Role-Centric Circle-of-Trust in Multi-Tenant Cloud IaaS

Prof. Ravi Sandhu
Executive Director and Endowed Chair

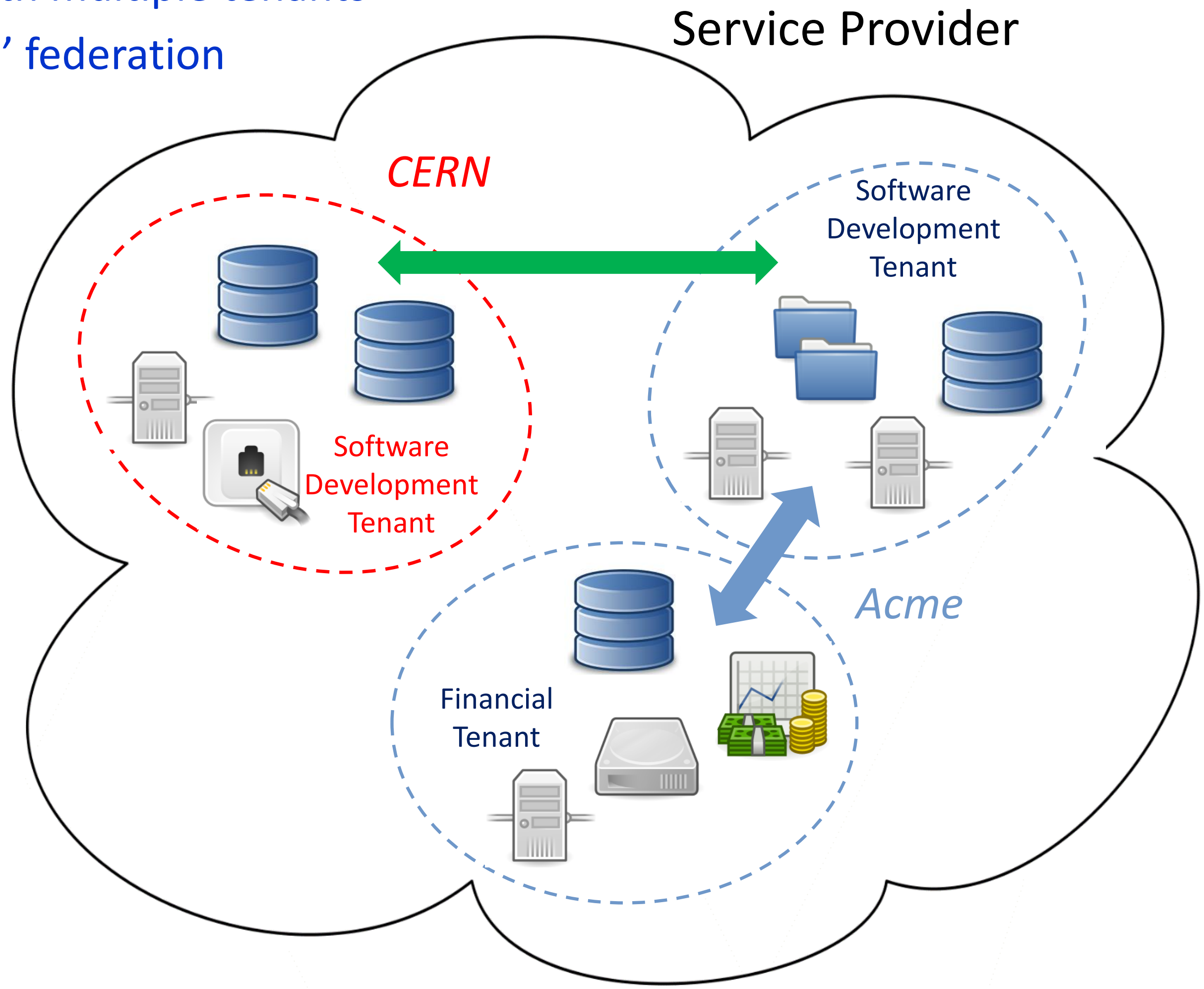
DBSec
July 20, 2016

ravi.sandhu@utsa.edu
www.profsandhu.com

Navid Pustchi and Ravi Sandhu

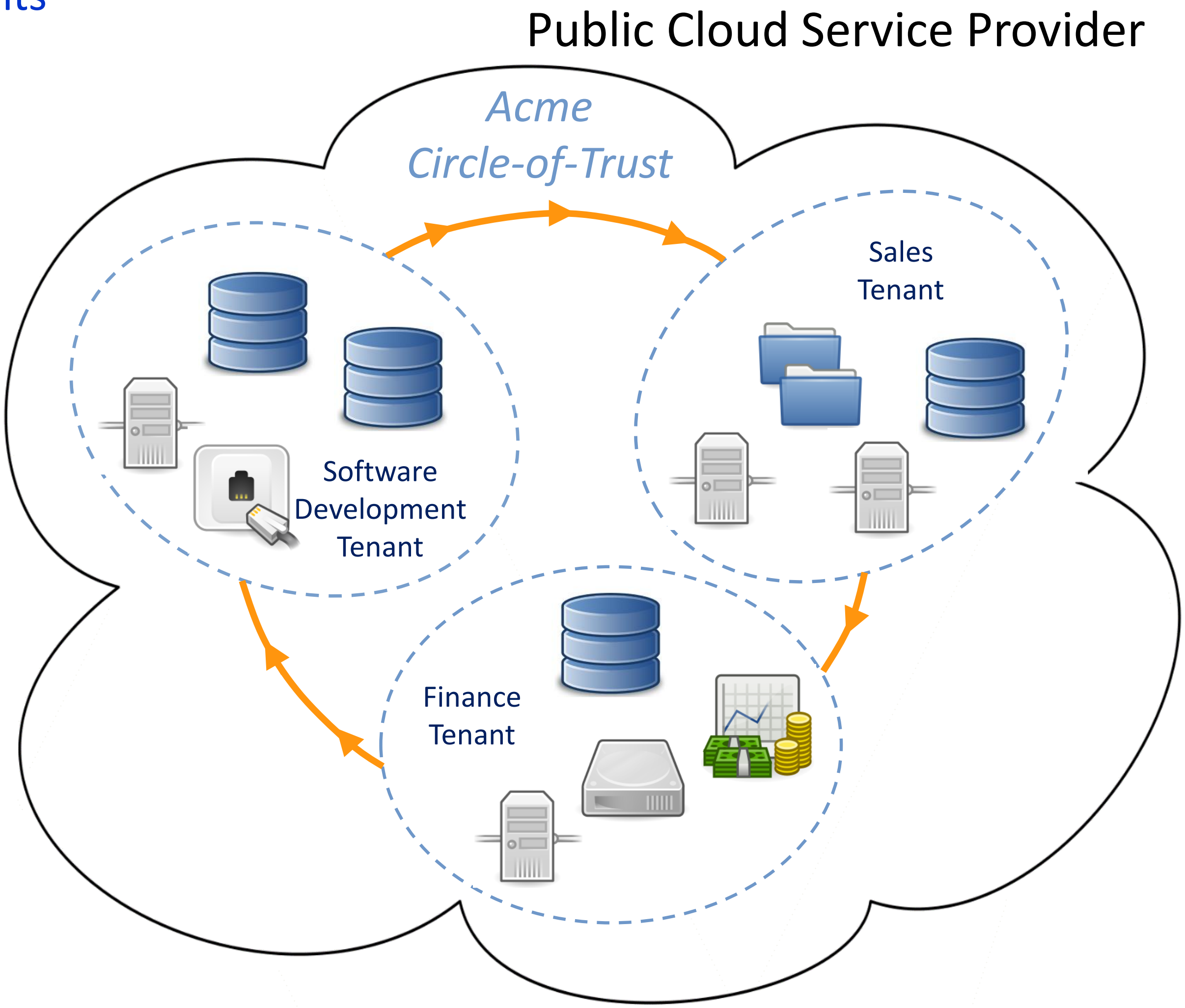
Why Federation ?

- Large organization with multiple tenants
- Distinct organizations' federation

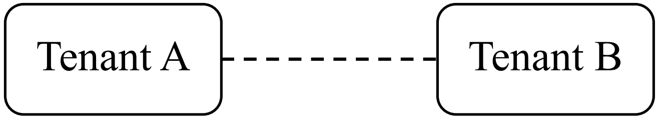


Why Circle-of-Trust in Cloud?

