IIT KHARAGPUR

NPTEL ONLINE
CERTIFICATION COURSES

CLOUD COMPUTING

CLOUD SECURITY IV

Security Issues in Collaborative SaaS Cloud

PROF. SOUMYA K. GHOSH

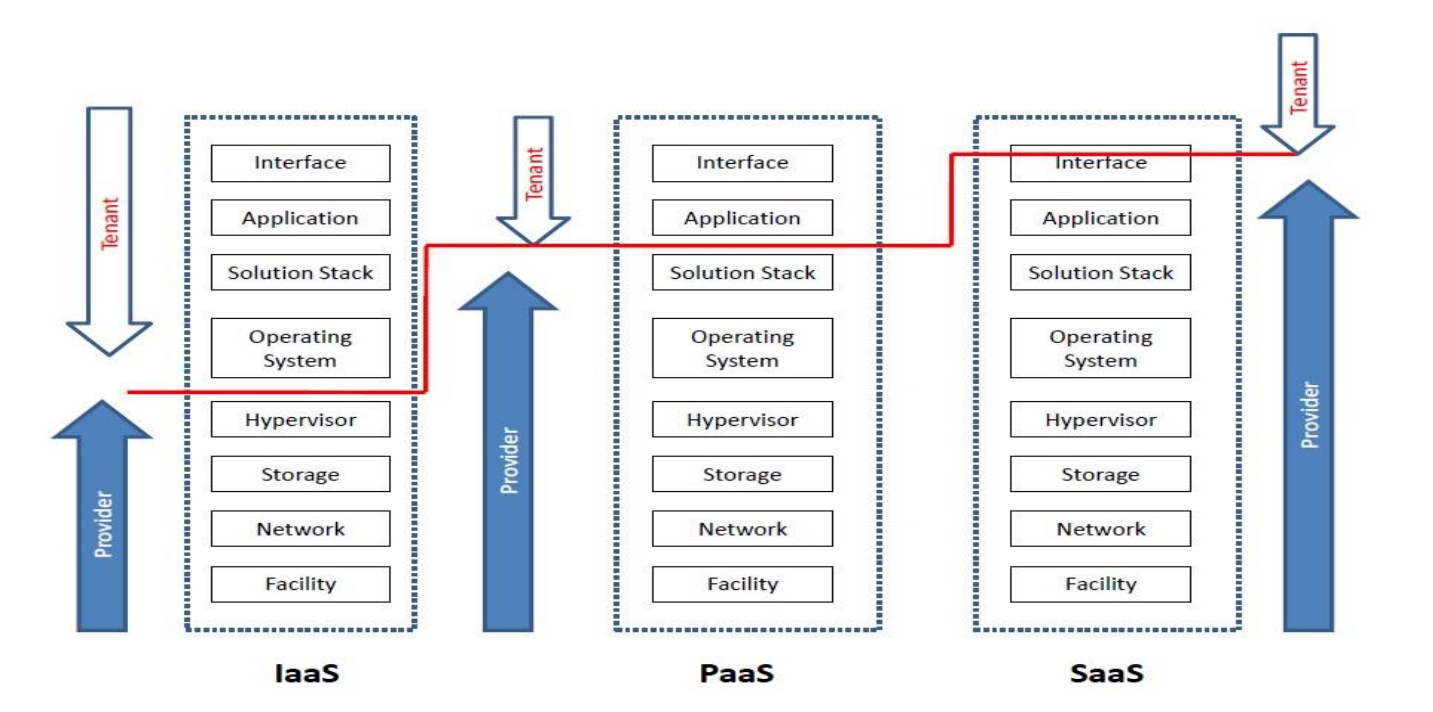
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

IIT KHARAGPUR

Security Issues in Cloud Computing

- Unique security features:
  - Co-tenancy
  - Lack of control on outsourced data and application
- General concerns among cloud customers [Liu'11]:
  - Inadequate policies and practices
  - Insufficient security controls
- Customers use cloud services to serve their clients
- Need to establish trust relationships
- Beneficial to both stakeholders

Security Responsibilities



SaaS Cloud-based Collaboration

- APIs for sharing resources/information
  - Service consumer(customers): human users, applications, organizations/domains, etc.
  - Service provider: SaaS cloud vendor
- SaaS cloud-centric collaboration: valuable and essential
  - Data sharing
  - Problems handled: inter-disciplinary approach
- Common concerns:
  - Integrity of data, shared across multiple users, may be compromised
  - Choosing an “ideal” vendor

SaaS Cloud-based Collaboration

- Types of collaboration in multi-domain/cloud systems:
  - Tightly-coupled or federated
  - Loosely-coupled
- Challenges: securing loosely-coupled collaborations in cloud environment
  - Security mechanisms: mainly proposed for tightly-coupled systems
  - Restrictions in the existing authentication/authorization mechanisms in clouds

