider.
  - SAML, OAuth, OpenID, SSO.



- Authorization Federation
  - Determining federated users’ permissions to access federated resources and services.
  - SAML, OAuth.
  - Authorization federation is dependent on authenticated users.

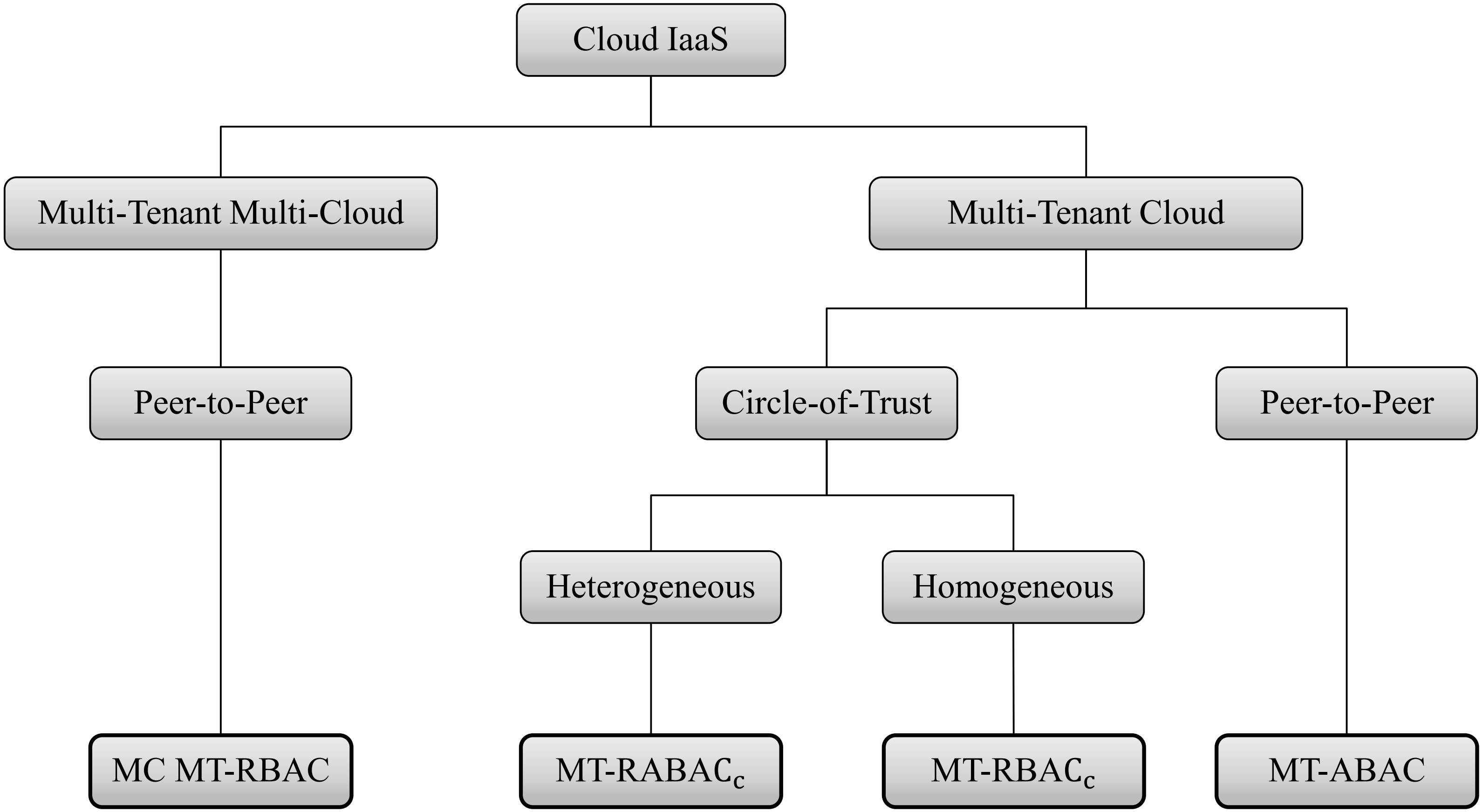

What permissions she should be granted?
(Authorization Federation)
Is the user the one she claims to be?
(Authentication Federation)

Scope of Contribution



World-Leading Research with Real-World Impact!

Scope of Contributed Models



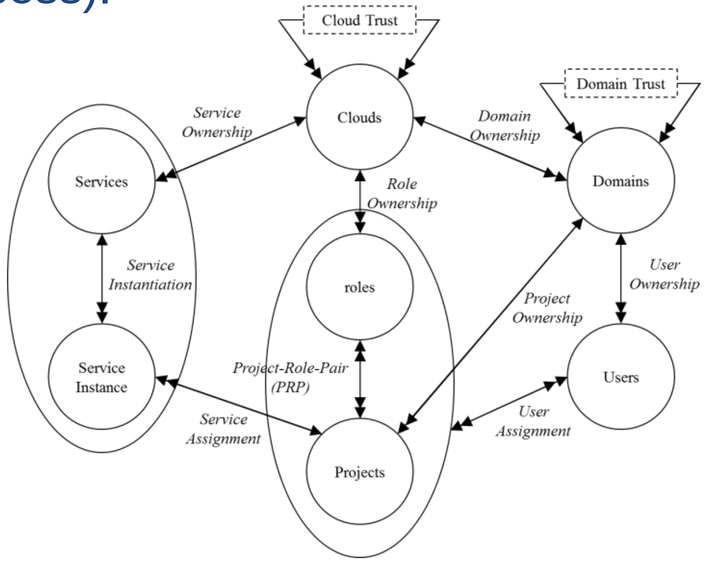
Administrative Domains

Cloud Domain

- Administration of services (compute, storage, network, and identity) and tenant domains.
- Cloud bursting.

