Authorization and Trust in the Cloud

Prof. Ravi Sandhu

Executive Director and Endowed Chair

USECSW

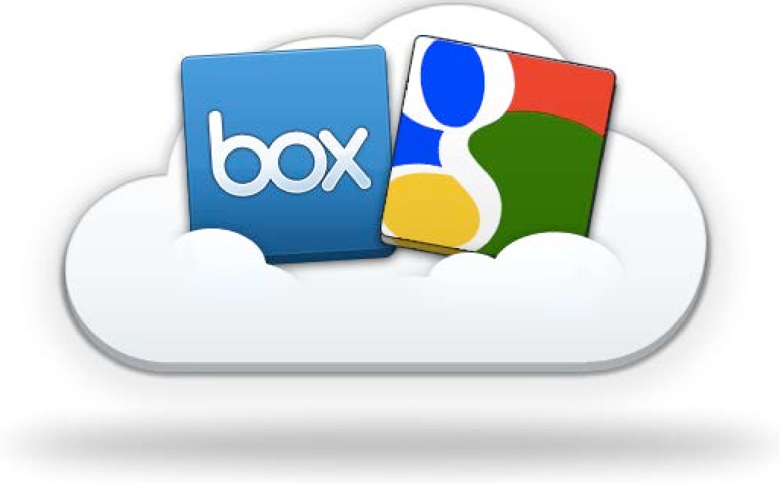
May 29, 2013

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

Joint work with
Bo Tang and Qi Li

Cloud Computing

- Shared infrastructure
  - [$$$] -----> [$|$|$]
- Multi-Tenancy
  - Virtually dedicated resources
- Drawbacks:
  - Data Locked-in
    - Collaborations can only be achieved through desktop.
    - E.g.: open files in Box with GoogleDoc.
  - How to collaborate?



Source: http://blog.box.com/2011/06/box-and-google-docs-accelerating-the-cloud-workforce/

Collaborative Access Control

- Centralized Facility
  - Chance for centralized models in distributed systems
- Agility
  - Collaboration and collaborators are temporary
- Homogeneity
  - Handful of popular brands
- Out-Sourcing Trust
  - Built-in collaboration spirit

Market Place

- Microsoft and IBM: Fine-grained data sharing in SaaS using DB schema
  - Only feasible in DB
- NASA: RBAC + OpenStack
  - Lacks ability to support collaborations
- Salesforce (Force.com): SSO + SAML
  - Focus on authentication
  - Heavy management of certificates

Source: http://msdn.microsoft.com/en-us/library/aa479086.aspx
http://nebula.nasa.gov/blog/2010/06/03/nebulas-implementation-role-based-access-control-rbac/
http://wiki.developerforce.com/page/Single_Sign-On_with_SAML_on_Force.com

Literature

Problem:
semantic mismatch

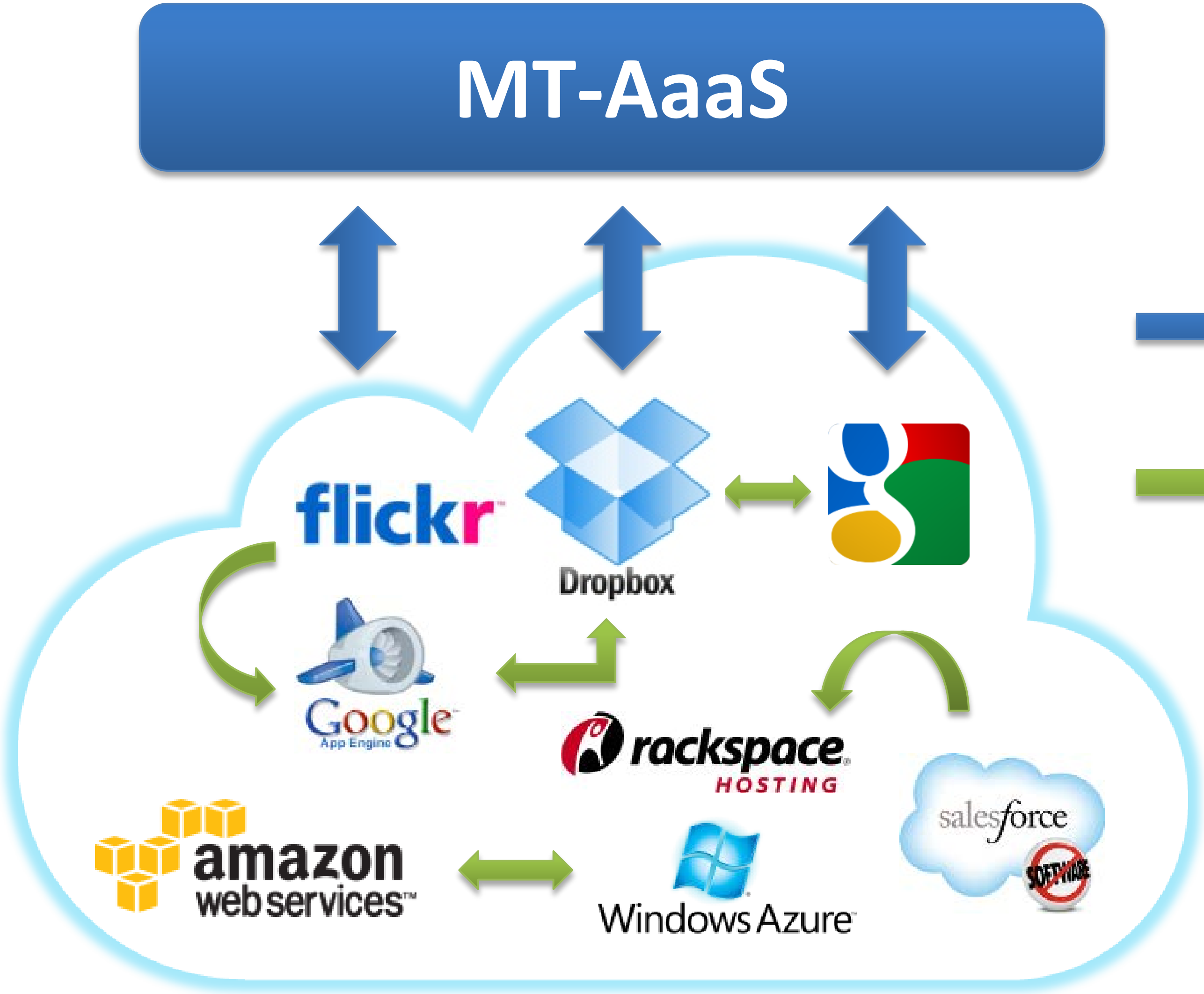
- RBAC
  - CBAC, GB-RBAC, ROBAC
  - Require central authority managing collaborations
- Delegation Models
  - dRBAC and PBDM
  - Lacks agility (which the cloud requires)
- Grids
  - CAS, VOMS, PERMIS
  - Absence of centralized facility and homogeneous architecture (which the cloud has)