Motivations and Challenges

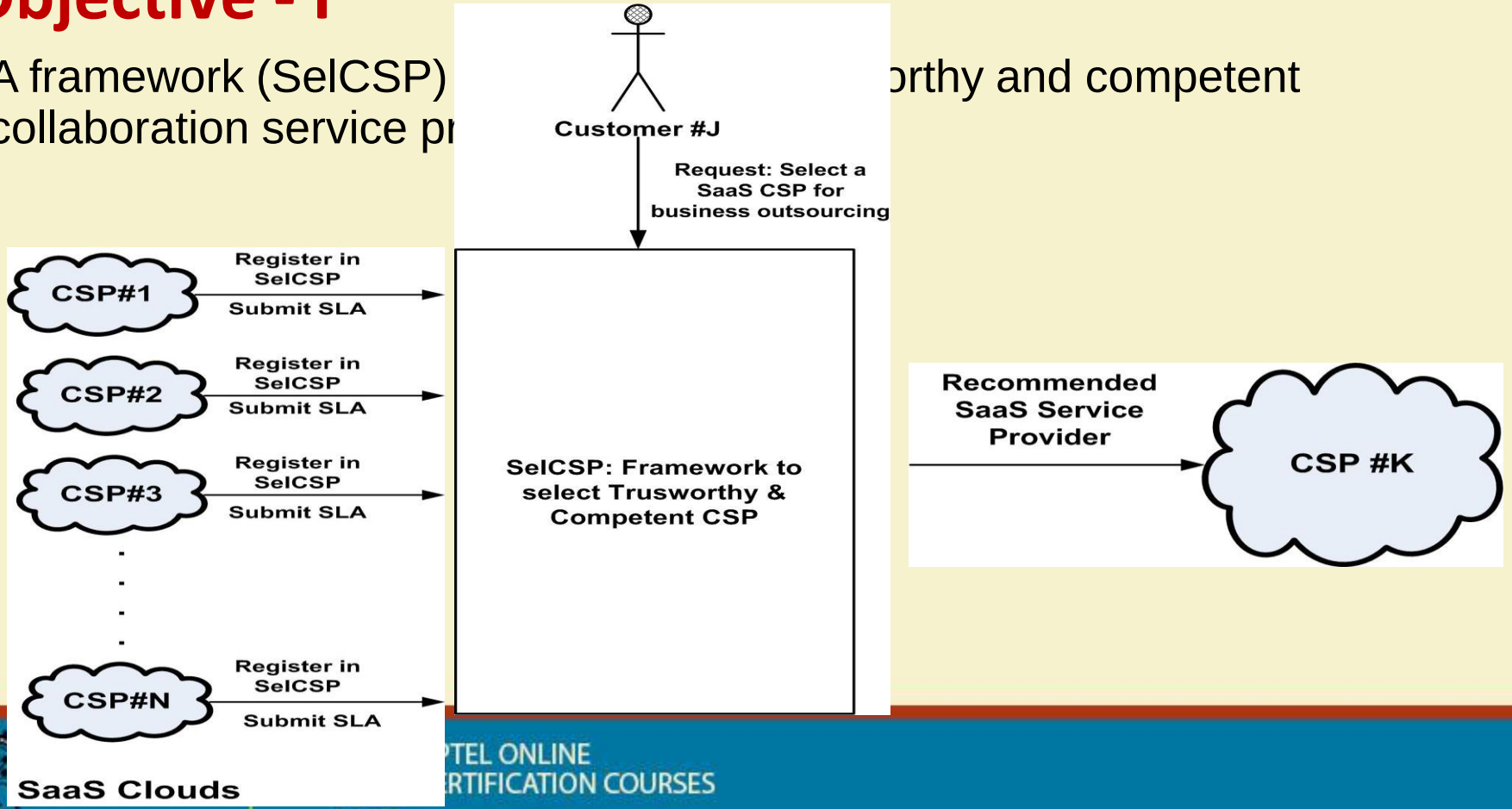
- SaaS cloud delivery model: maximum lack of control
- No active data streams/audit trails/outage report
  - **Security**: Major concern in the usage of cloud services
- Broad scope: *address security issues in SaaS clouds*
- Cloud marketplace: rapid growth due to recent advancements
- Availability of multiple service providers
  - Choosing SPs from SLA guarantees: not reliable
    - Inconsistency in service level guarantees
    - Non-standard clauses and technical specifications
- Focus: *selecting an "ideal" SaaS cloud provider and address the security issues*

Motivations and Challenges

- Online collaboration: popular
- Security issue: unauthorized disclosure of sensitive information
  - Focus: *selecting an ideal SaaS cloud provider and secure the collaboration service offered by it*
- Relevance in today's context: *loosely-coupled collaboration*
  - Dynamic data/information sharing
- Final goal (problem statement): *selecting an ideal SaaS cloud provider and securing the loosely-coupled collaboration in its environment*