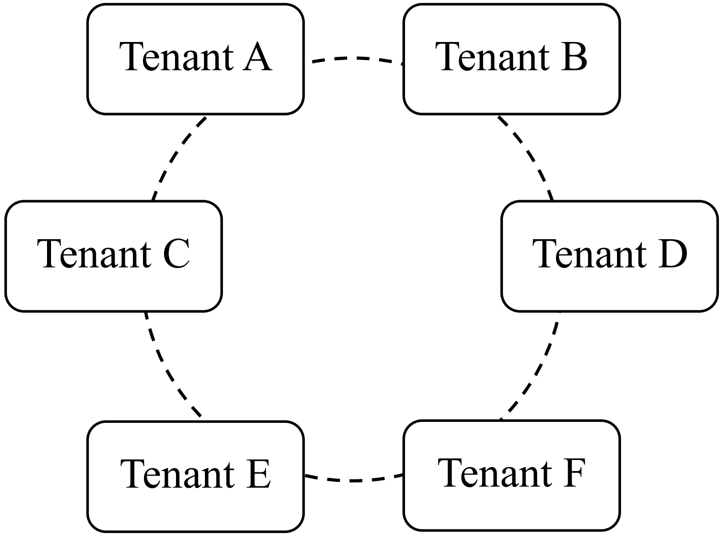
- A circle of Acme tenants



Peer-to-Peer vs Circle-of-Trust



- ***Peer-to-Peer***
  - Trust between a pair of tenants.
  - Specific set of actions between tenants.
  - Only trusted tenant acceptance.

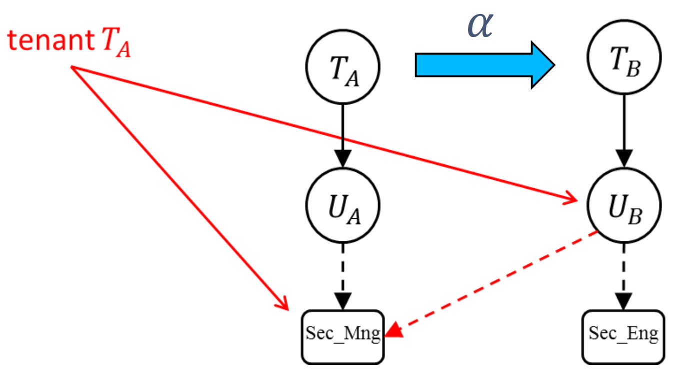


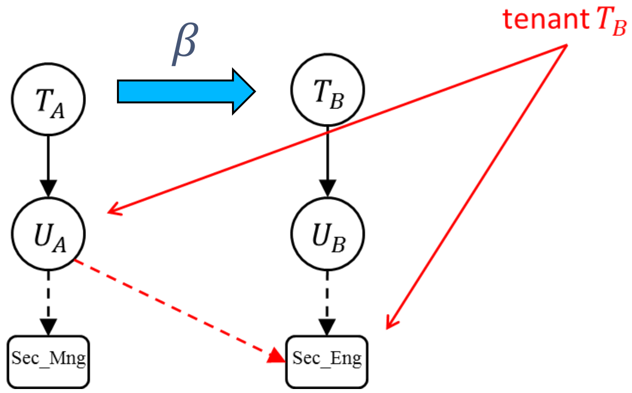
- ***Circle-of-Trust***
  - Trust between a group of tenants.
  - Similar policies and rules.
  - Acceptance of all tenants in the circle.