Literature (Contd.)

- Role-based Trust
  - RT, Traust, RMTN AND RAMARS_TM
  - Calero et al: towards a multi-tenant authorization system for cloud services
    - Implementation layer PoC
    - Open for extensions in trust models
  - Suits the cloud (out-sourcing trust)

Challenge:
trust relation

Multi-Tenant Authorization as a Service (MT-AaaS)

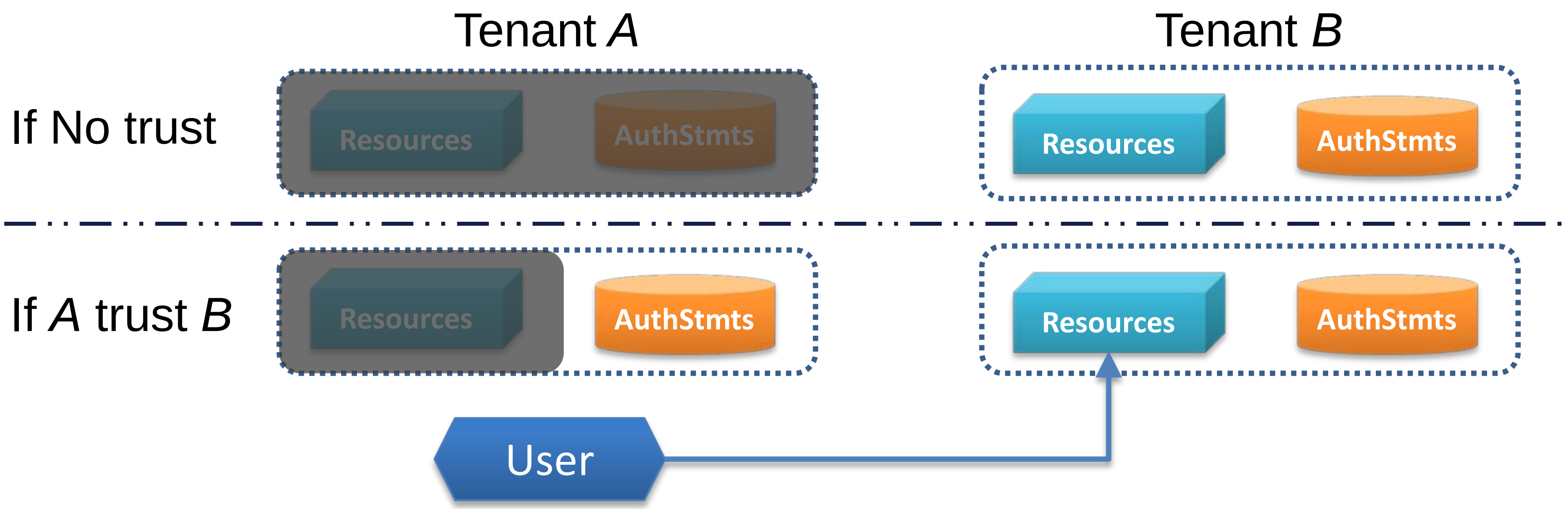


Multi-Tenant Access Control

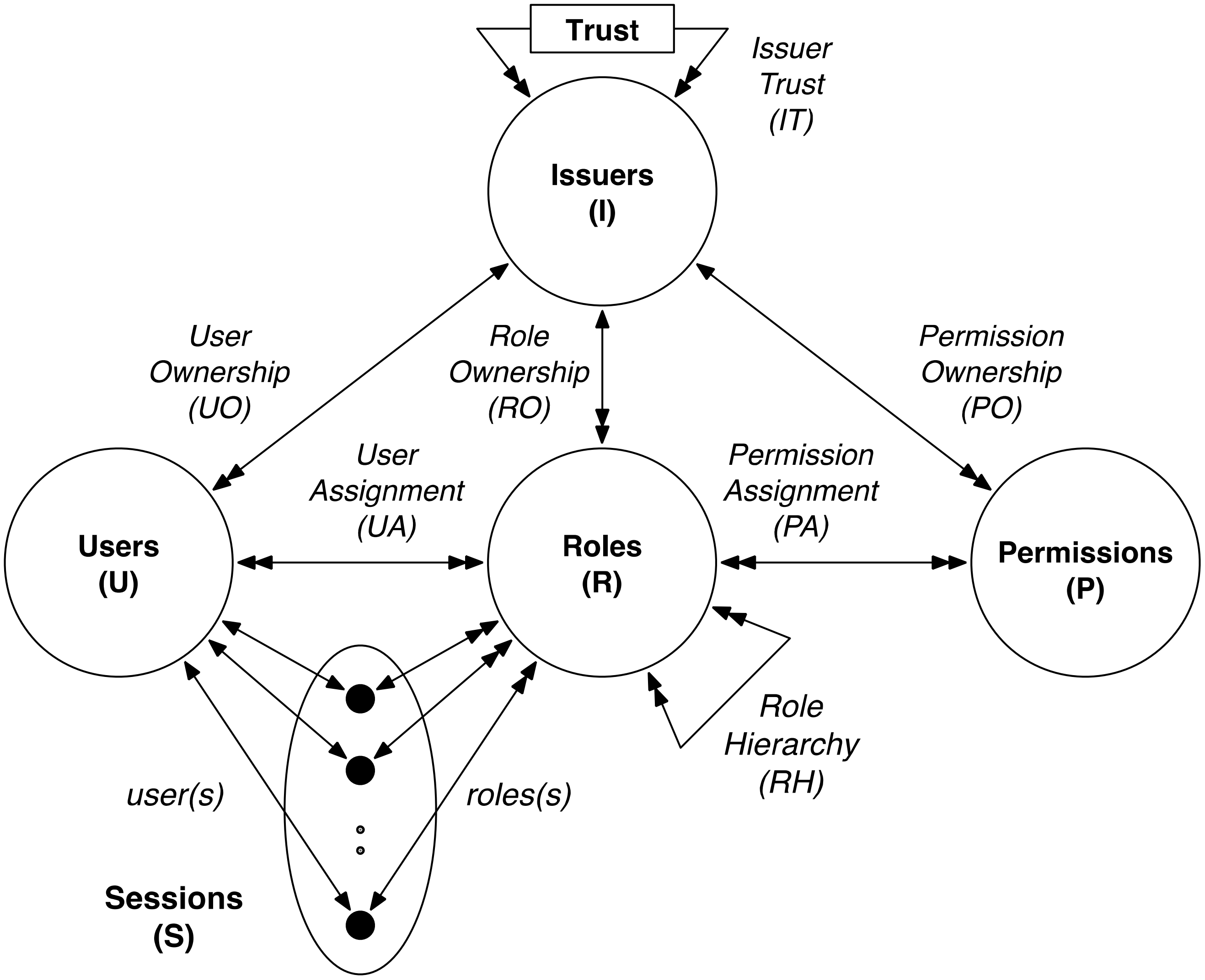
Cross-Tenant Access

MTAS Trust Model

- If A trusts B then B (resource owner) can assign
  - B's permissions to A's roles; and
  - B's roles as junior roles to A's roles.