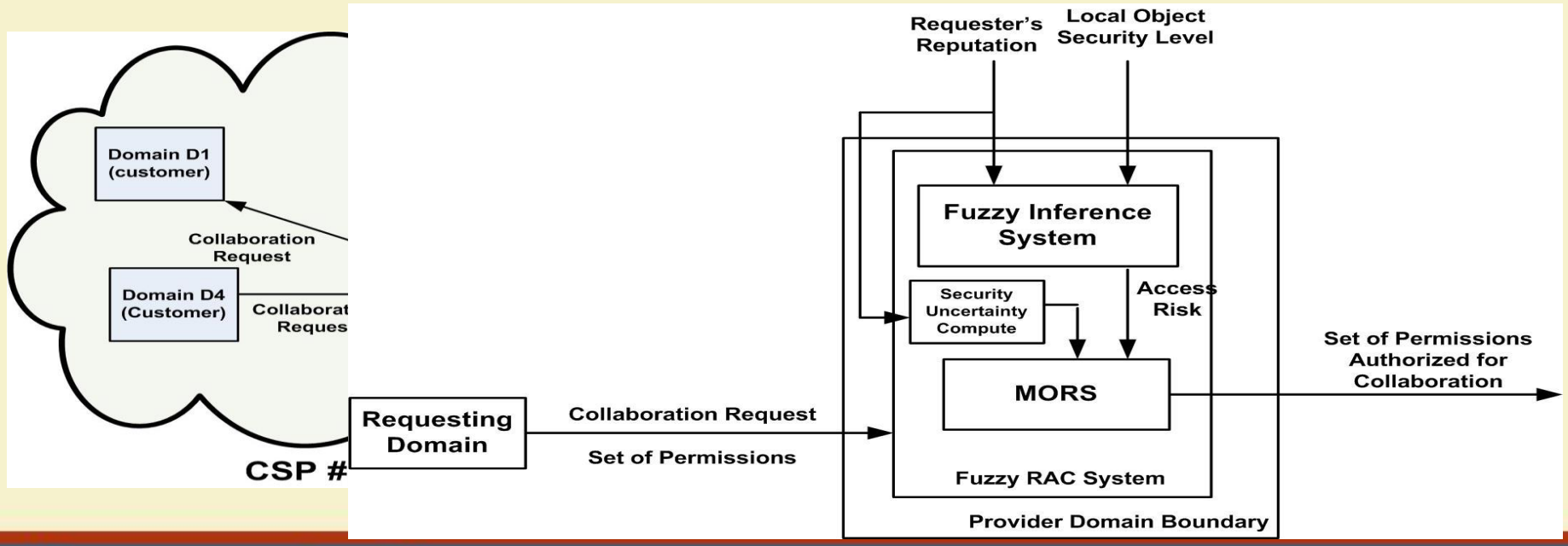
Objective - I

A framework (SelCSP) orthy and competent collaboration service pr



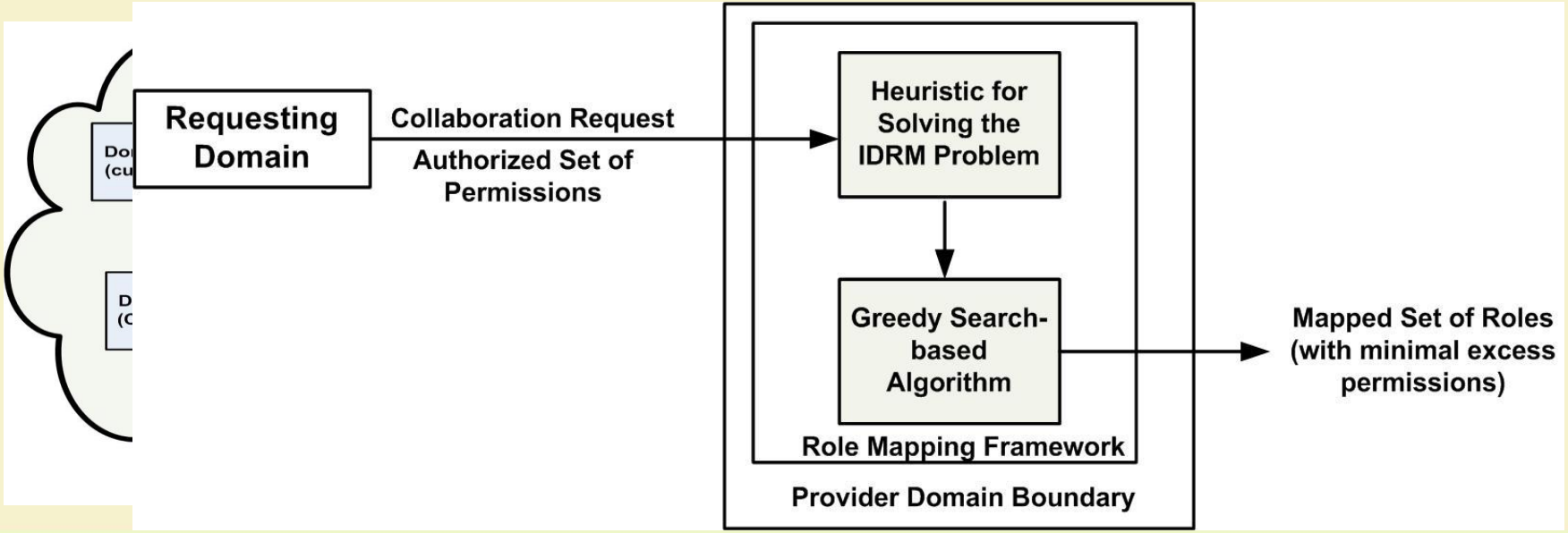
Objective - II

Select requests (for accessing local resources) from anonymous users, such that both access risk and security uncertainty due to information sharing are kept low.