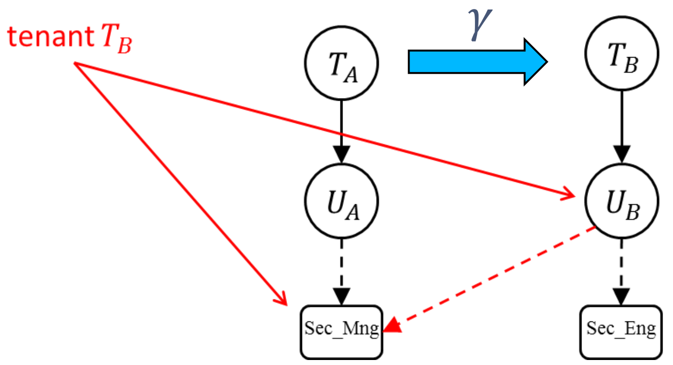
Peer-to-Peer Tenant-Trust

Peer-to-Peer Tenant-Trust

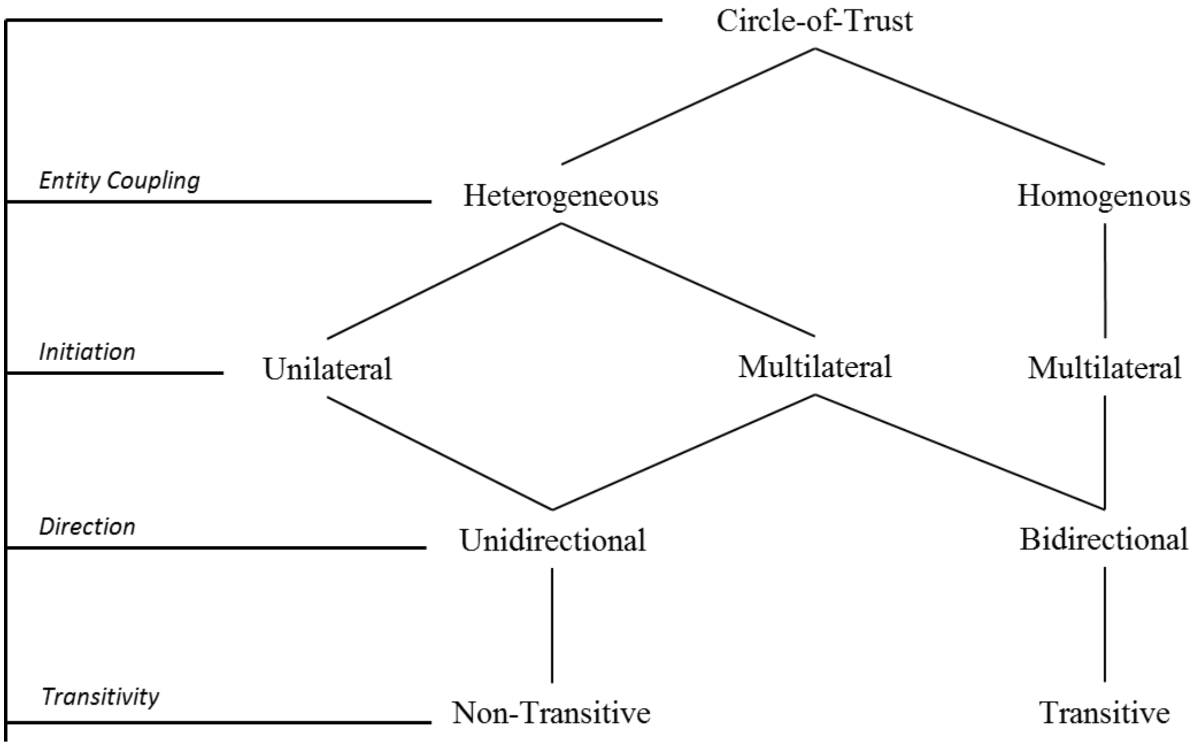
- User- role and attribute assignments across tenants.
- Tenant-trust types $\alpha, \beta, and\ \gamma$.