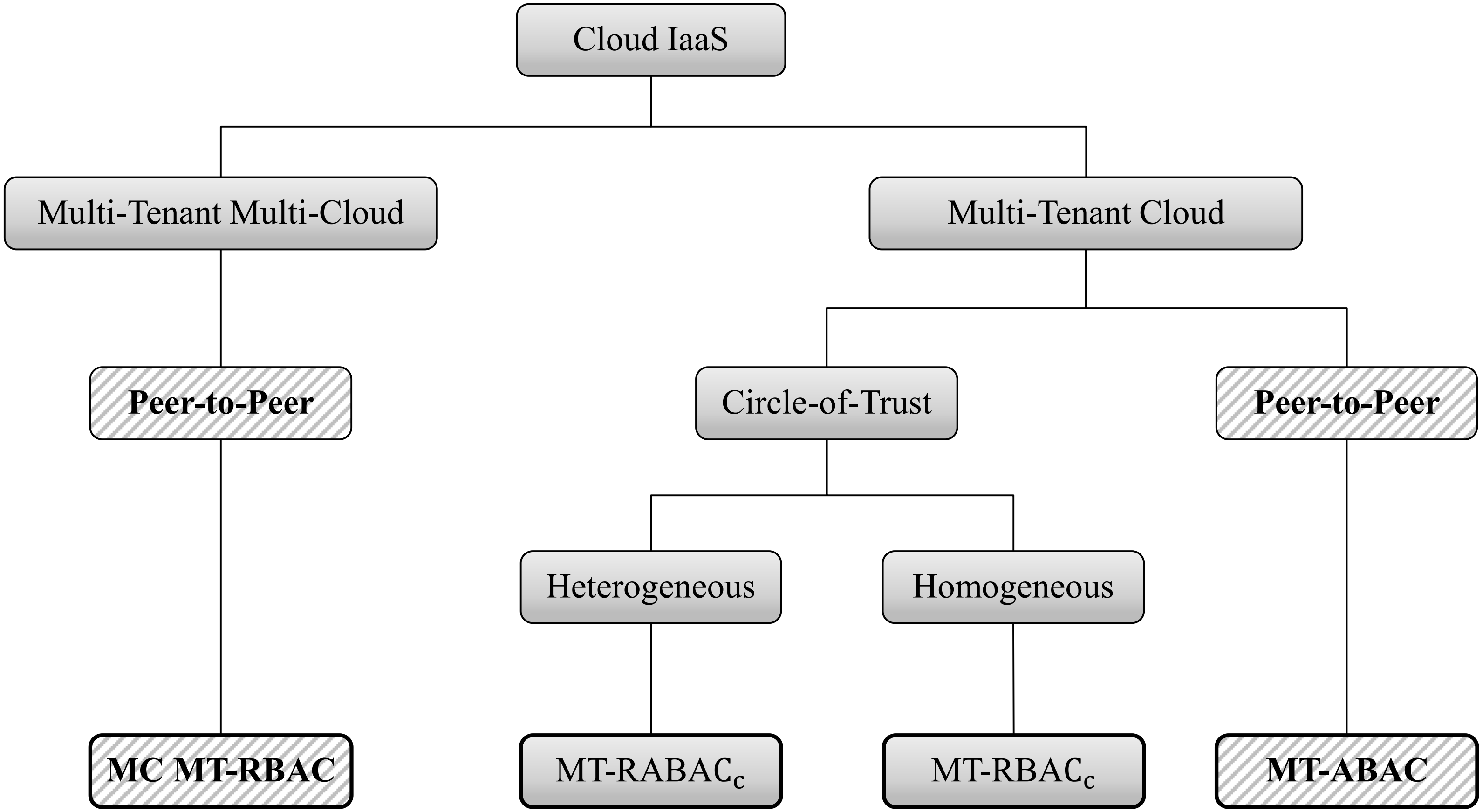
Tenant Domain

- Administration of resources (users, groups and projects in OpenStack).
- Resource federation (cross-tenant access).

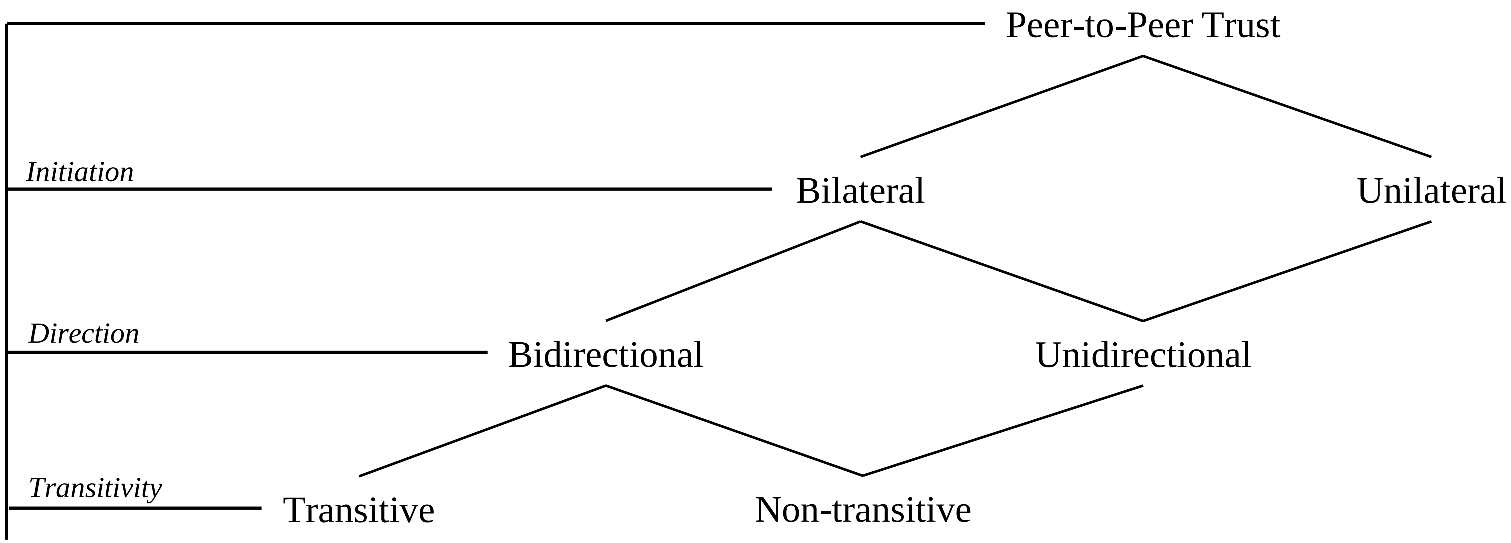


World-Leading Research with Real-World Impact!

Peer-to-Peer Federation Models



Peer-to-Peer Federation Trust



- **Tenant-Trust**
  - *Unilateral, Unidirectional, and Non-Transitive.*

P2P Trust Types Use Case

- **UTSA and BoA contract**
  - BoA employees can get UTSA courses at discounted rates.
  - UTSA students can get student accounts at BoA.
  - BoA can select courses for its employee students at UTSA.