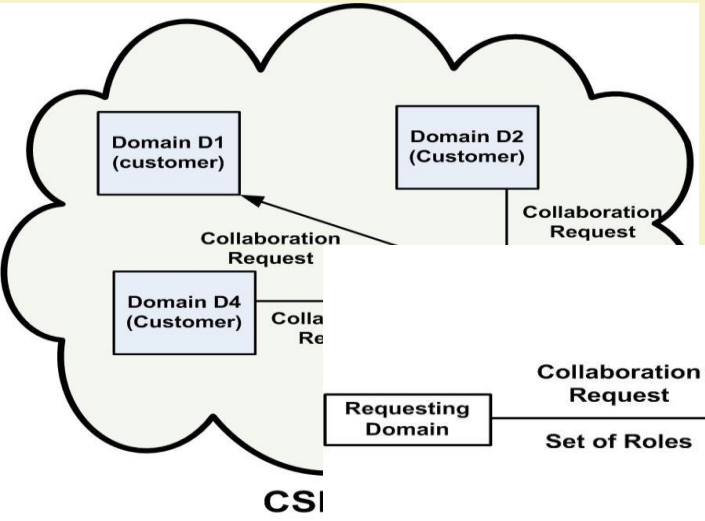


Objective - III

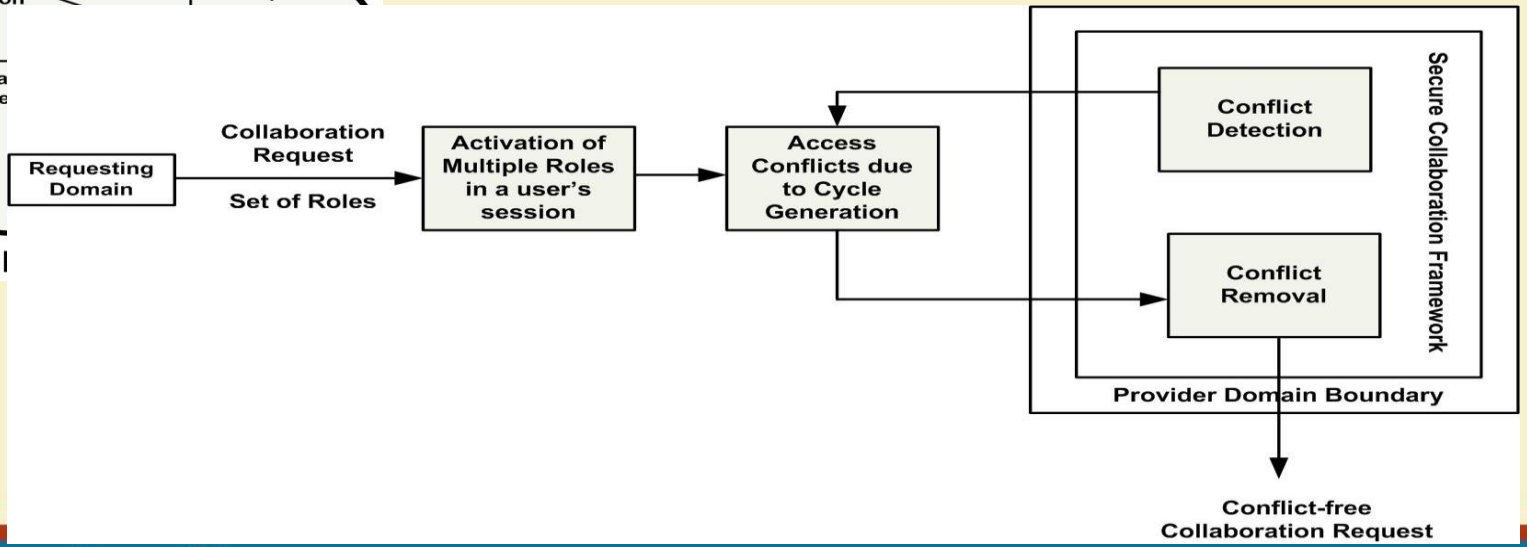
Formulate a heuristic for solving the IDRM problem, such that minimal excess privilege is granted



Objective - IV



A distributed secure collaboration framework, which uses only local information to dynamically detect and remove access conflicts.



Selection of Trustworthy and Competent SaaS Cloud Provider for Collaboration

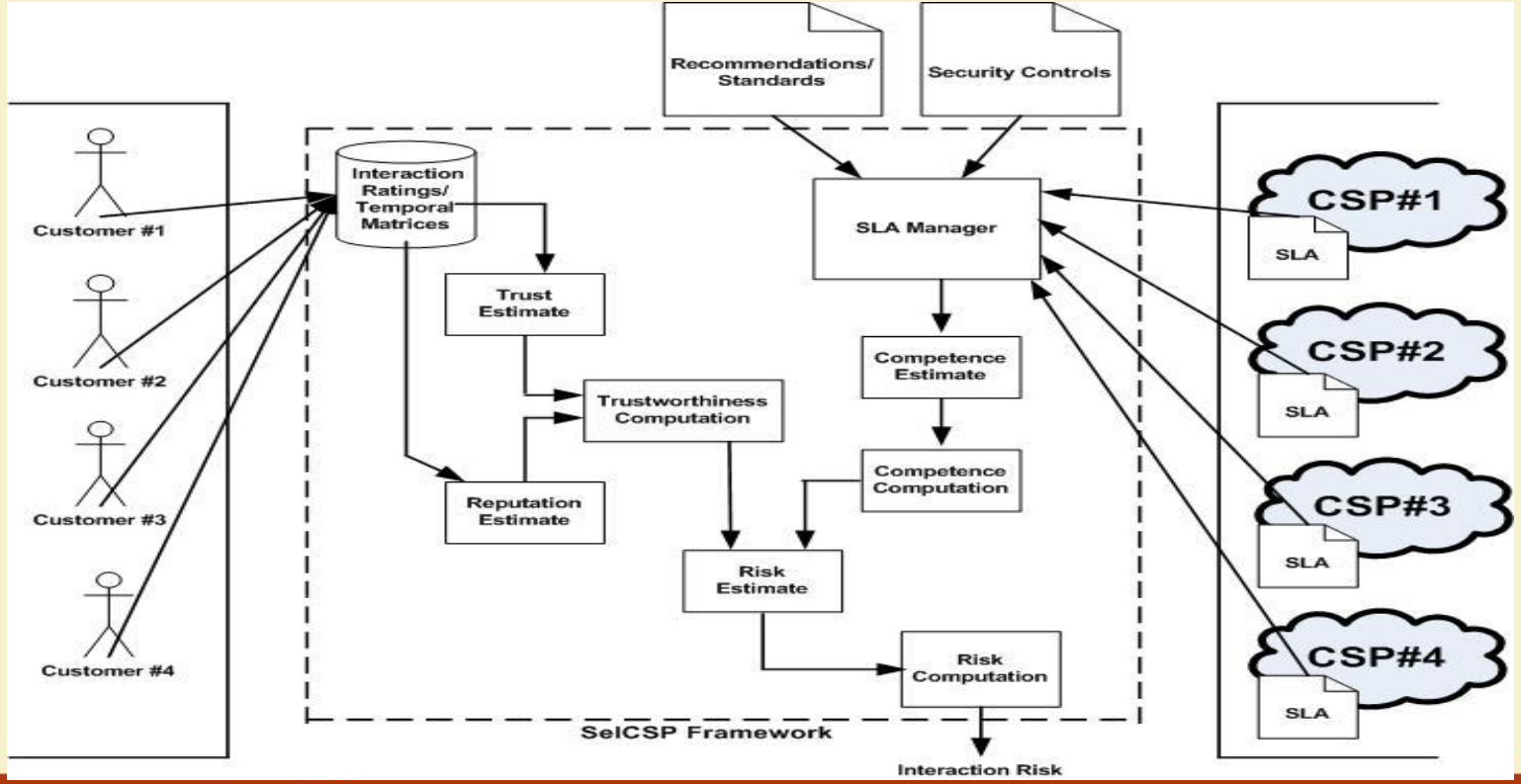
Trust Models in Cloud

- Challenges
  - Most of the reported works have not presented mathematical formulation or validation of their trust and risk models
  - Web service selection [Liu'04][Garg'13] based on QoS and trust are available
    - Select resources (e.g. services, products, etc.) by modeling their performance
- **Objective: Model trust/reputation/competence of service provider**