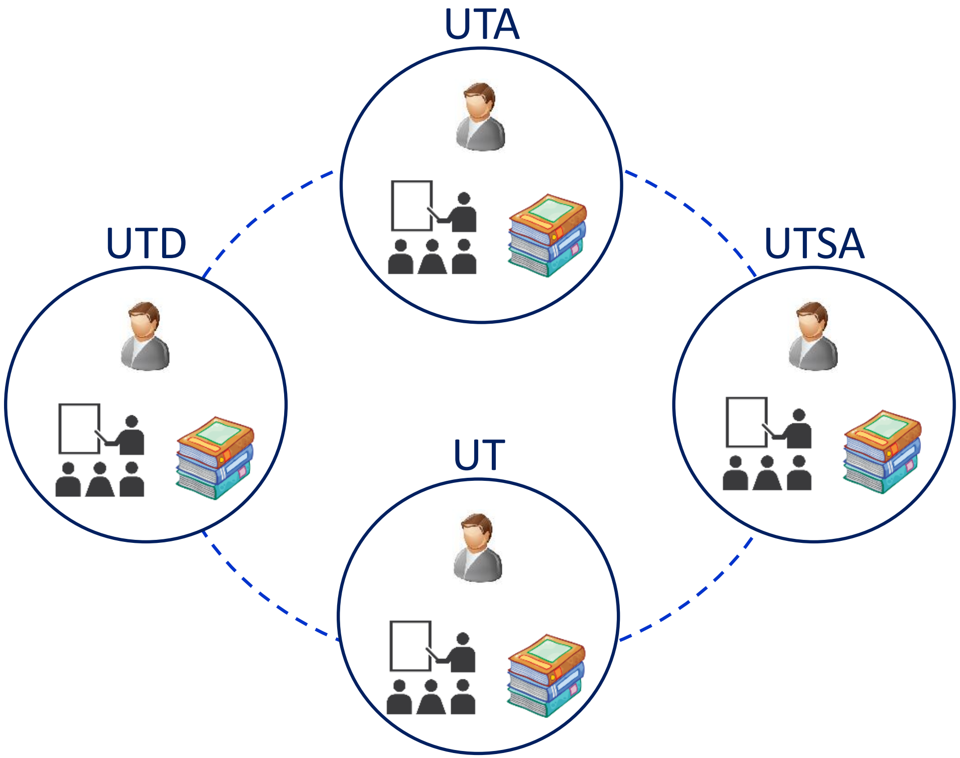
Circle-of-Trust Federation Trust



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

CoT Trust Types Use Case

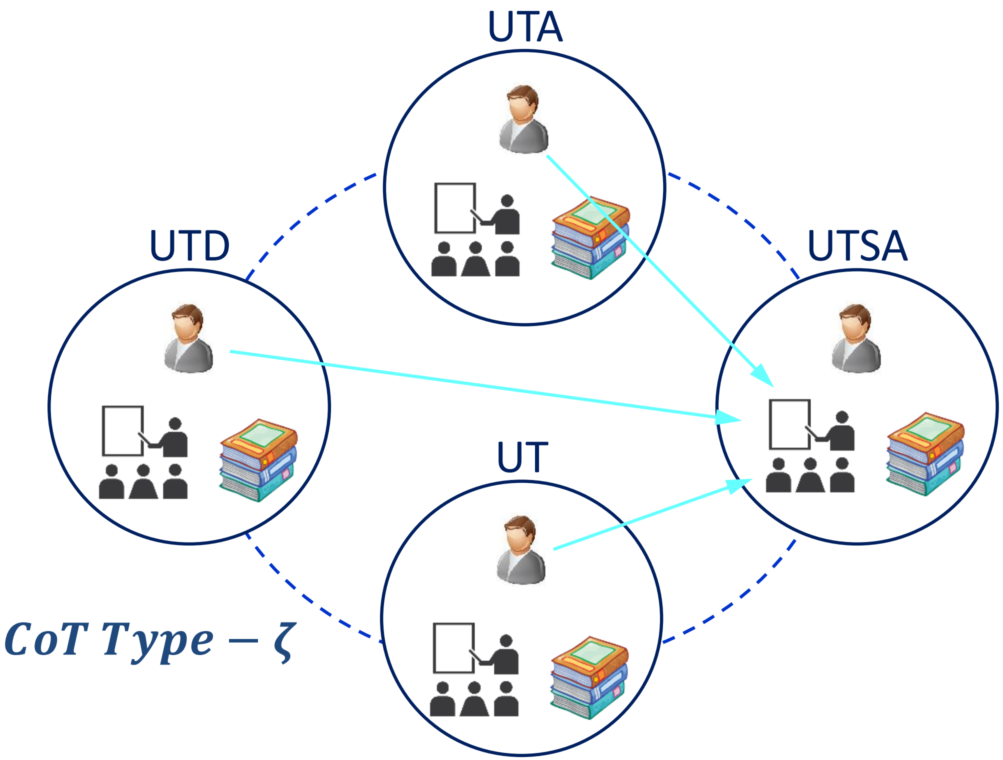
- **UT System CoT Federation.**
  - UT system students can take courses at any UT campus.
  - Students can access to libraries in UT system.



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.

