I·C·S
The Institute for Cyber Security

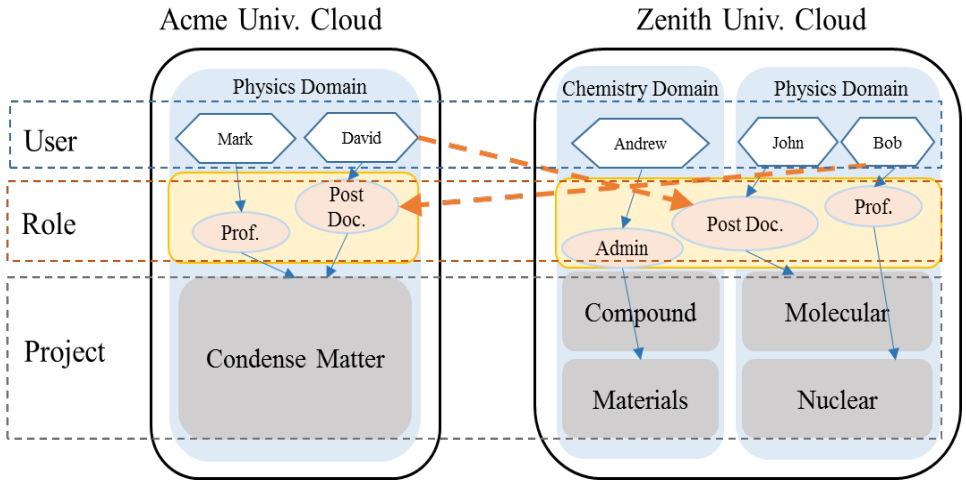
UTSA

Authorization Federation in IaaS Multi Cloud

Navid Pustchi, Ram Krishnan and Ravi Sandhu

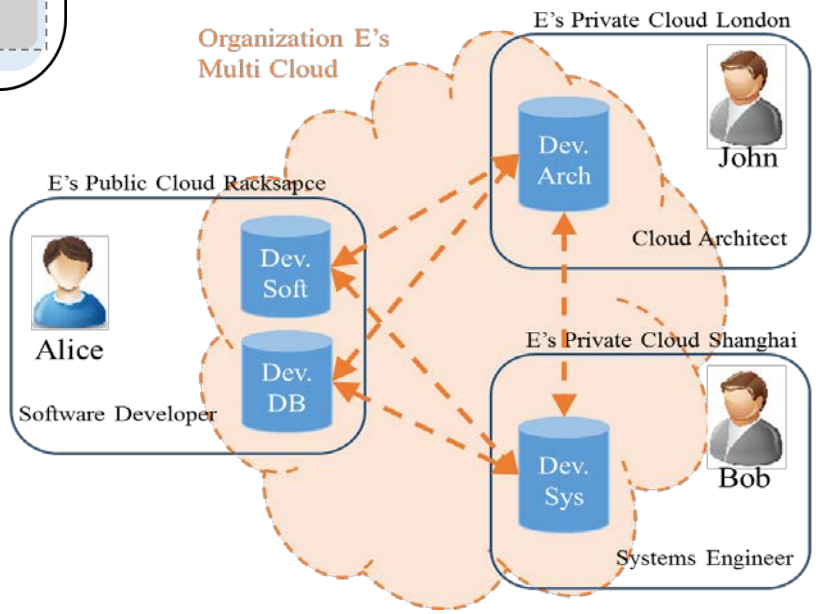
SCC 2015

Why Multi Cloud?