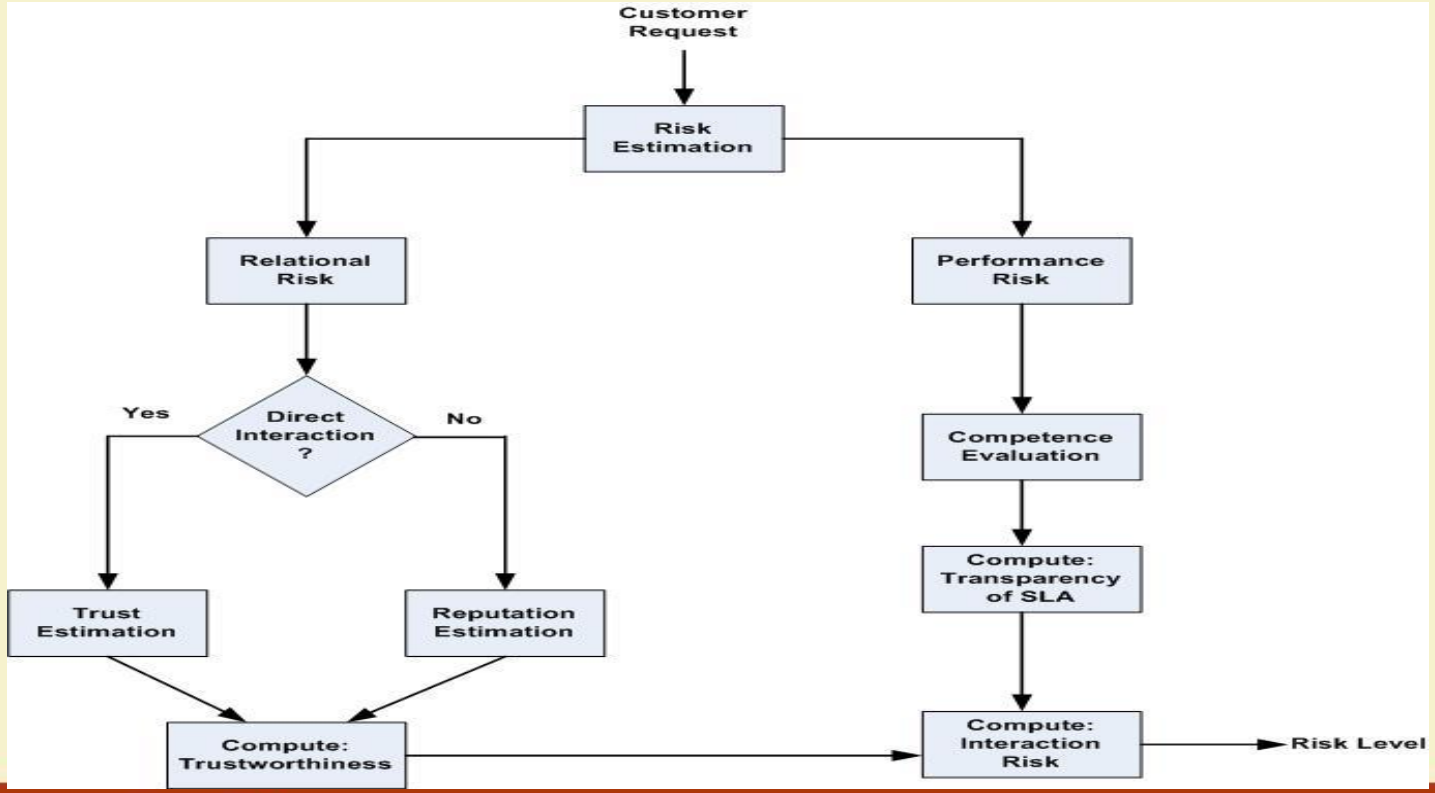
Service Level Agreement (SLA) for Clouds

- Challenges:
  - Majority of the cloud providers guarantee “availability” of services
  - Consumers not only demand availability guarantee but also other performance related assurances which are equally business critical
  - Present day cloud SLAs contain non-standard clauses regarding assurances and compensations following a violation[Habib’11]
- Objective: **Establish a standard set of parameters for cloud SLAs, since it reduces the perception of risk in outsourced services**