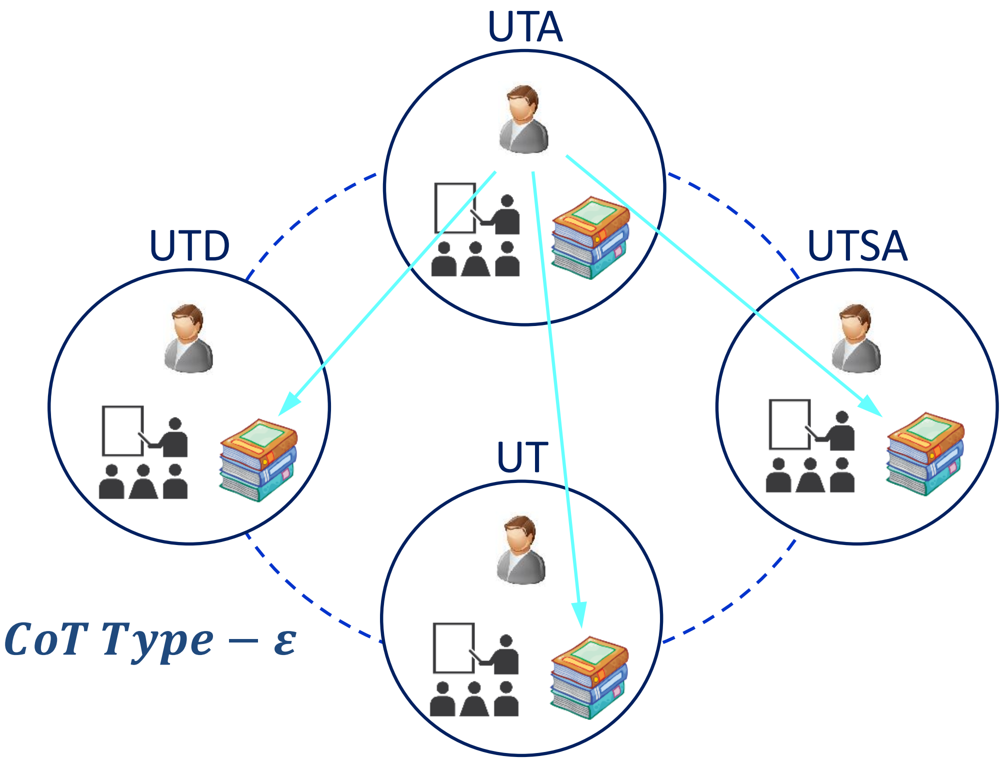


$CoT\ Type - \zeta$

CoT Trust Types Use Case

UT System CoT Federation.

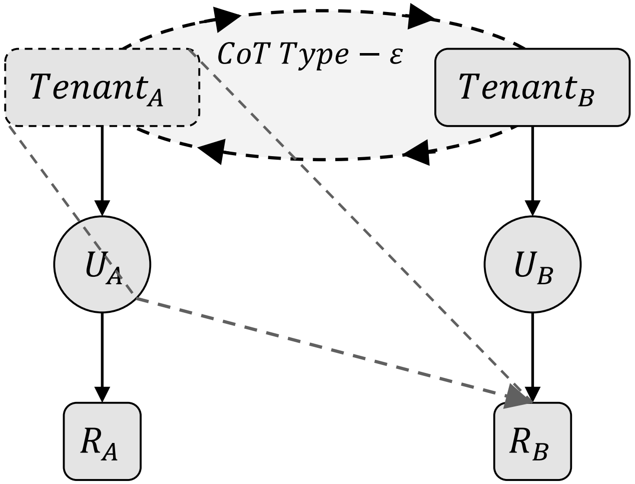
- Students can access to libraries in UT system.
- UTA can assign its students to libraries in UT system.

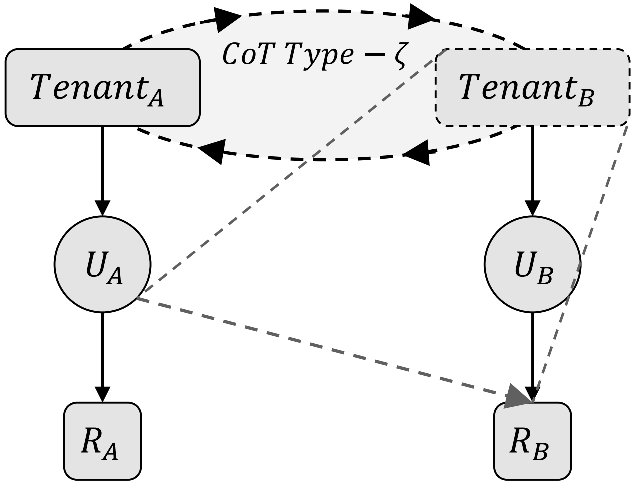


CoT Trust Types

- **Tenant-Trust Type−ϵ:**
  - User-owner tenants are authorized to assign their users to roles in the circle.

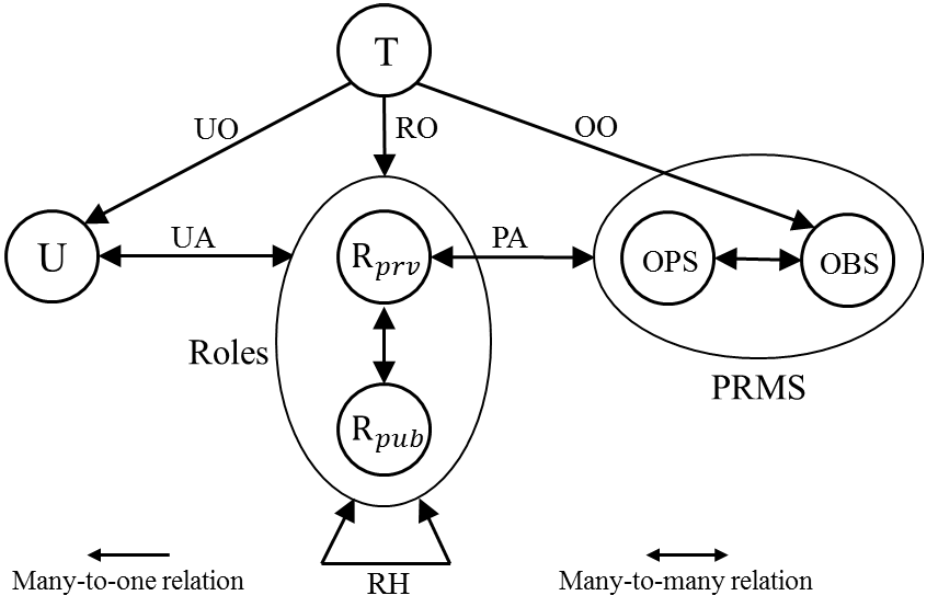
- **Tenant-Trust Type−ζ:**
  - Resource-owner tenants are authorized to assign users in the circle to their roles.