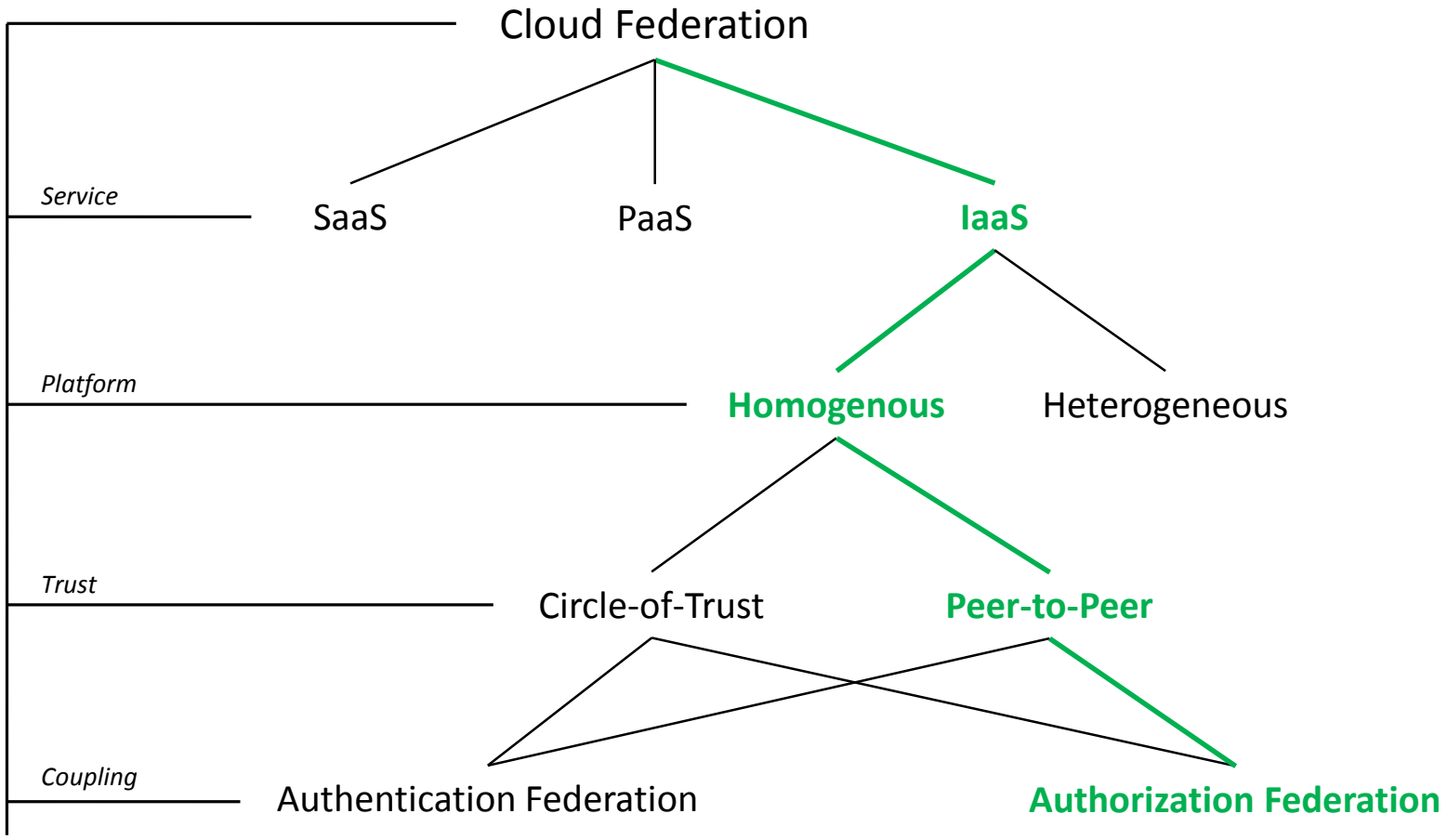


Collaboration of organizations across clouds.

Organizations with resources across multiple clouds.