SelCSP Framework



SelCSP Framework - Overview

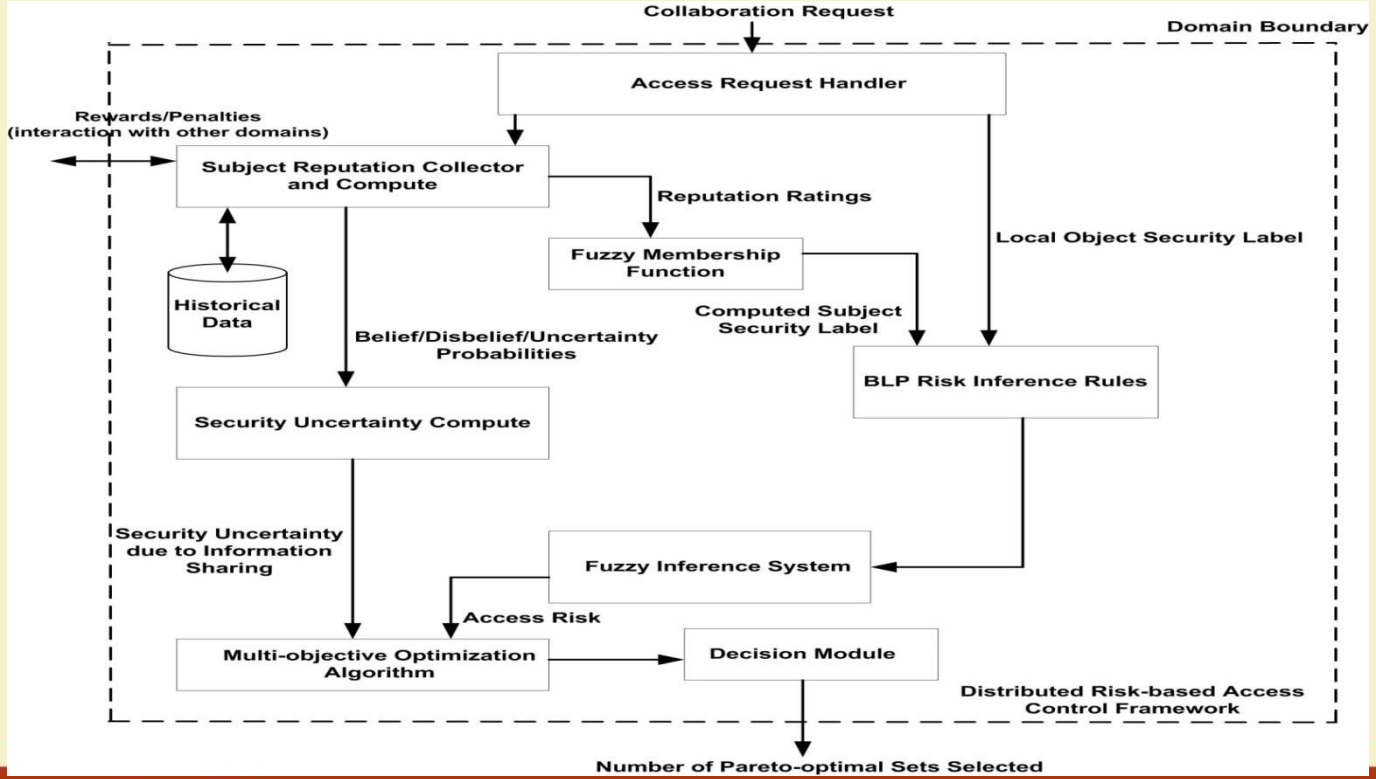


Recommending Access Requests from Anonymous Users for Authorization

Risk-based Access Control (RAC)

- RAC: Gives access to subjects even though they lack proper permissions
  - Goal: balance between *access risk* and *security uncertainty due to information sharing*
  - Flexible compared to binary MLS
- Challenges
  - Computing security uncertainty: not addressed
  - Authorization in existing RAC system: based on risk threshold and operational need.
    - Operational need: not quantified.
    - Discards many requests which potentially maximizes information sharing

Distributed RAC using Fuzzy Inference System

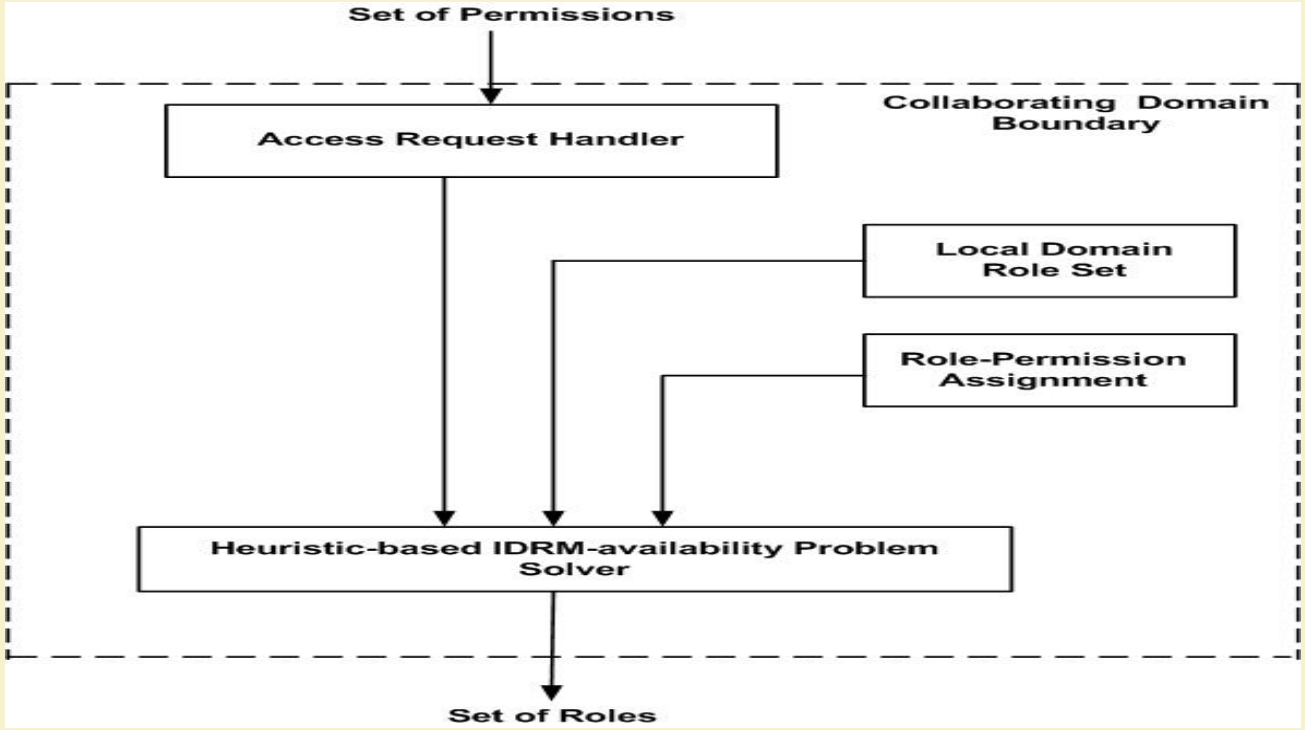


Mapping of Authorized Permissions into Local Roles

Inter-Domain Role Mapping (IDRM)