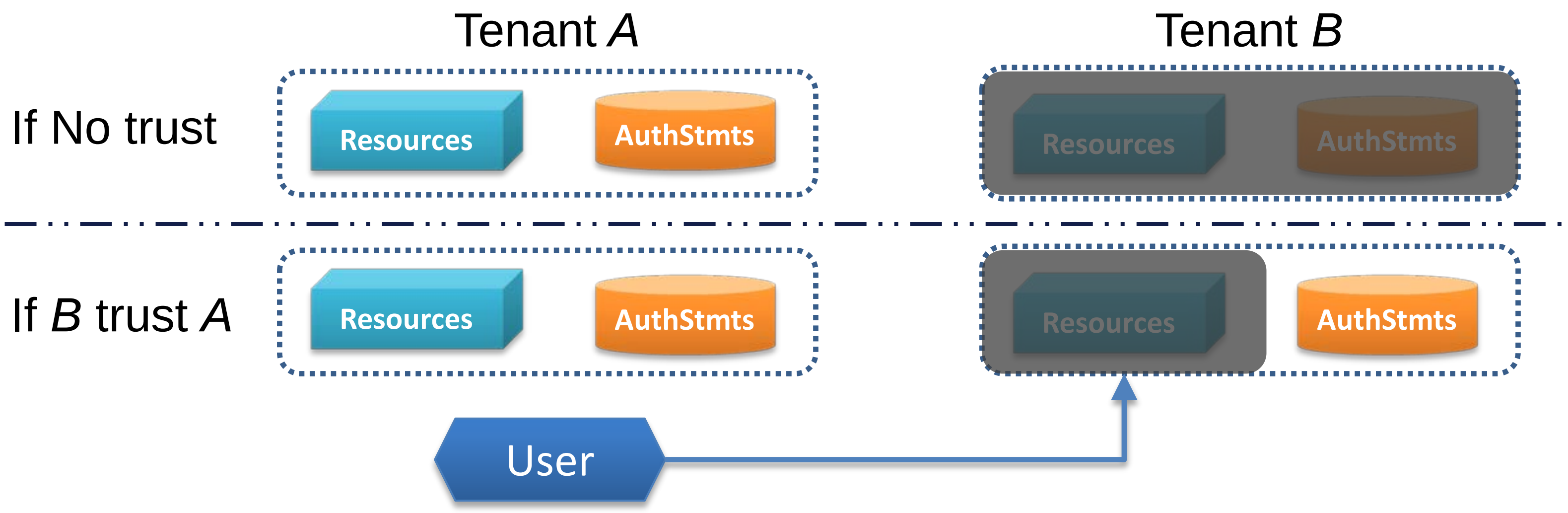


MTAS

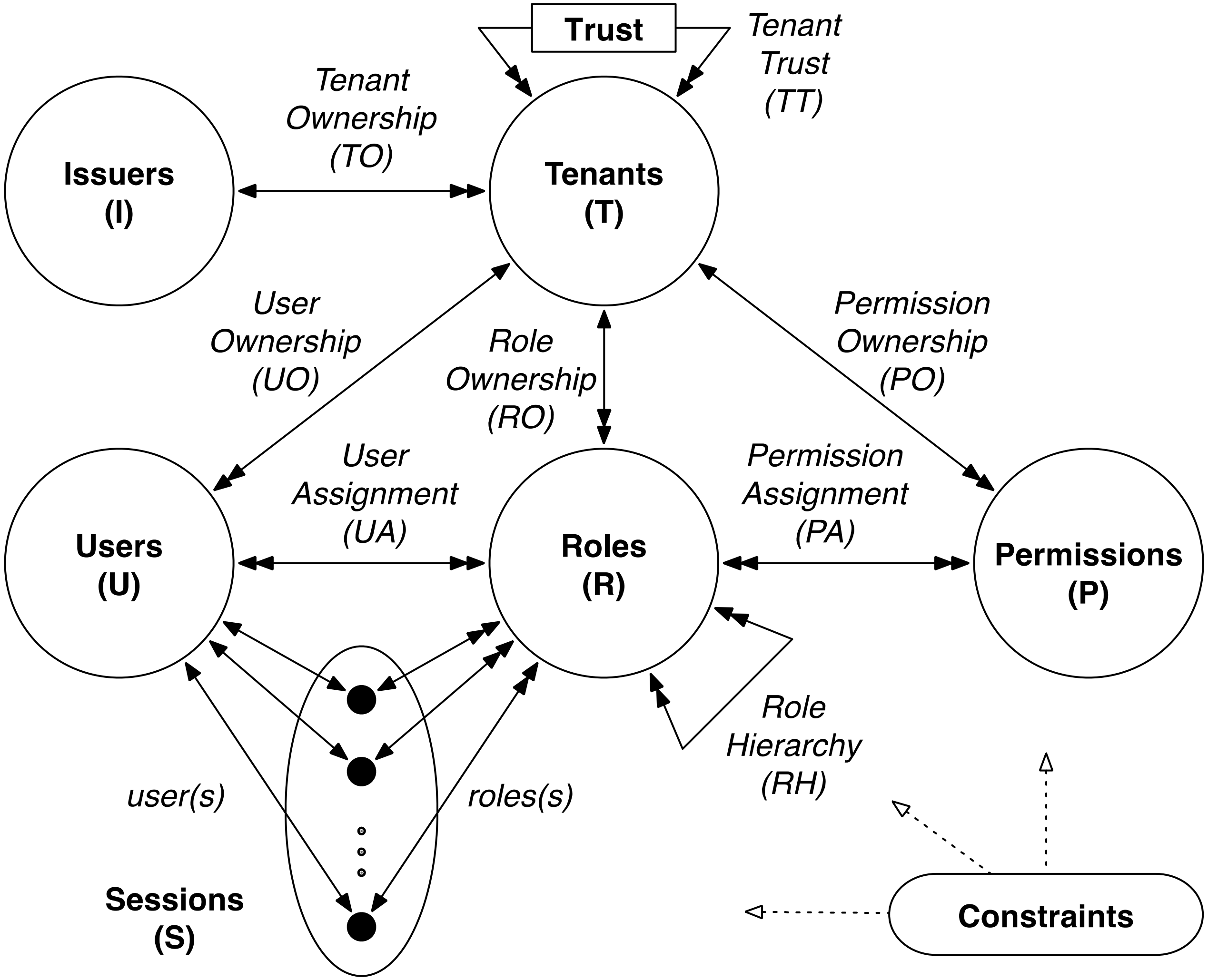

Trust
Issuer Trust (IT)
Issuers (I)
User Ownership (UO)
Role Ownership (RO)
Permission Ownership (PO)
User Assignment (UA)
Permission Assignment (PA)
Users (U)
Roles (R)
Permissions (P)
Role Hierarchy (RH)
user(s)
roles(s)
Sessions (S)