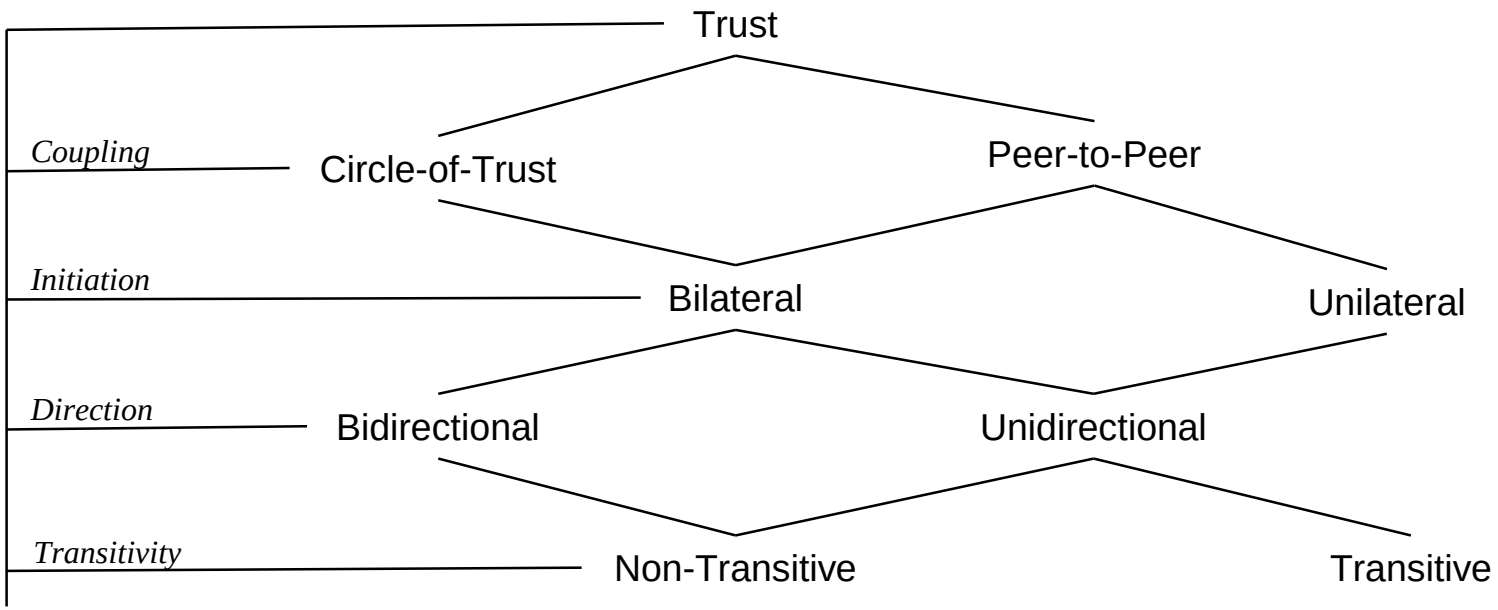
Scope of Contribution



Multi Cloud Collaboration

- Cloud Federation
  - Service (IaaS, PaaS, SaaS)
    - Heterogeneous: Google account (Open ID 2.0) Heterogeneous within google.
    - Homogenous: Eduroam federated network access.
  - Platform
    - Heterogeneous: OpenStack federation with AWS.
    - Homogenous: 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.
    - Authorization Federation: SAML, OAuth.