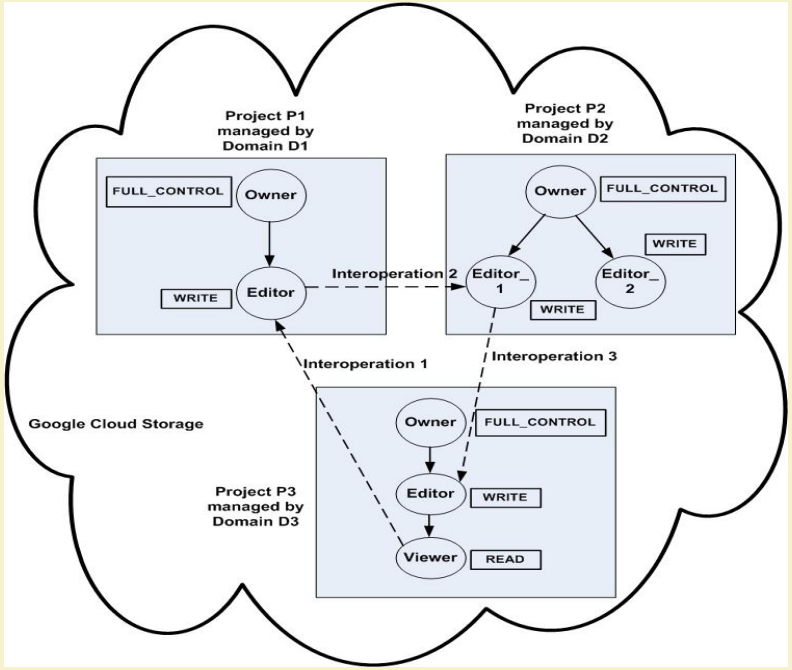
- Finds a minimal set of role which encompasses the requested permission set.
  - No polynomial time solution
  - Greedy search-based heuristics: suboptimal solutions
- Challenges:
  - There may exist multiple minimal role sets
  - There may not exist any role set which exactly maps all permissions
- Two variants of IDRM proposed: *IDRM-safety*, *IDRM-availability*
- Objective: formulate a novel heuristic to generate better solution for the IDRM-availability problem.
- Minimize the number of additional permissions

Distributed Role Mapping Framework

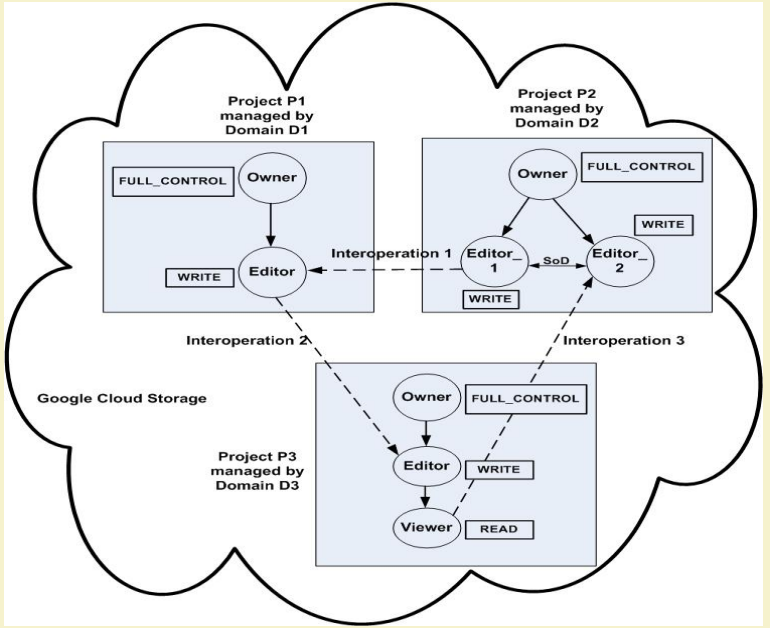


Dynamic Detection and Removal of Access Policy Conflicts

Access Conflicts



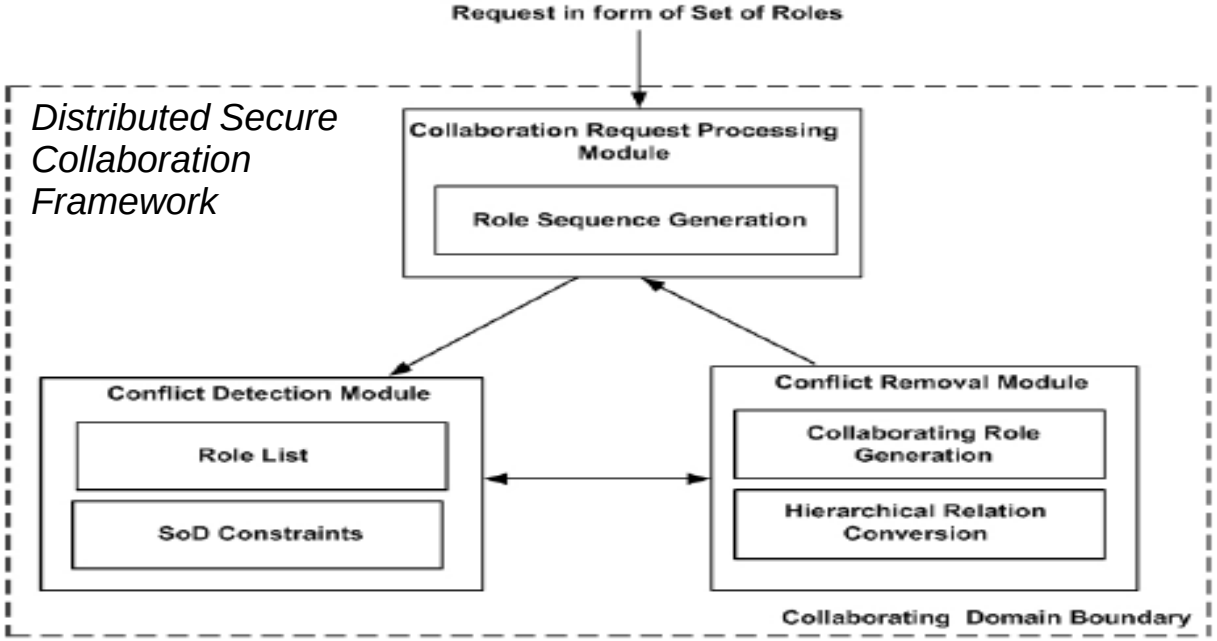
Cyclic Inheritance Conflict



Violation of SoD Constraint

Objective

- Dynamic detection of conflicts to address **security** issue
- Removal of conflicts to address **availability** issue
- Proposed: distributed secure collaboration framework