MT-RBAC Trust Model

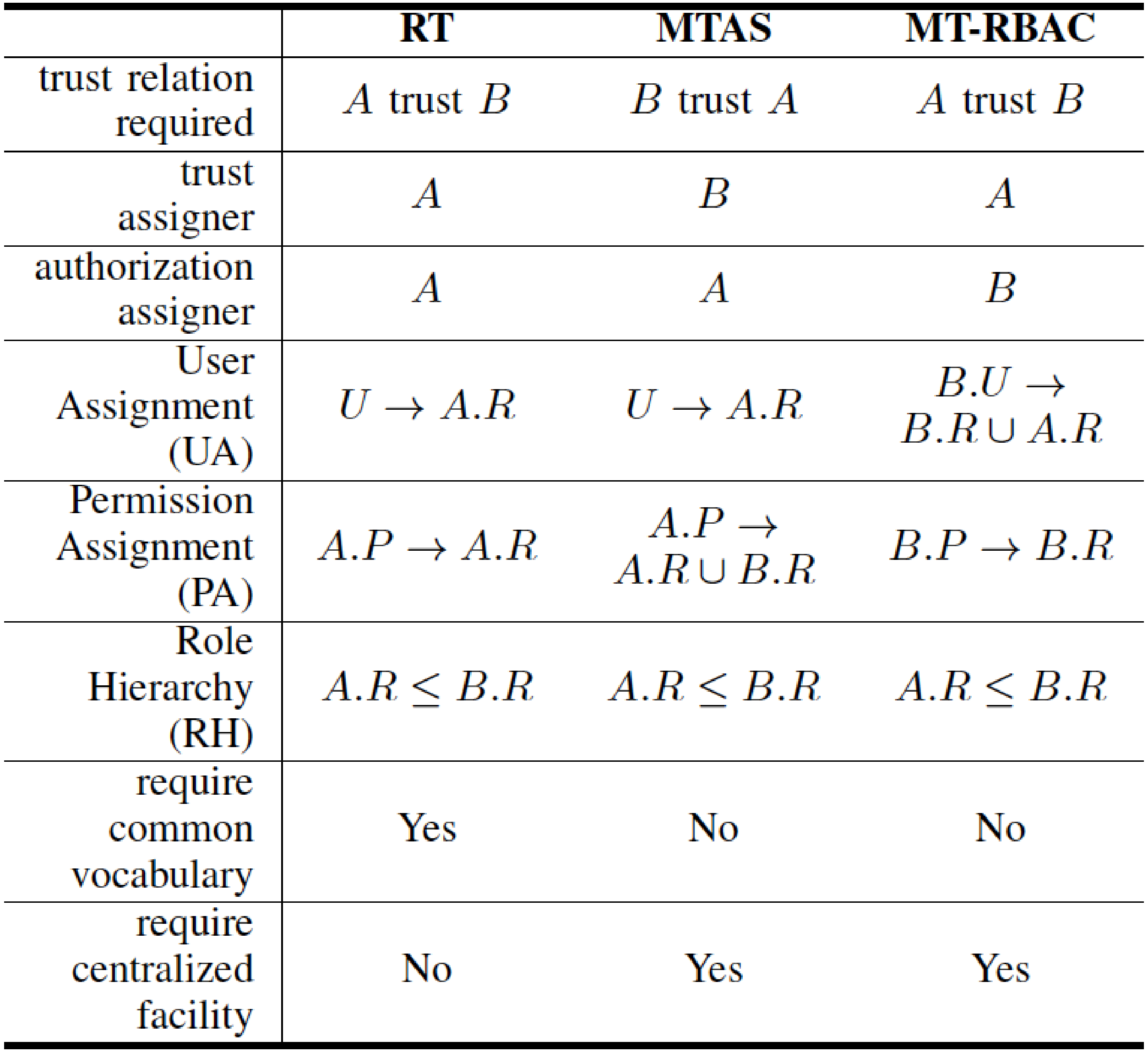
- If B (resource owner) trusts A then A can assign
  - B's permissions to A's roles; and
  - B's roles as junior roles to A's roles.