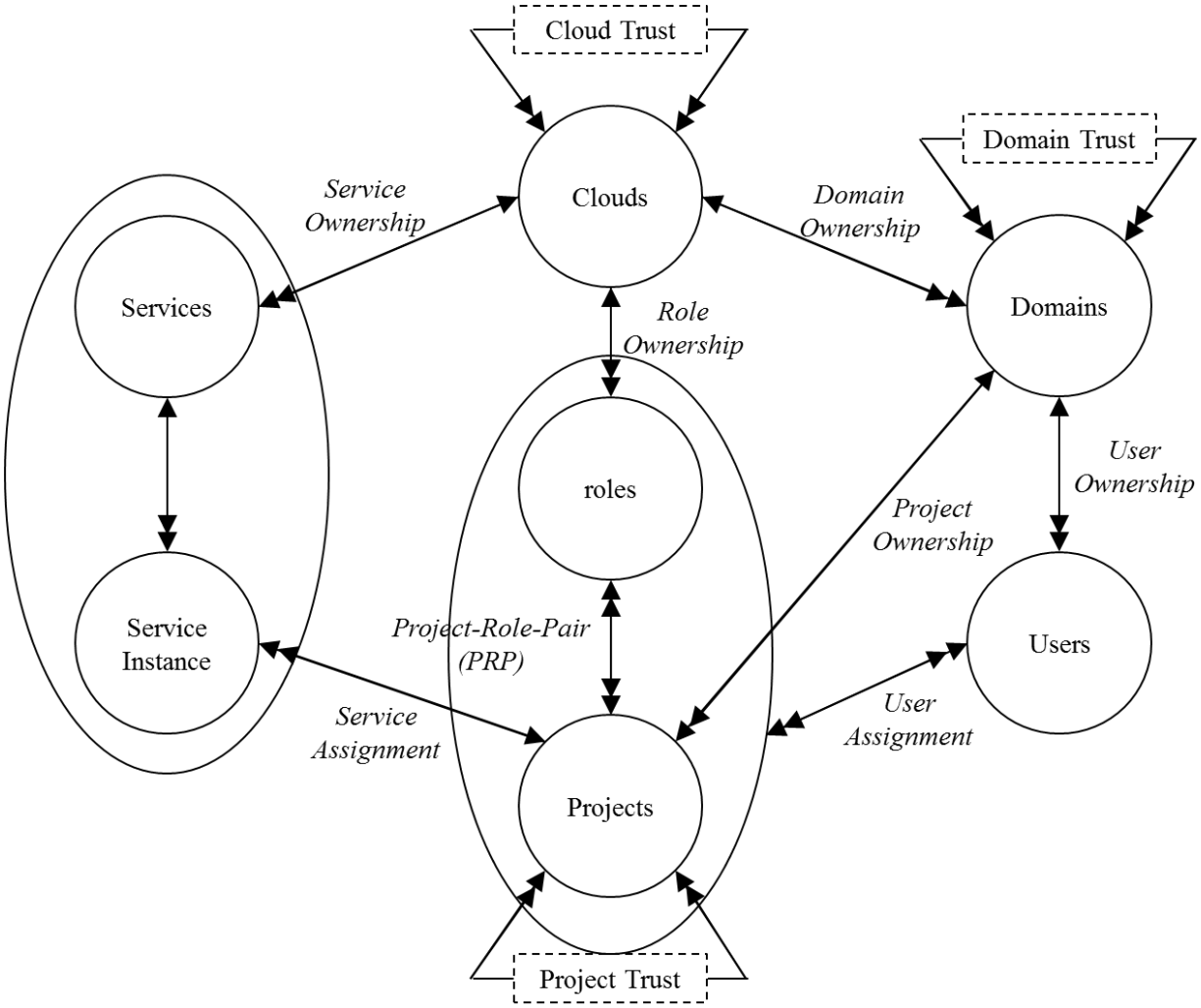
Trust Framework



Concept of Trust

- Four trust types:
  - $\boldsymbol{Type-\alpha}$: (Trustor grants inter-cloud access to trustee)
    - *If $A \trianglelefteq_{\alpha} B$, cloud A is authorized to assign B's users to cloud A's resources. In such trust type, A controls trust relation existence and cross-cloud assignments.*
  - $\boldsymbol{Type-\beta}$: (Trustee grants inter-cloud access to trustor)
    - *If $A \trianglelefteq_{\beta} B$, cloud B is authorized to assign A's users to its resources. In such trust type, A controls trust relation and B controls cross-cloud assignments.*
  - $\boldsymbol{Type-\gamma}$: (Trustee takes inter-cloud access to trustor)
    - *If $A \trianglelefteq_{\gamma} B$, cloud B is authorized to assign its users to cloud A's resources. In such trust type, A controls trust relation and B controls cross-cloud assignments.*
  - $\boldsymbol{Type-\delta}$: (Trustee controls intra-cloud access to trustor)
    - *If $A \trianglelefteq_{\gamma} B$, cloud B is authorized to assign A's users to A's resources. In such trust type, A controls trust relation and B controls intra-cloud assignments within A.*

Administrative Realms

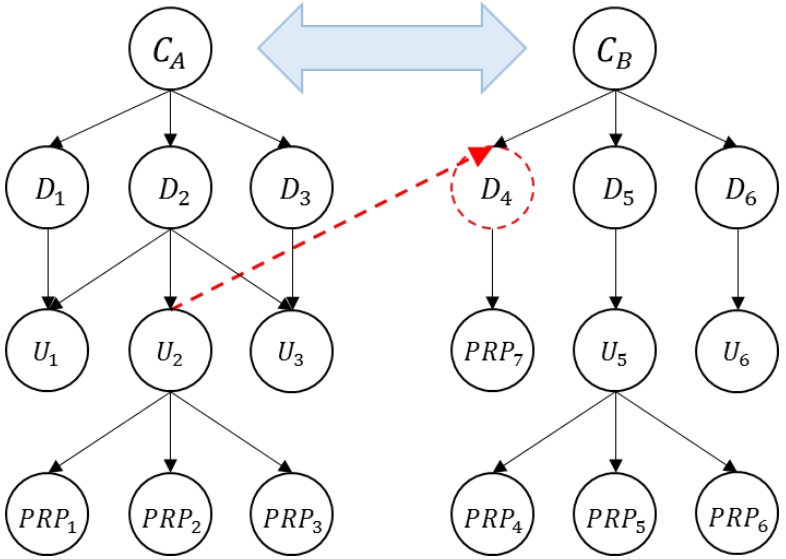


Multi Cloud Trust

- Three 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.*
  - *Cross Project Trust*
    - *Sharing project resources such as VMs.*