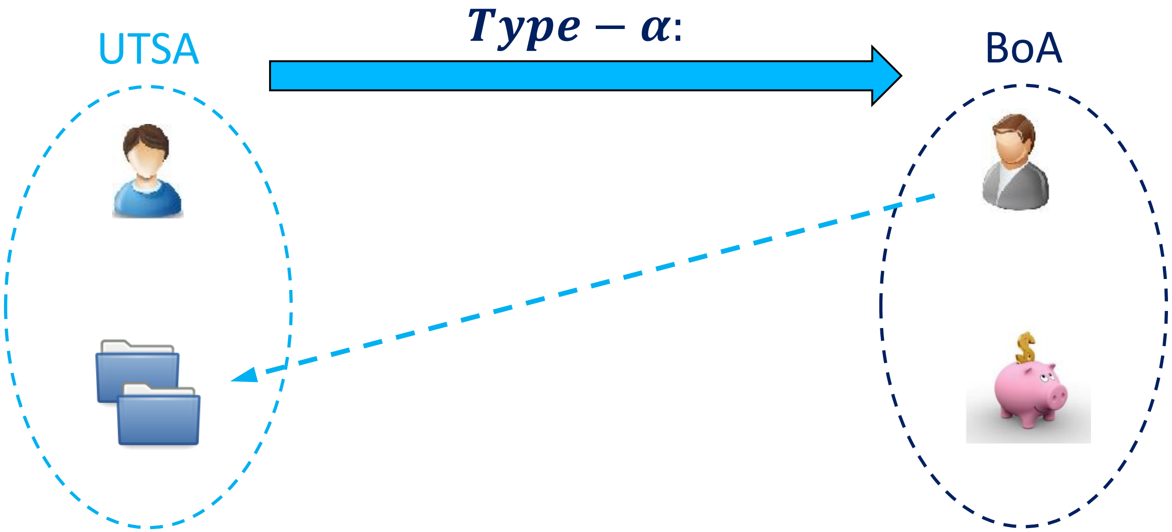
UTSA

BoA

P2P Trust Types Use Case

UTSA and BoA contract

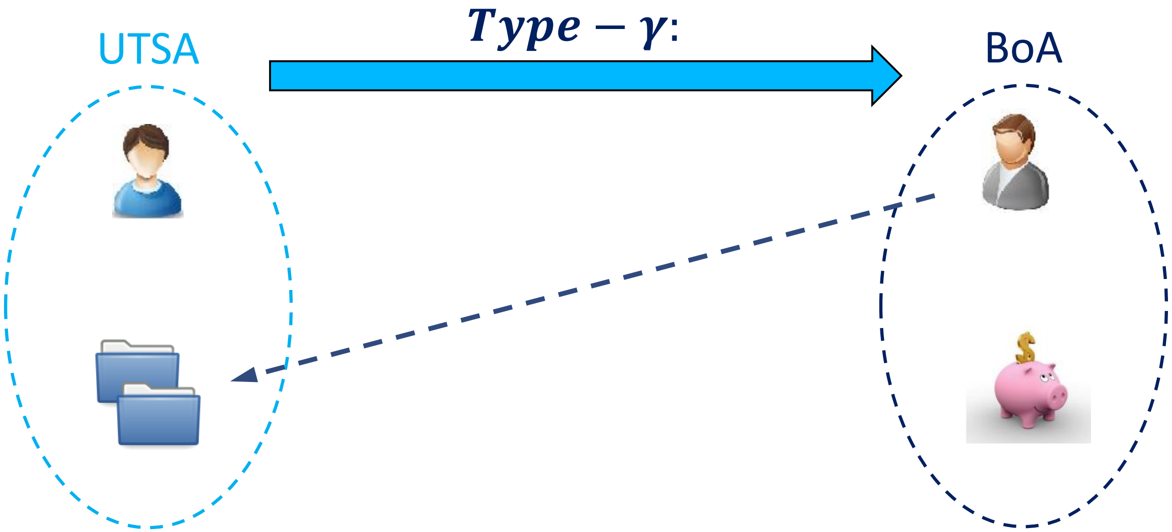
- BoA employees can get UTSA courses at discounted rates.
  - UTSA can assign BoA employees to courses.
- UTSA students can get student accounts at BoA.
- BoA can select courses for its employee students at UTSA.



P2P Trust Types Use Case

UTSA and BoA contract

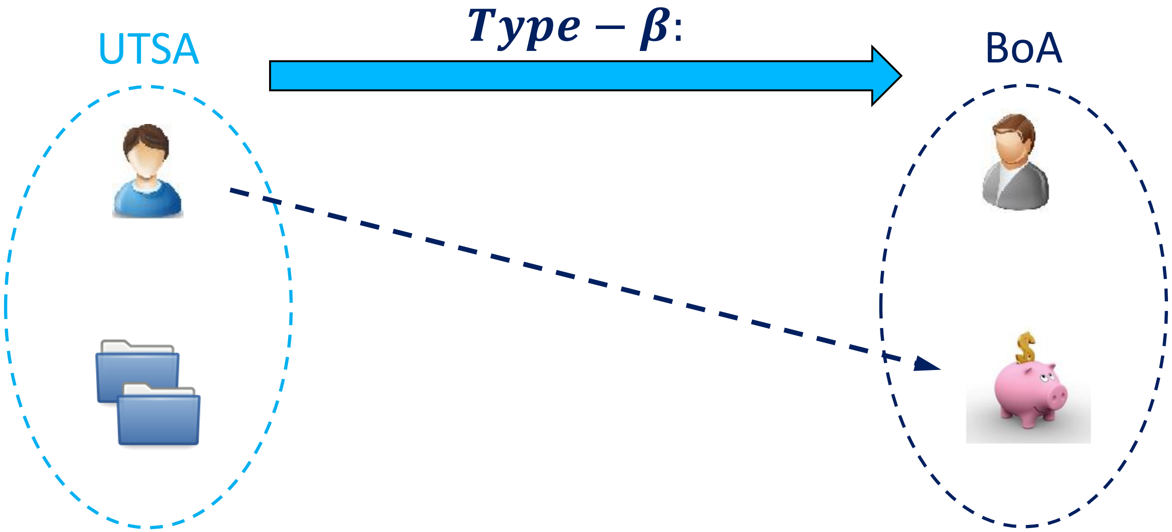
- BoA employees can get UTSA courses at discounted rates.
  - BoA can assign employees to UTSA courses.
- UTSA students can get student accounts at BoA.
- BoA can select courses for its employee students at UTSA.



P2P Trust Types Use Case

UTSA and BoA contract

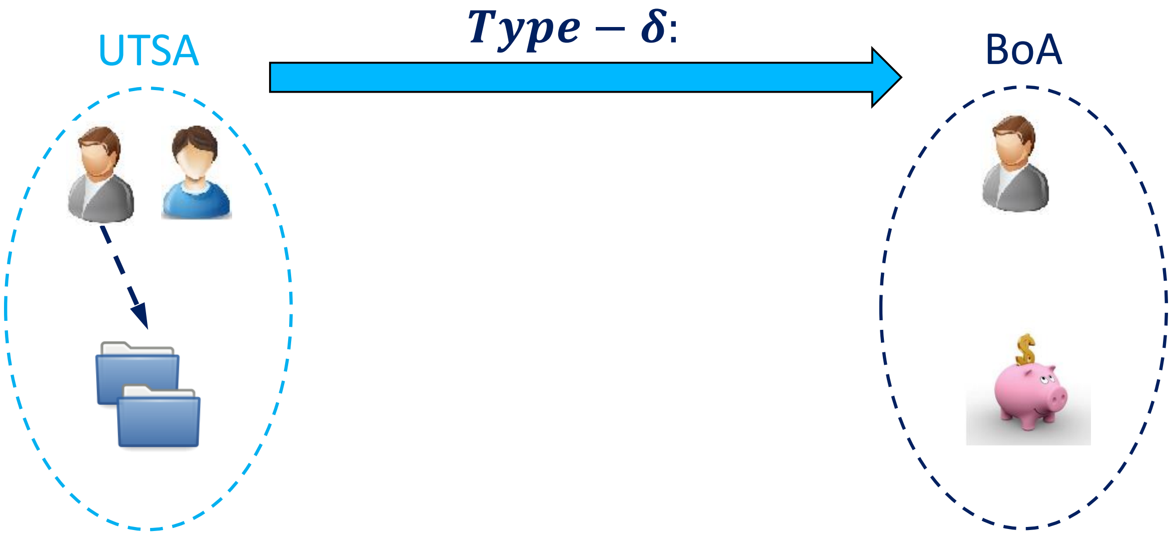
- BoA employees can get UTSA courses at discounted rates.
- UTSA students can get student accounts at BoA.
- BoA can select courses for its employee students at UTSA.



P2P Trust Types Use Case

UTSA and BoA contract

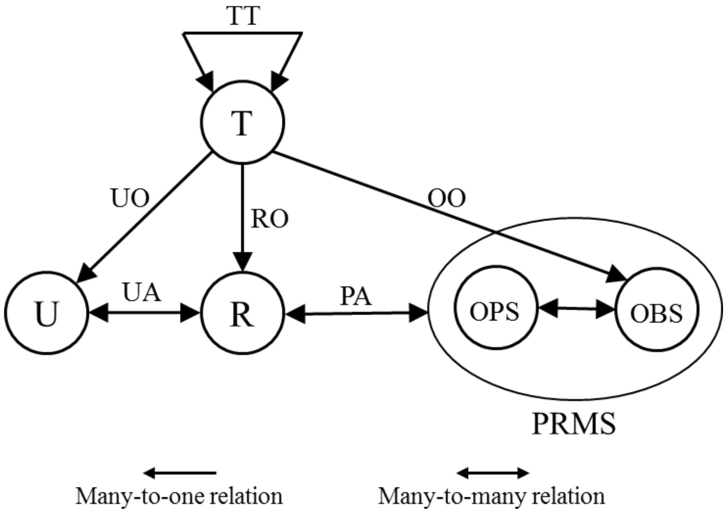
- BoA employees can get UTSA courses at discounted rates.
- UTSA students can get student accounts at BoA.
- BoA can select courses for its employee students at UTSA.