$\mathrm{MT} - \mathrm{RBAC}_c$

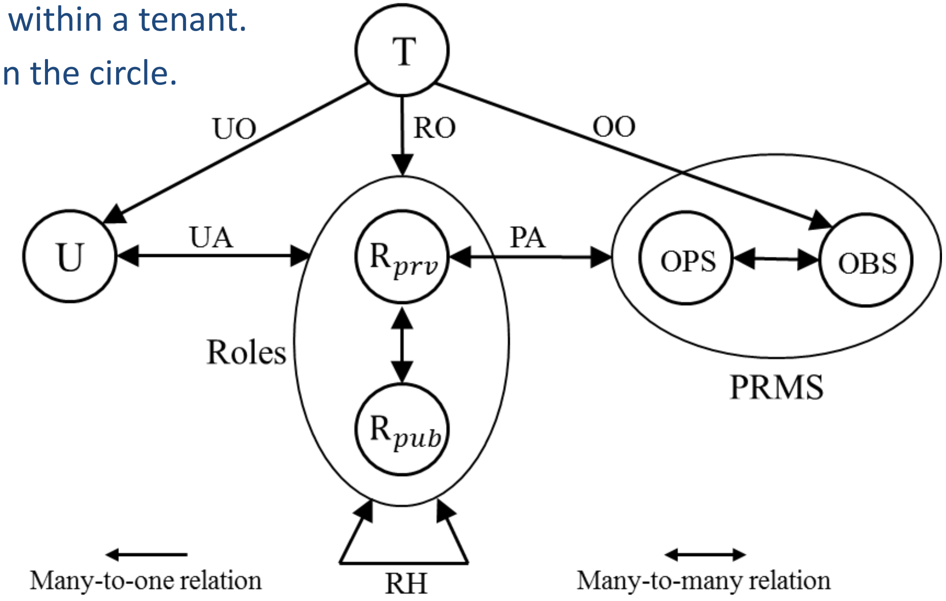
- **Multi-Tenant Role-Based Access Control in Circle ($\mathrm{MT} - \mathrm{RBAC}_c$)**
  - Homogeneous circles.
  - Cross-tenant user-role assignments.
  - Trust is defined between tenants.
  - Tenant-trust types ε and ζ.



$\mathbf{MT - RBAC_c}$

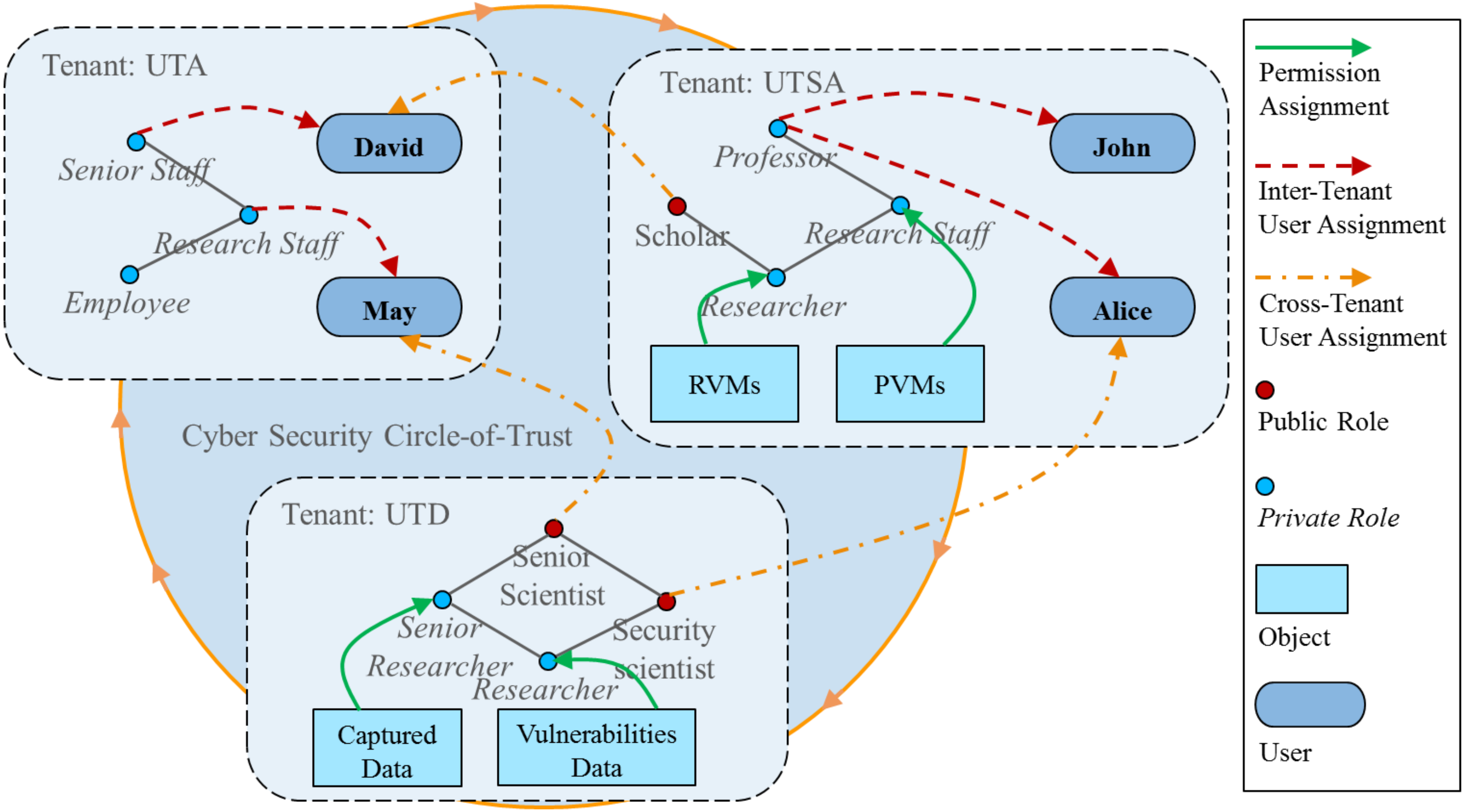
➢ Multi-Tenant Role-Based Access Control in Circle ($\mathbf{MT - RBAC_c}$)