MT-RBAC


Trust
Tenant Trust (TT)
Tenant Ownership (TO)
Issuers (I)
Tenants (T)
User Ownership (UO)
Role Ownership (RO)
Permission Ownership (PO)
User Assignment (UA)
Permission Assignment (PA)
Users (U)
Roles (R)
Permissions (P)
Role Hierarchy (RH)
user(s)
roles(s)
Sessions (S)
Constraints

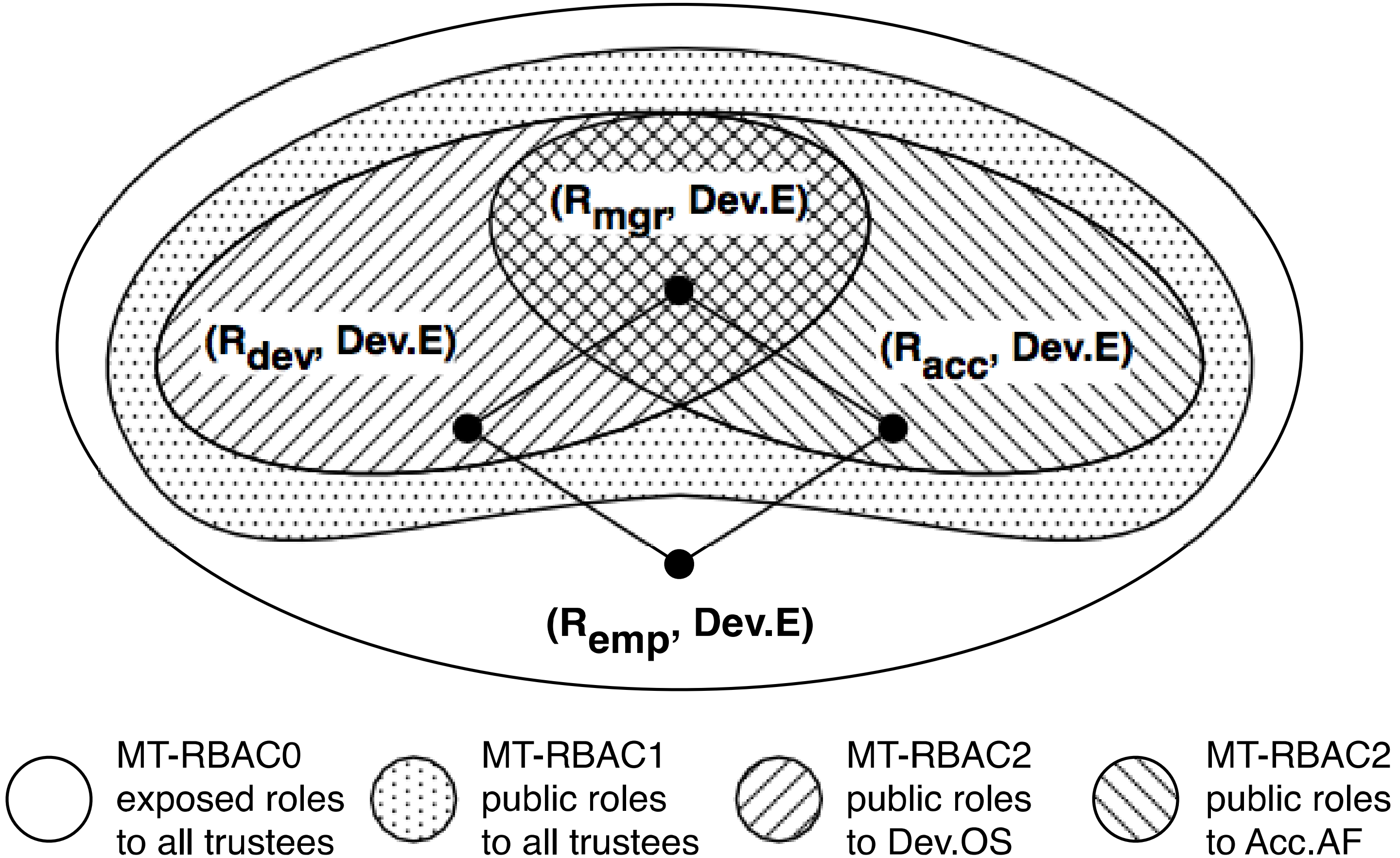
Trust Model Comparison



	RT	MTAS	MT-RBAC
trust relation required	A trust B	B trust A	A trust B
trust assigner	A	B	A
authorization assigner	A	A	B
User Assignment (UA)	$U \to A.R$	$U \to A.R$	$B.U \to B.R \cup A.R$
Permission Assignment (PA)	$A.P \to A.R$	$A.P \to A.R \cup B.R$	$B.P \to B.R$
Role Hierarchy (RH)	$A.R \leq B.R$	$A.R \leq B.R$	$A.R \leq B.R$
require common vocabulary	Yes	No	No
require centralized facility	No	Yes	Yes

A: resource owner
B: resource requester

Finer-grained Trust Models



○ MT-RBAC0 exposed roles to all trustees

░ MT-RBAC1 public roles to all trustees

▨ MT-RBAC2 public roles to Dev.OS

▧ MT-RBAC2 public roles to Acc.AF

Constraints

- Role Cycles: lead to implicit role upgrades in the role hierarchy.
- SoD: conflict of duties
  - Tenant-level
    - E.g.: SOX compliance companies may not hire same the same company for both consulting and auditing.
  - Role-level
    - Across tenants
- Chinese Wall: conflict of interests among tenants.