Multi-Cloud MT-RBAC

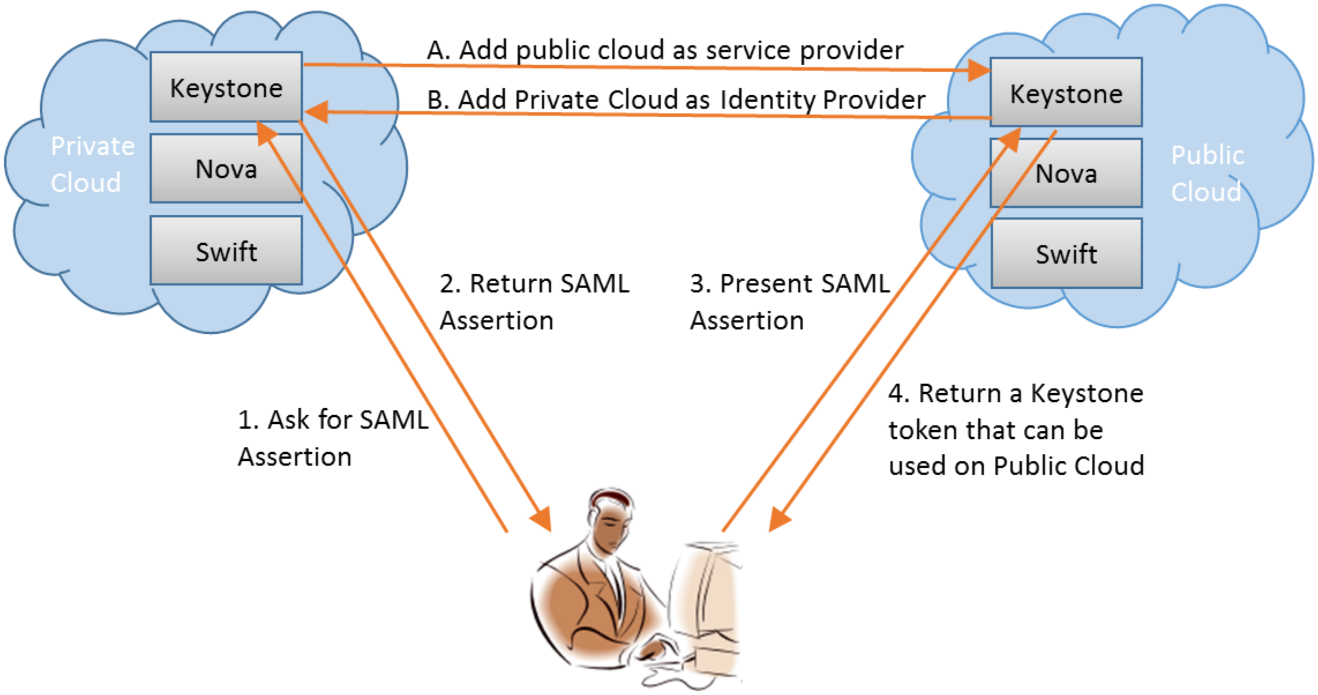
Multi-Cloud Multi-Tenant Role-Based Access Control

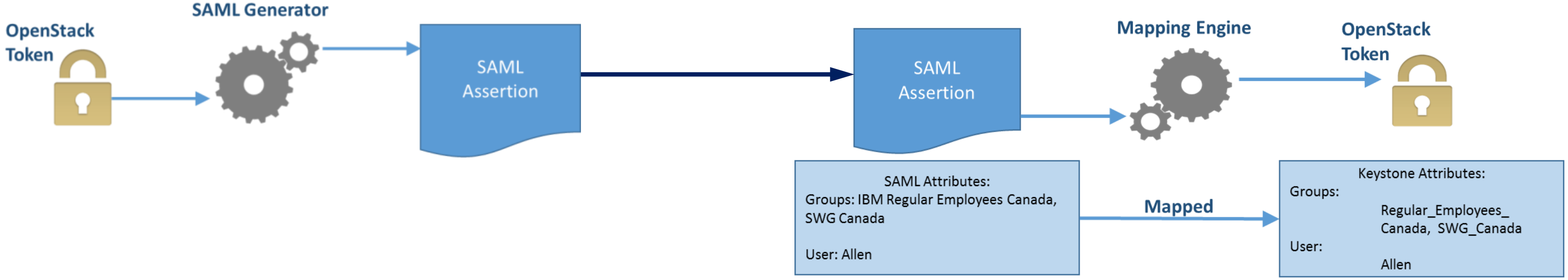
- Homogeneous multi-cloud IaaS (OpenStack).
- Peer-to-Peer federation between tenants across cloud service providers.
- User-role assignments.
- Trust is defined as tenant-trust.
- Trust types $\alpha, \beta, \gamma,$ and δ authorizes user-role assignments.



World-Leading Research with Real-World Impact!

Keystone to Keystone Federation


Keystone
Nova
Swift
Private Cloud
A. Add public cloud as service provider
B. Add Private Cloud as Identity Provider
Keystone
Nova
Swift
Public Cloud
2. Return SAML Assertion
3. Present SAML Assertion
1. Ask for SAML Assertion
4. Return a Keystone token that can be used on Public Cloud



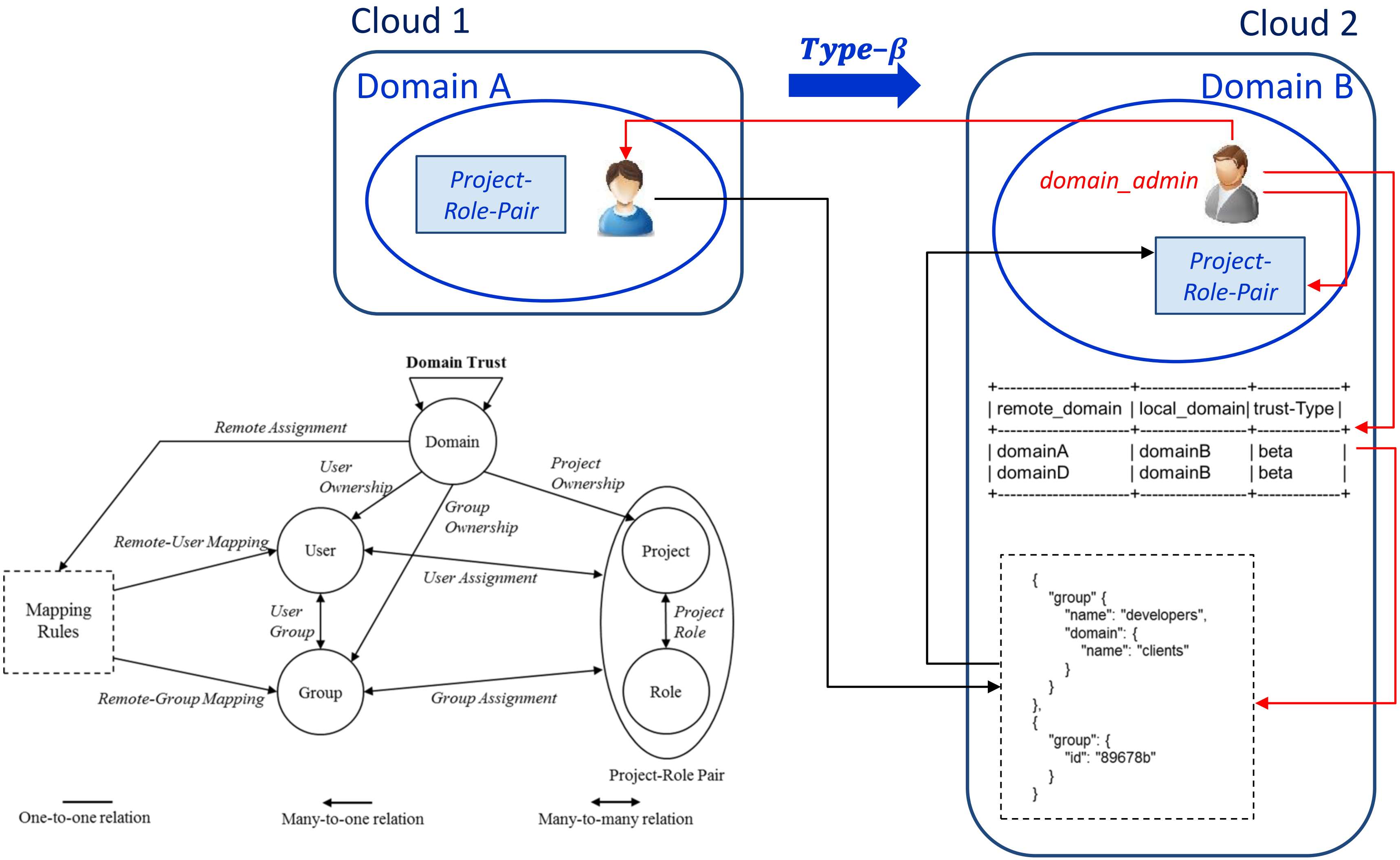
SAML Attributes:
Groups: IBM Regular Employees Canada, SWG Canada