- ❖ Users, roles, and permissions are owned by tenants.
- ❖ Users are assigned to private roles in tenants and public roles across tenants.
- ❖ Permissions are assigned only to private roles.
- ❖ Role Hierarchy:
  - ○ Private roles only inherit private roles within a tenant.
  - ○ Public roles inherit private role roles within a tenant.
  - ○ Public roles inherit public roles within the circle.



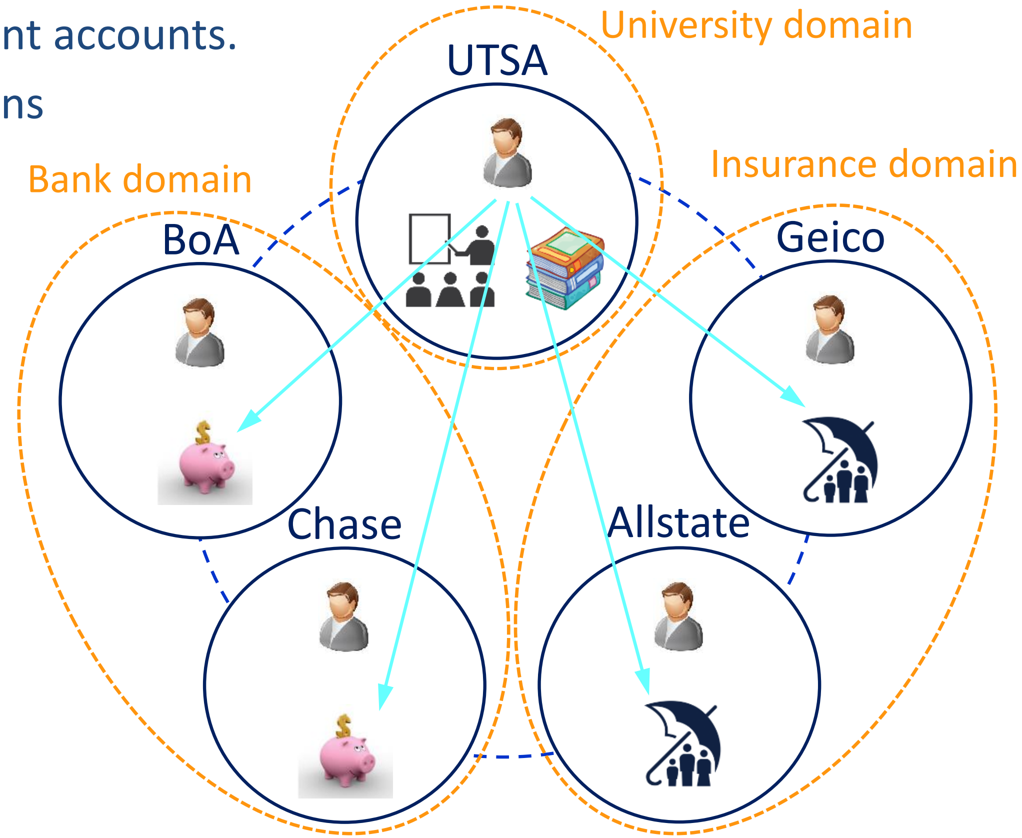
MT – RBAC$_C$ Use Case

- Homogeneous circle of UTA, UTSA, and UTD



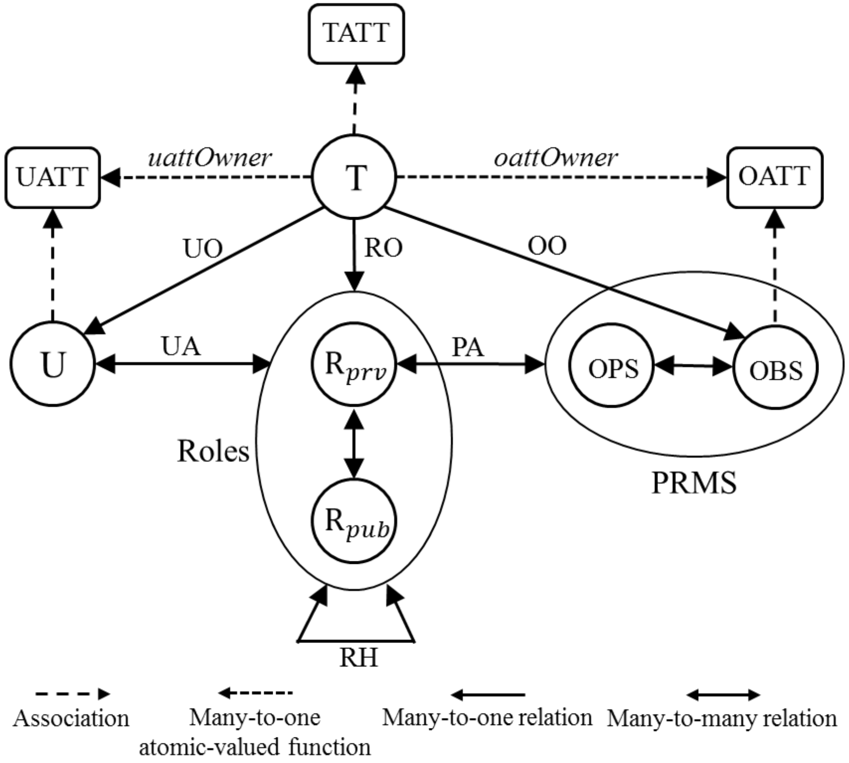
Heterogeneous Circle Use Case

- **Heterogeneous circle of BoA, Chase, UTSA, Geico, and Allstate.**
  - Each tenant can make user-role assignment based on its type.
  - UTSA can assign its students to discounted insurance offers and student accounts.
  - Bank and Insurance domains are not allowed to assign their users to UTSA resources.