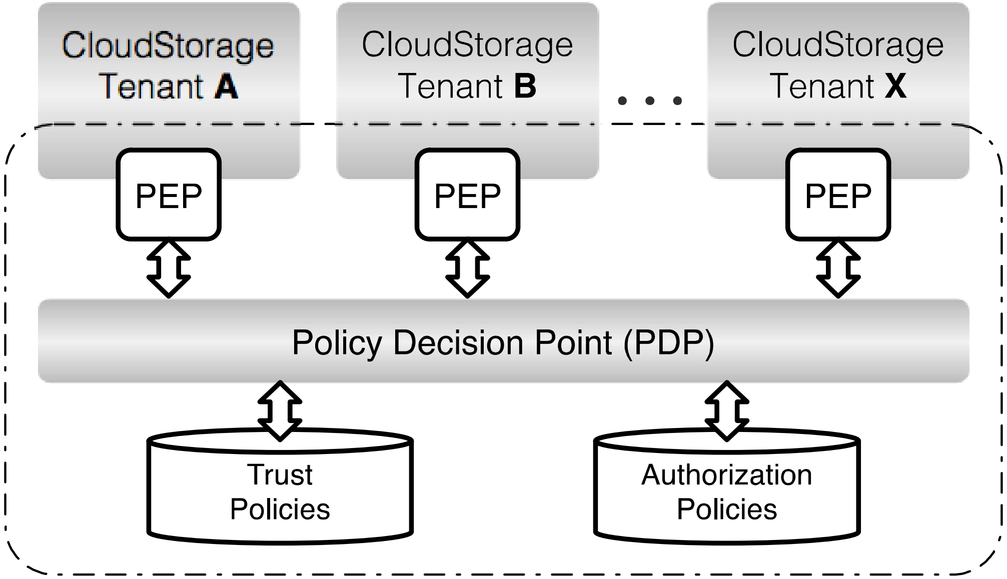
Collaboration Admin.

- Decentralized management
  - Trusters maintain the trust relation
- Immediately effective when trust changes
  - Automatic revocation of cross-tenant accesses
  - Agility in cloud environments

PROTOTYPE AND EVALUATION

- Cloud Service
  - CloudStorage: an open source web based cloud storage and sharing system.

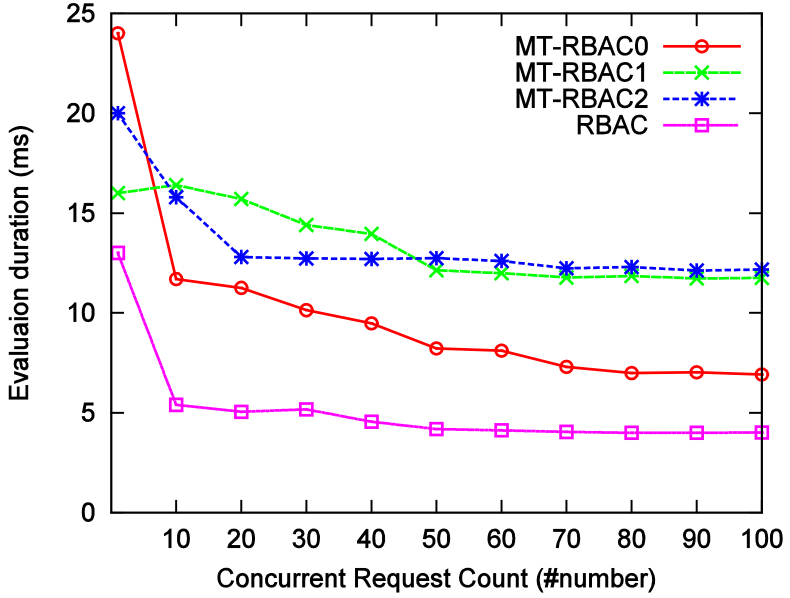
- Authorization Service
  - Centralized PDP
  - Distributed PEP



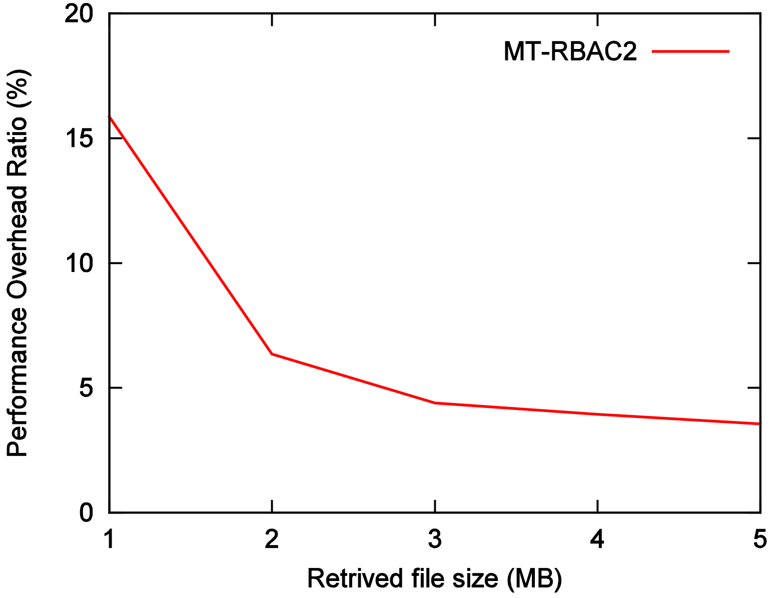
Authorization as a Service

Evaluation: Performance

- MT-RBAC vs RBAC
  - More policy references incur more decision time
- MT-RBAC$_2$ introduces 6.82% overhead in average.