User: Allen

Keystone Attributes:
Groups:
Regular_Employees_ Canada, SWG_Canada
User:
Allen

- OpenStack Paris Summit, Keystone to Keystone Federation, https://www.openstack.org/summit/openstack-paris-summit-2014/session-videos/presentation/keystone-to-keystone-federation, (2014)

Multi-Cloud MT-RBAC OpenStack



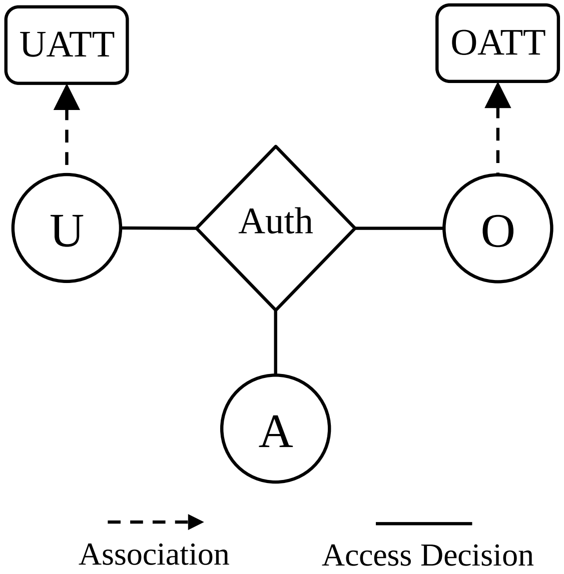
```
+-------------------+---------------+-----------+
| remote_domain  | local_domain| trust-Type |
+-------------------+---------------+-----------+
| domainA           | domainB       | beta          |
| domainD           | domainB       | beta          |
+-------------------+---------------+-----------+
```

```
{
    "group" {
        "name": "developers",
        "domain": {
            "name": "clients"
        }
    }
},
{
    "group": {
        "id": "89678b"
    }
}
```

$\mathbf{ABAC_0}$

Attribute-Based Access Control ($ABAC_0$)

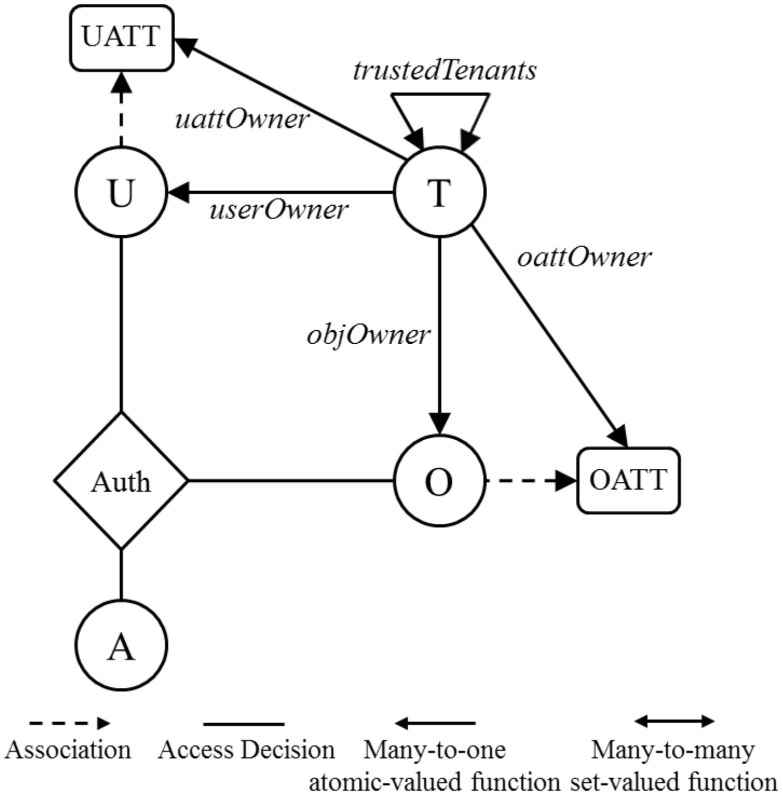
- Attributes are name:value pairs.
  - Represents user and resource properties.
- Associated with
  - Users
  - Objects
  - Tenants
  - Contexts
- Converted to rights by authorization policies
  - In-time
  - Entity attributes
  - Set of actions