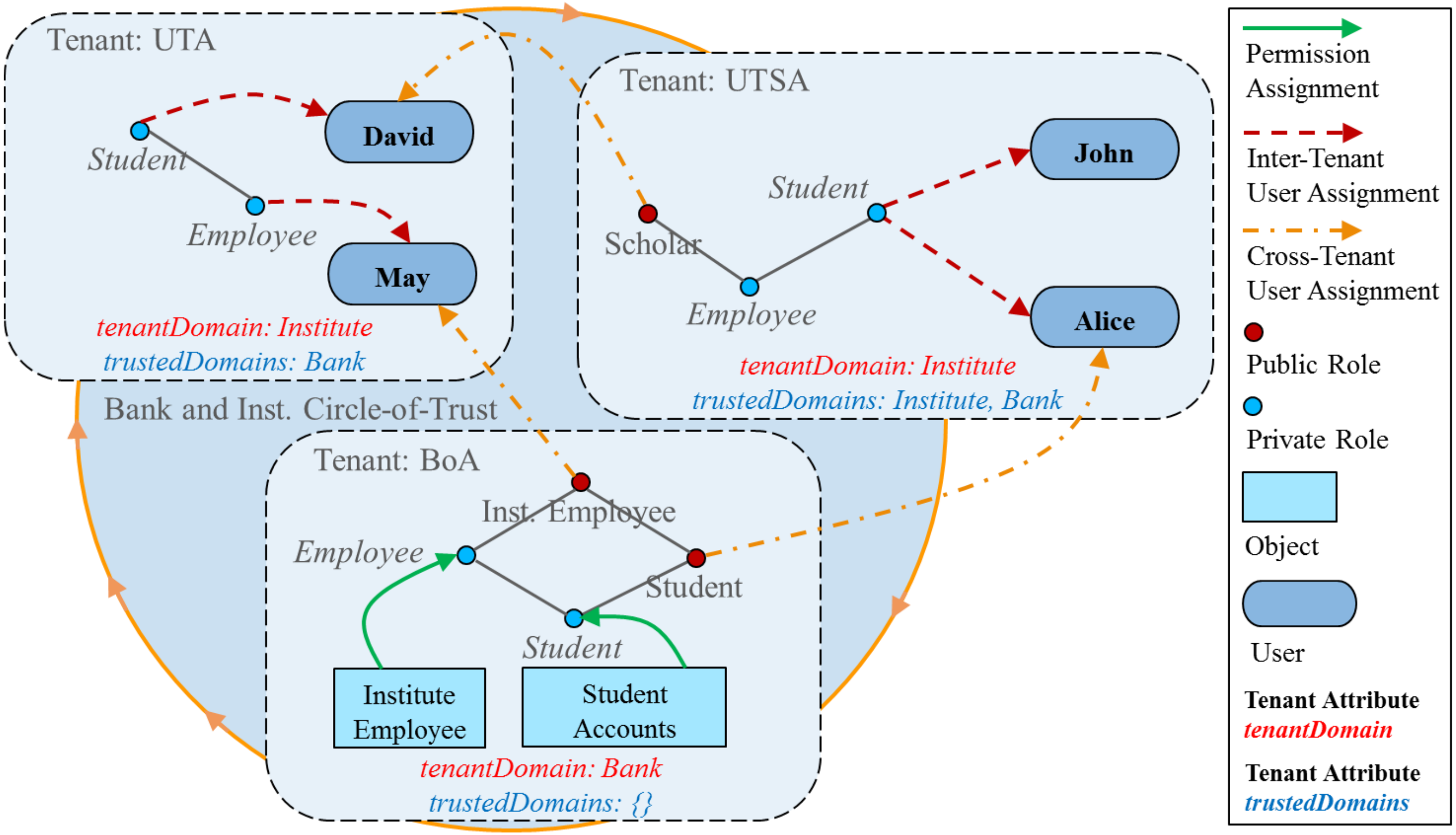
$\mathbf{MT - RABAC_c}$

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



MT – RABAC$_c$ Use Case

- **Heterogeneous circle of UTA, UTSA, and BoA**



Conclusion

- **Role-Centric Circle-of-Trust in Multi-Tenant cloud IaaS**
  - $\mathbf{MT-RBAC_c}$ in homogeneous circles.
    - Collaboration through *user to public role assignments*.
    - Resource protection by limited role hierarchy.
    - Trust is defined as tenant-trust *types* ε *and* ζ in the circle.
  - $\mathbf{MT-RABAC_c}$ in heterogeneous circles.
    - Classifying tenants into domains based on tenant type by tenant-attributes.
    - Tenant-trust defined conditionally with *trustedDomain* tenant-attribute.

- **Future Work**
  - Attribute-based model in Circle-of-Trust.
  - Further model generalization into multi-cloud Circle-of-Trust environment.
  - Model implementation as a proof of concept.