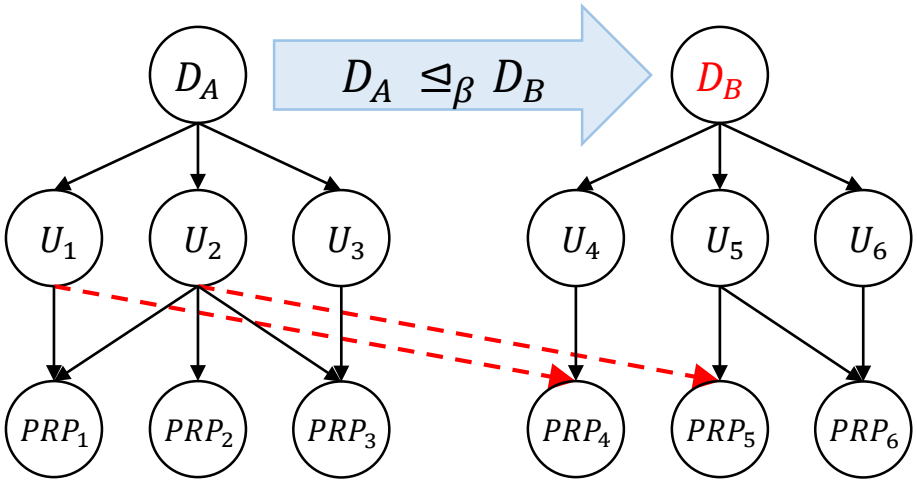
Cloud Trust

- Enables sharing cloud resources, services and domains.
  - Set of domains shared between clouds with trust type (for domain trust).
  - Sharing services by creating private domains for service allocation.
- Trust relation in Cloud Trust is Peer-to-Peer, bilateral, bidirectional, non-transitive.



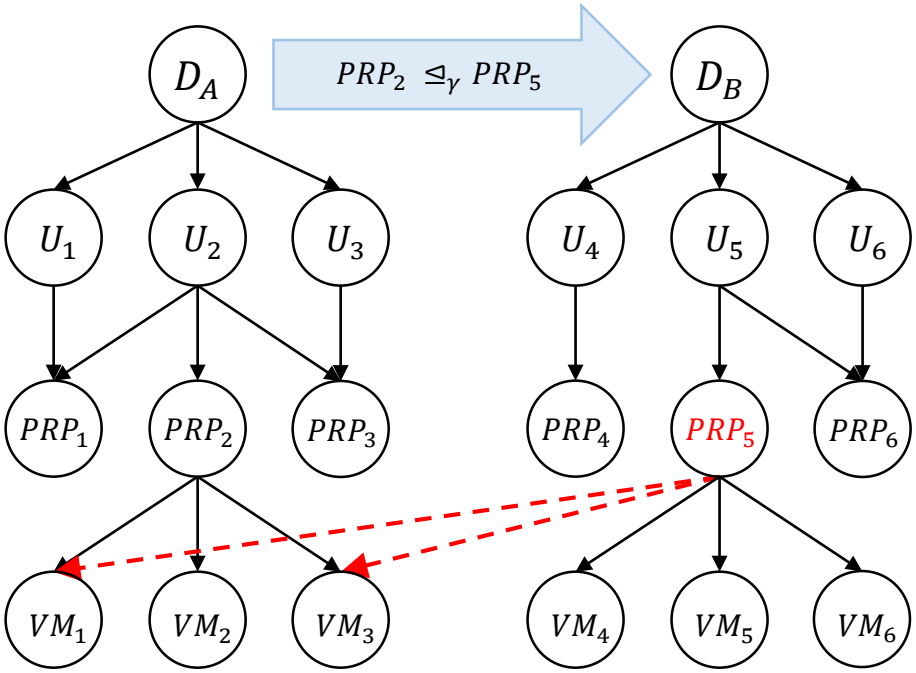
Domain Trust

- Enabling cross cloud access by assigning users to *PRPs* between trusted domains.
- Trust relations are Peer-to-Peer, unilateral, unidirectional, non-transitive.



Project Trust

- Enabling cross cloud access to service instances by assigning users to *PRPs* between trusted projects.
- Trust relations are Peer-to-Peer, unilateral, unidirectional, non-transitive.



Related Work

- RBAC extensions
  - ROBAC (collaboration ins not supported).
  - GB-RBAC (group does own users).
- Role Based delegation models
  - Delegation chains lacks dynamicity of trust in cloud federation environments.
- Multi-tenant trust models in single cloud.
  - MT-RBAC (Multi-Tenant RBAC).
  - CTTM (Cross Tenant Trust model).
  - OSAC-DT (OpenStack Access Control with Domain Trust).

Conclusion & Future Work

- Multi-cloud trust model
  - Cloud trust.
  - Domain trust.
  - Project trust.
- Trust framework & trust types
  - Four types of trust applicable to administrative realms in cloud.
- Implementation in single cloud
  - Partial implementation of domain-trust in single cloud OpenStack.
- Future Work
  - Cloud trust implementation.
  - Implementation in federated OpenStack clouds.
  - Project trust implementation.
  - Hierarchical multi-domain model.
  - Attribute based models.