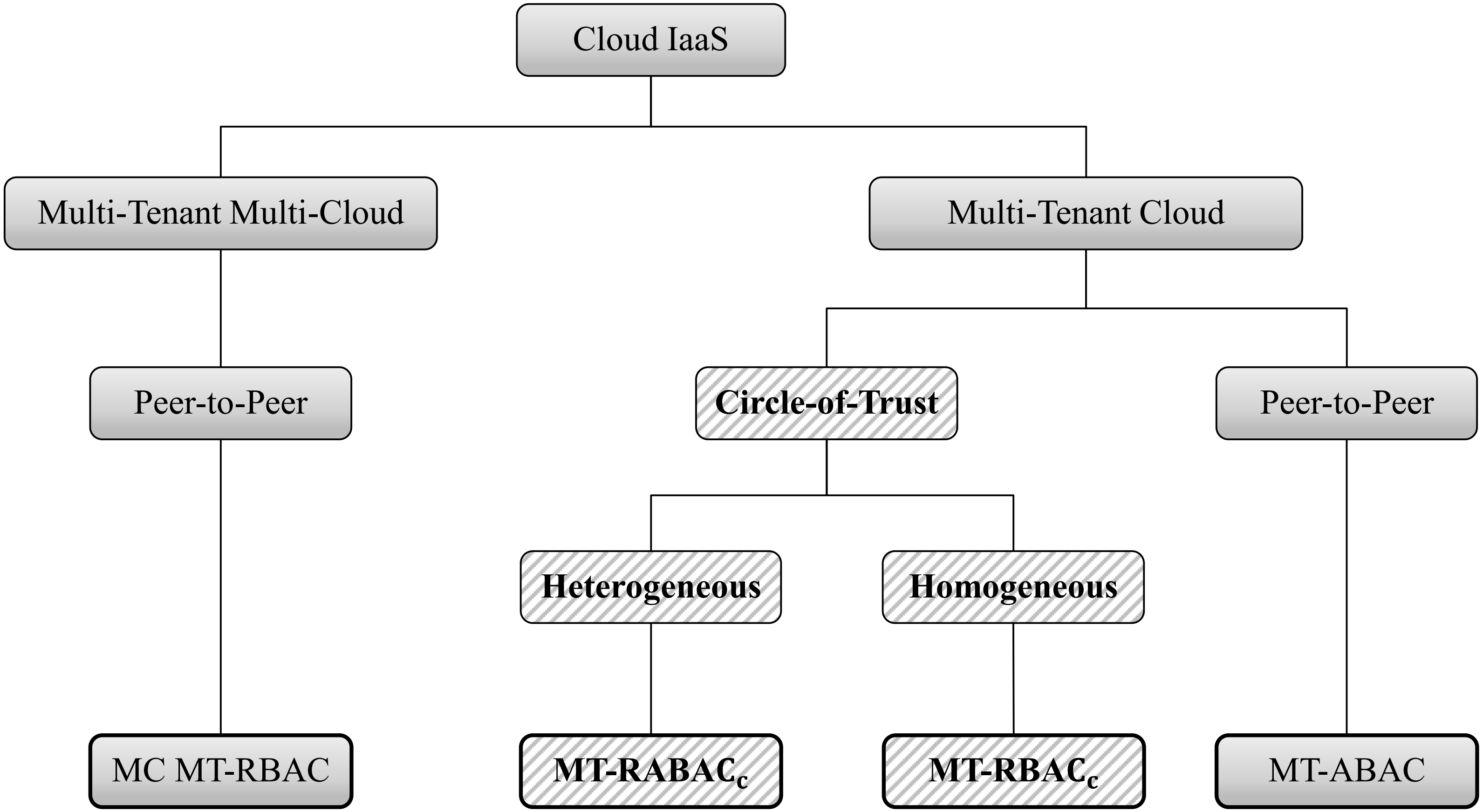
$\mathbf{MT - ABAC_0}$

Multi-Tenant Attribute-Based Access Control ($\mathbf{MT - ABAC_0}$)

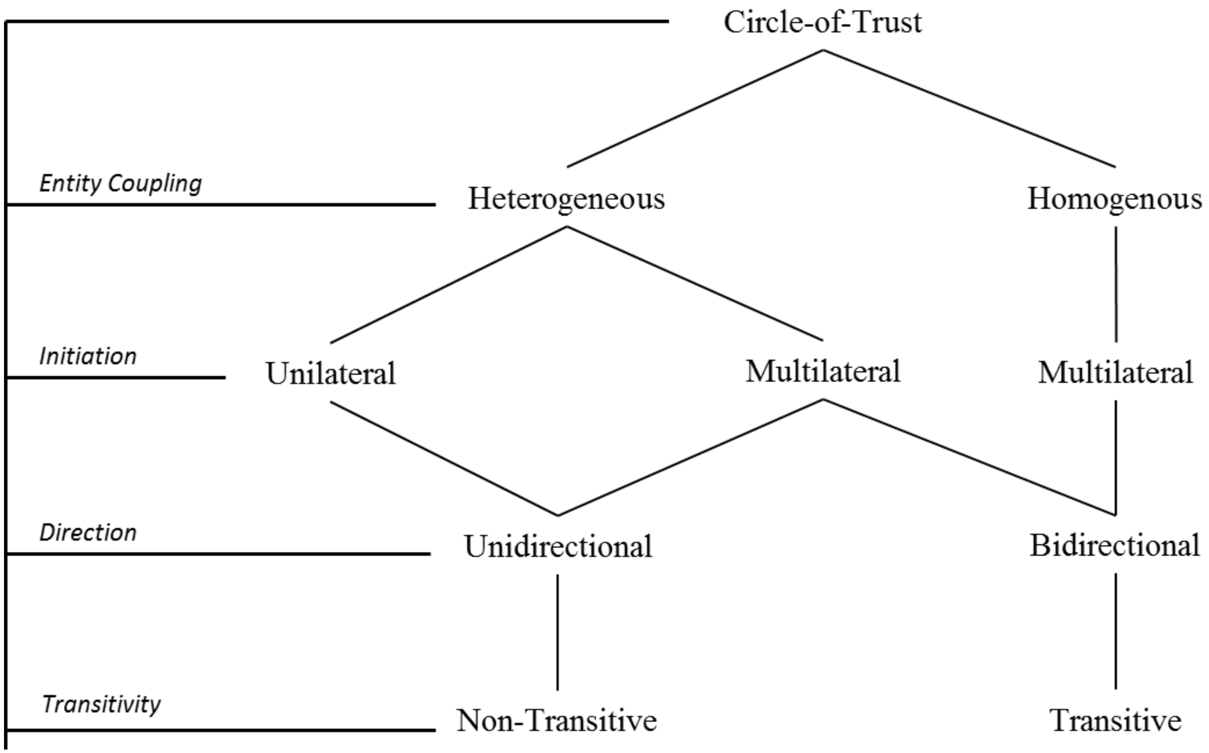
- Multi-tenant cloud IaaS.
- Peer-to-Peer Federation.
- Attribute assignments.
- Trust is defined as tenant-trust.
- Trust types α, β, γ, and δ authorizes attribute assignments.



Contributed Models



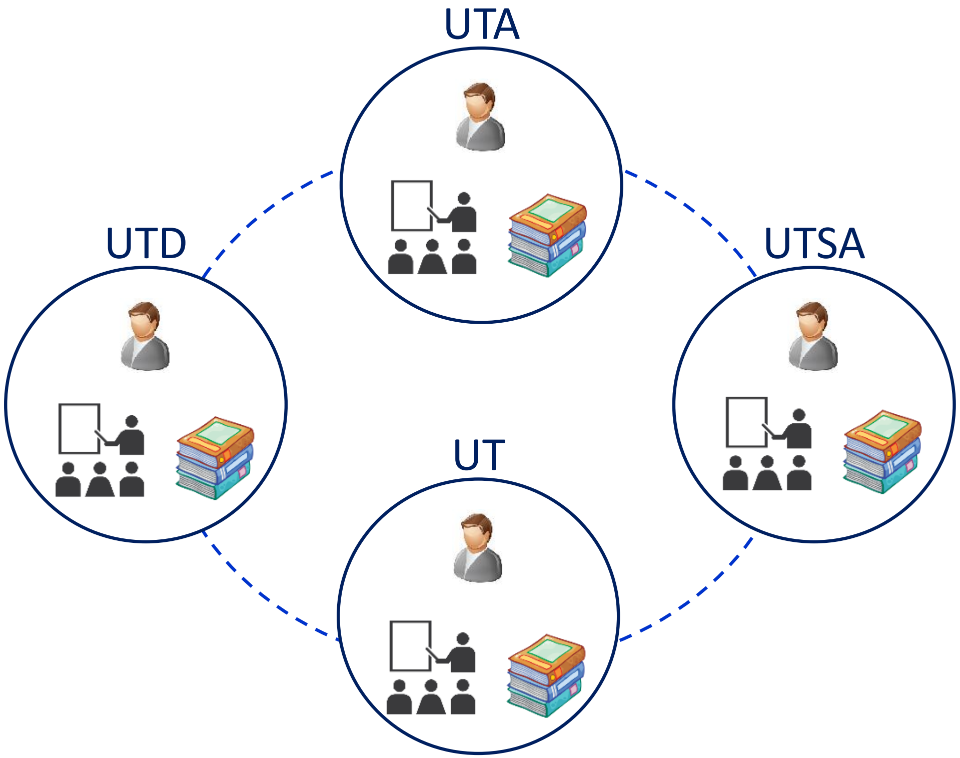
Circle-of-Trust Federation Trust



- **Homogeneous Circles**
  - *Multilateral, Bidirectional, Transitive.*
- **Heterogeneous Circles**
  - *Multilateral, Unidirectional, Non-Transitive.*

CoT Trust Types Use Case

- **UT System CoT Federation.**
  - UT system students can take courses at any UT campus.
  - Students can access to libraries in UT system.