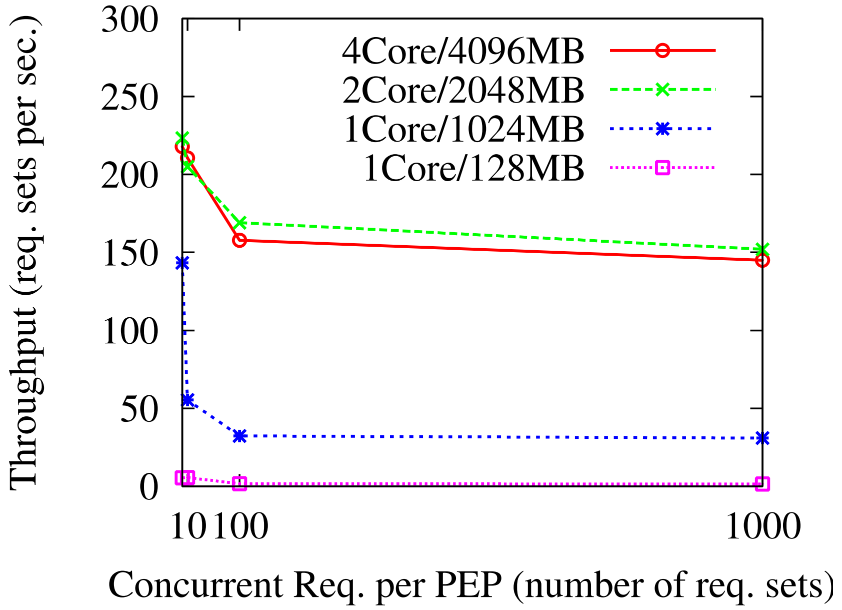
Performance comparison at PDP



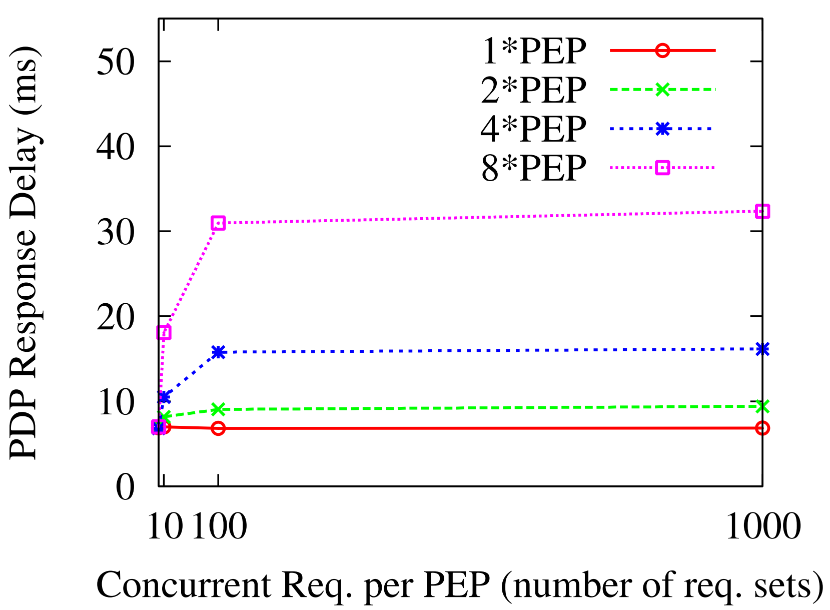
File retrieval delay ratio introduced

Evaluation: Scalability

- Scalable by either
  - Enhancing PDP capability; or
  - Increasing PEP amount.



Different Flavors of PDP



Different Numbers of PEP

Summary

- Collaboration needs in the cloud eco-system
- Novel service model: MT-AaaS
- Proposed formal models
  - MTAS
  - MT-RBAC
  - Constraints and administration
- Prototype and evaluation
  - Performance overhead ≤ 6.82%
  - Scalable in the cloud
- Trust Model Comparison

Future Work

- OpenStack Keystone extensions
- Integrate trust into ABAC: MT-ABAC
- Unified trust framework for the cloud

- Bo Tang, Ravi Sandhu and Qi Li. Multi-Tenancy Authorization Models for Collaborative Cloud Services. CTS, 2013.
- Bo Tang, Qi Li and Ravi Sandhu. A Multi-Tenant RBAC Model for Collaborative Cloud Services. PST 2013.