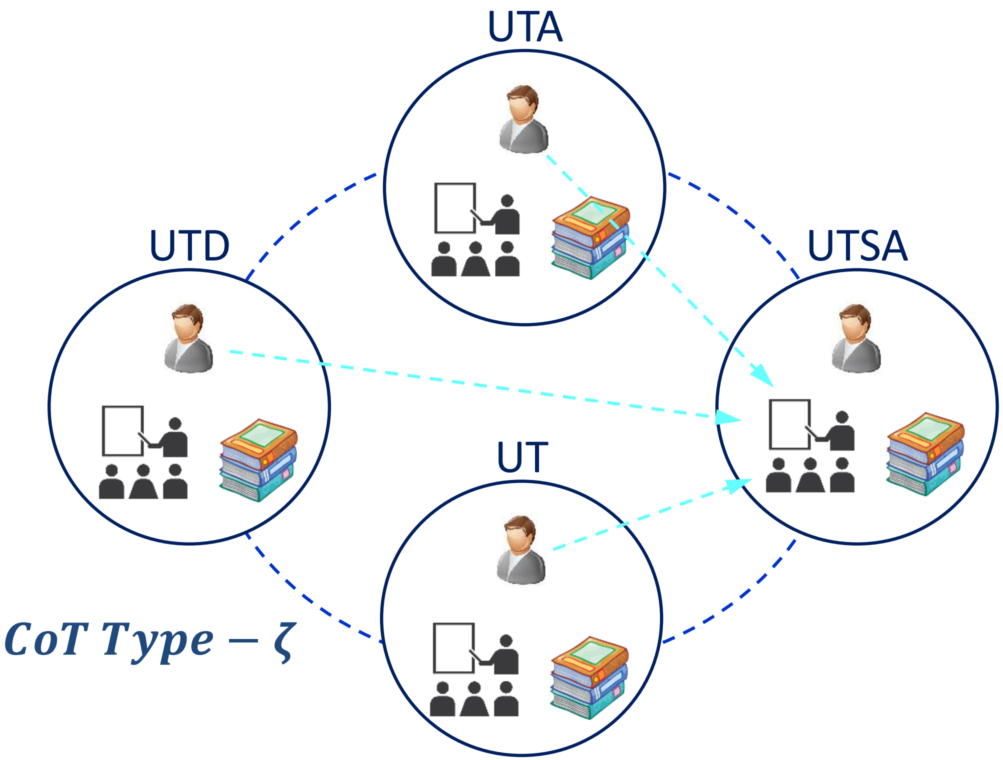


World-Leading Research with Real-World Impact!

CoT Trust Types Use Case

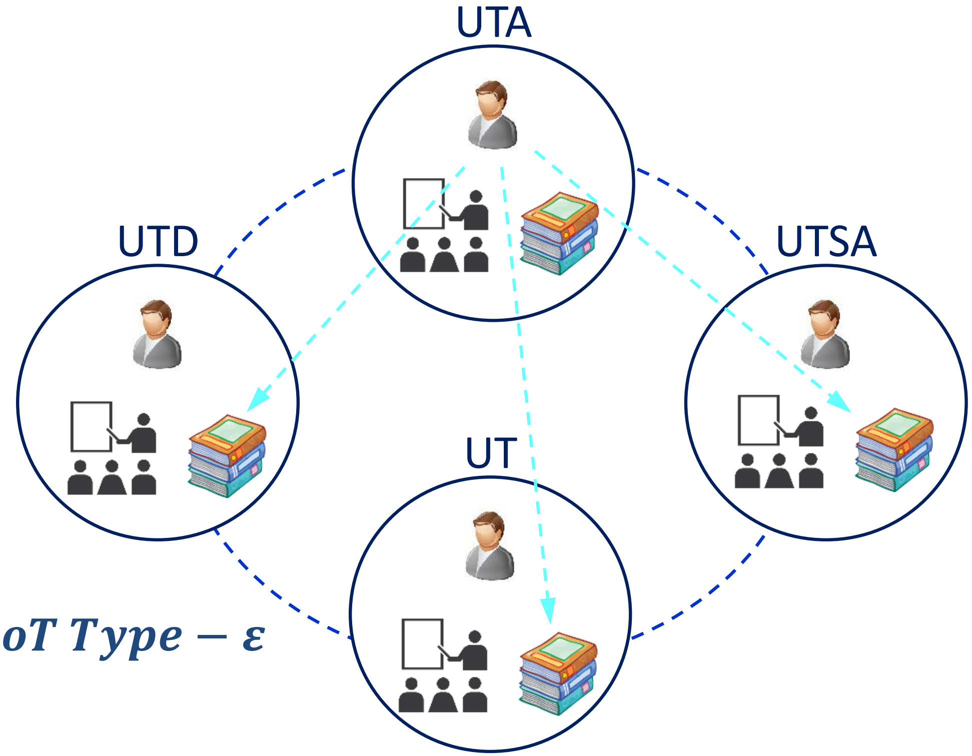
UT System CoT Federation.

- ❖ UT system students can take courses at any UT campus.
  - ○ UTSA can assign students in UT to its courses.



CoT Trust Types Use Case

- **UT System CoT Federation.**
  - Students can access to libraries in UT system.
    - UTA can assign its students to libraries in UT system.

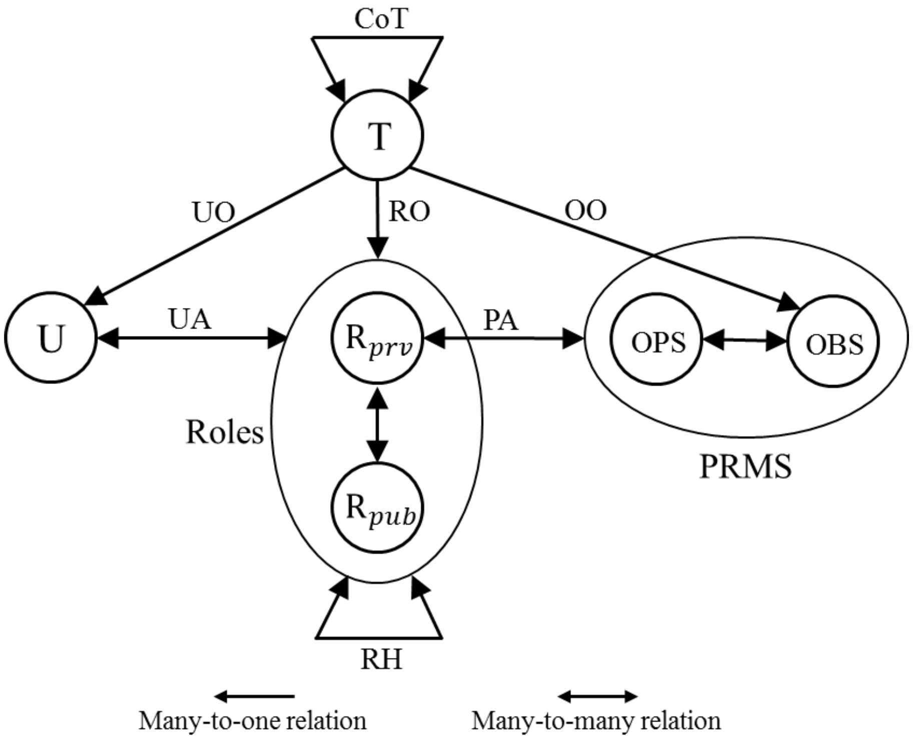


$\boldsymbol{CoT\ Type - \varepsilon}$

$MT - RBAC_c$

Multi-Tenant Role-Based Access Control in Circle ($MT - RBAC_c$)

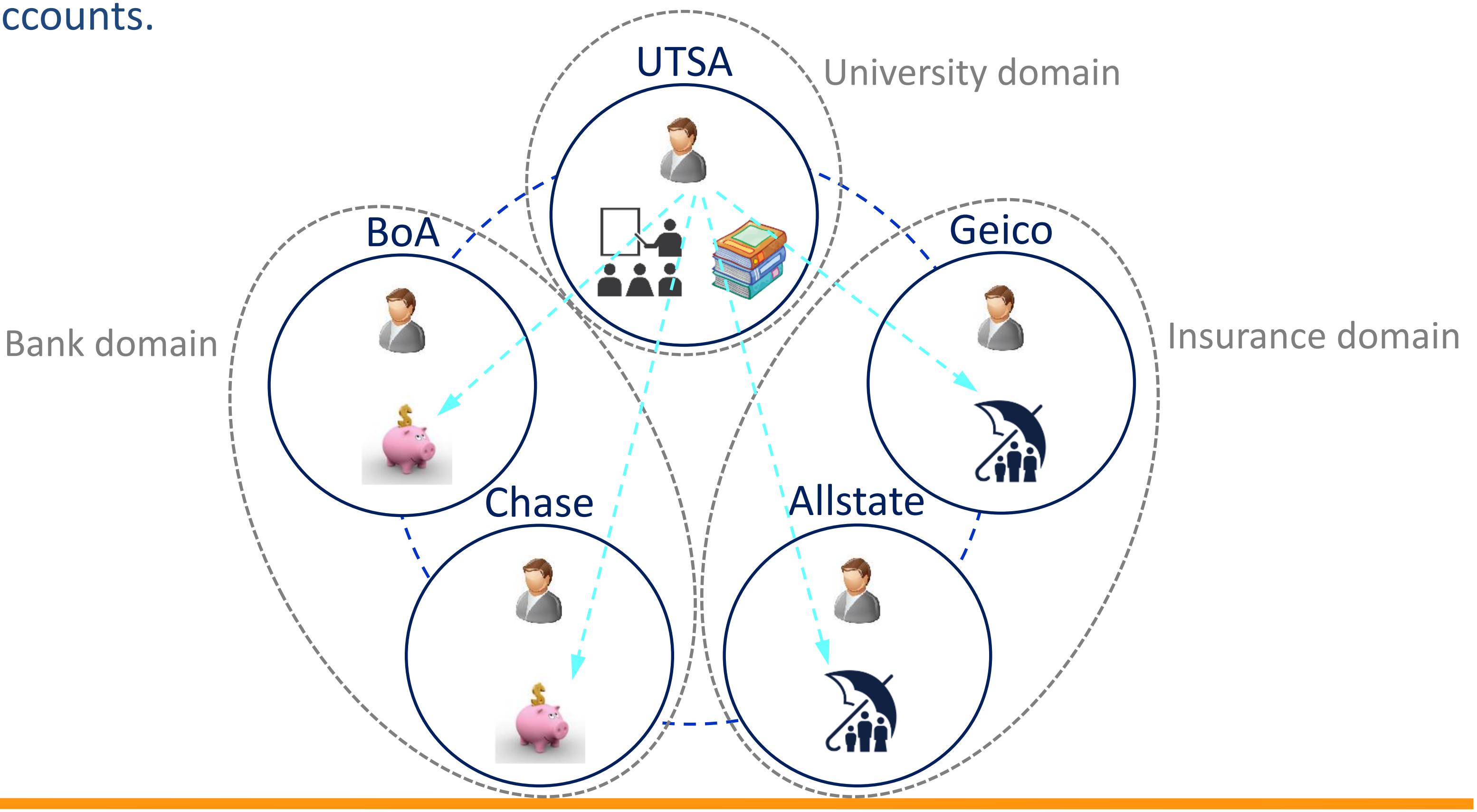
- Multi-tenant cloud IaaS.
- Circle-of-Trust Federation.
- Homogeneous circles.
- User-role assignments.
- Trust is defined as tenant-trust.
- Trust types ε and ζ authorizes user-role assignments.



World-Leading Research with Real-World Impact!

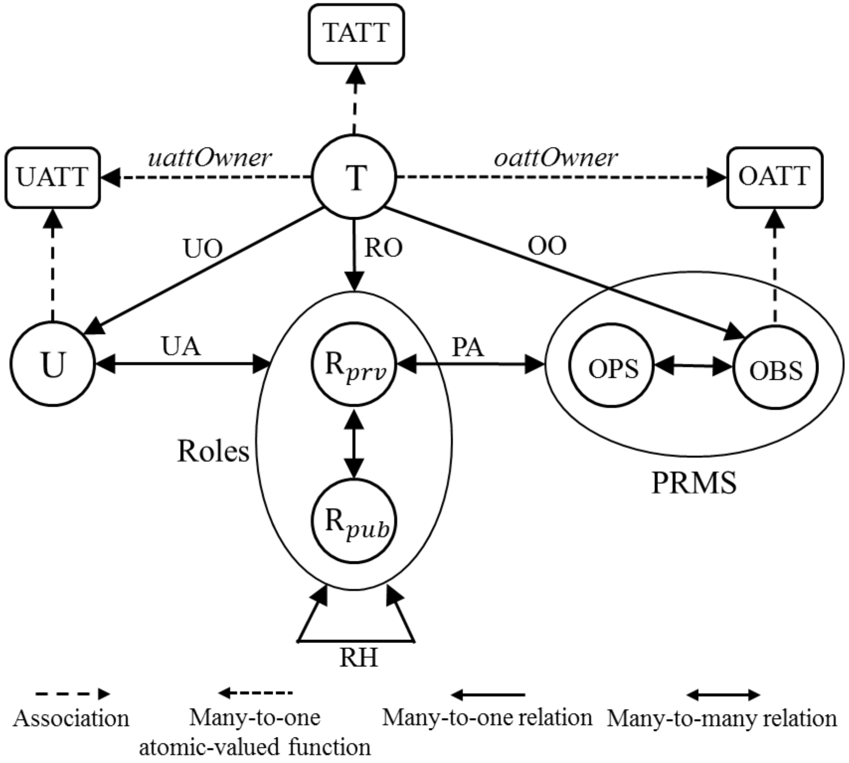
Heterogeneous Circle Use Case

- **Heterogeneous circle of BoA, Chase, UTSA, Geico, Allstate.**
  - Each tenant can make user-role assignment based on its type to a domain.
  - UTSA can assign its students to discounted insurance offers and student accounts.



$\mathbf{MT-RABAC_c}$

- **Multi-Tenant Role-Centric Attribute-Based Access Control ($\mathbf{MT-RABAC_c}$)**
  - Multi-tenant cloud IaaS.
  - Circle-of-Trust Federation.
  - Heterogeneous circles.
  - Attributes are associated with
    - Tenants
    - Users
    - Objects
  - Tenant attributes separate tenants with tenant type attribute.



World-Leading Research with Real-World Impact!

Questions ?

- Peer-to-Peer Policy
  - Multi-cloud multi-tenant role-based model.
  - Multi-tenant attribute-based model.
- Circle-of-Trust Policy
  - Multi-tenant role-based access control model in circle.
  - Multi-tenant role-centric attribute-based access control model.
- Implementation
  - Federated-cloud role-based tenant trust.