- Role Sequence Generation
  - Interoperation request: pair of *entry* (from requesting domain), *exit* (from providing domain) roles
  - Role sequence: ordered succession of entry and exit roles
  - Role cycle:
    - Safe role cycle
    - **Unsafe role cycle**

Conflict Detection

- Detection of inheritance conflict
  - Necessary condition: at least one exit role
  - Sufficient condition: current entry role is senior to at least one exit role
- Detection of SoD constraint violation
  - Necessary condition: at least one exit role
  - Sufficient condition: current entry role and at least one exit role forms *conflicting pair*

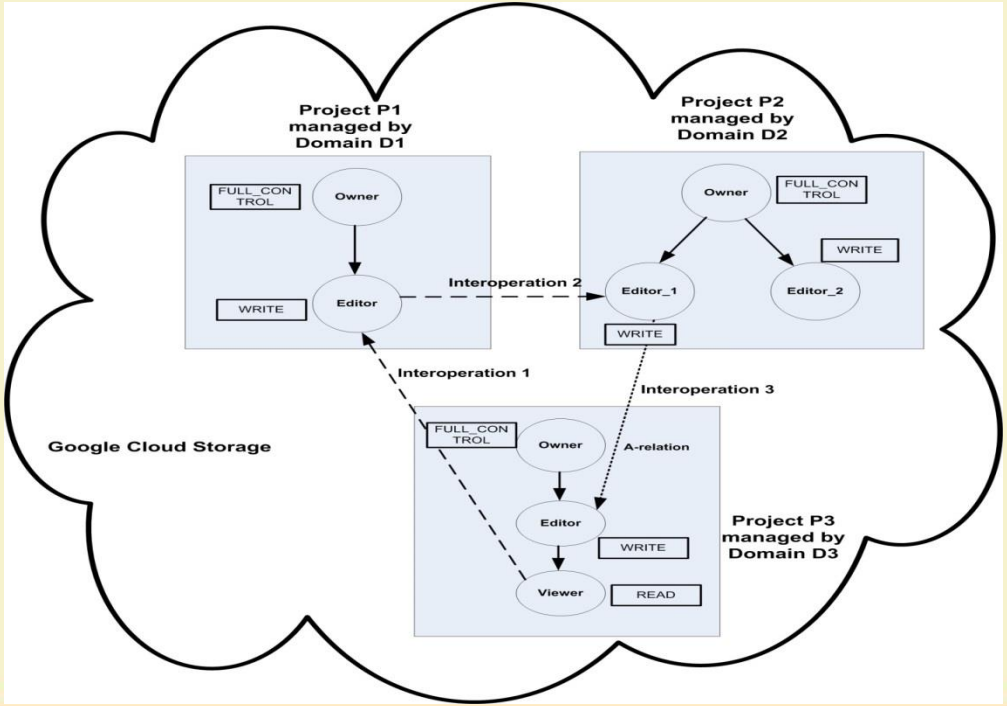
Conflict Removal

Cyclic Inheritance

- Two cases arise:
  - Exactly matched role set exists
    - RBAC hybrid hierarchy
      - *I-hierarchy, A-hierarchy, IA-hierarchy*
    - Replacing *IA-relation* with *A-relation* between exit role in previous domain and entry role in current domain
  - No-exactly matched role set exists
    - Introduce a virtual role

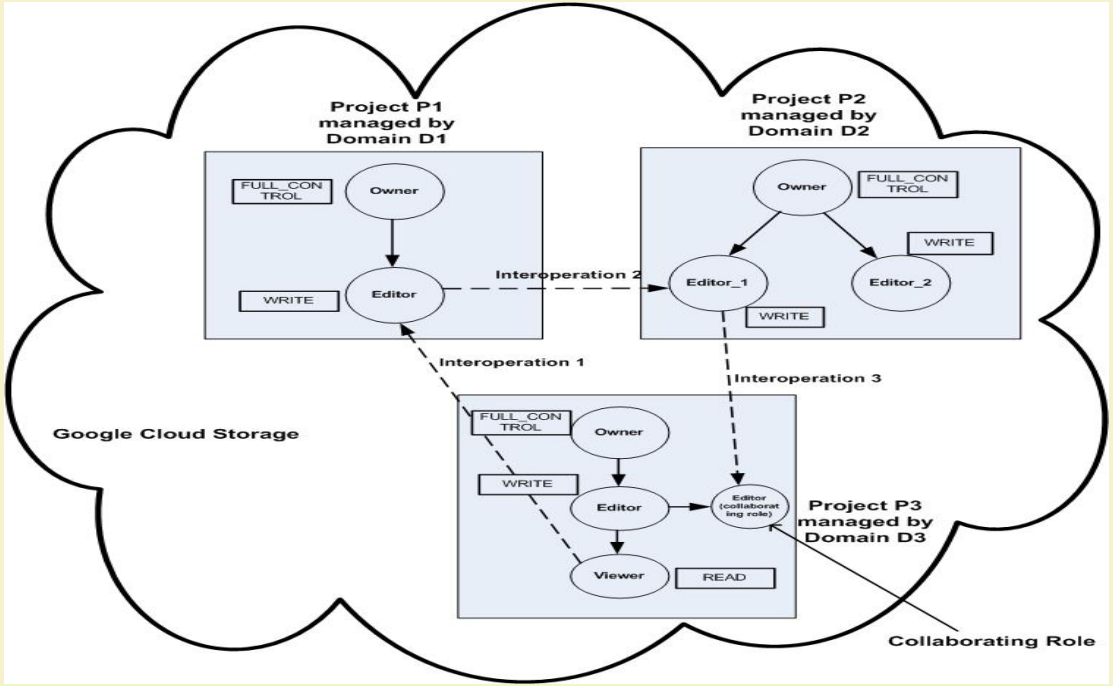
Conflict Removal

Cyclic Inheritance: Inheritance Conflict Removal Rule for Exactly Matched Role



Conflict Removal

Cyclic Inheritance: Inheritance Conflict Removal Rule for No-Exactly Matched Role



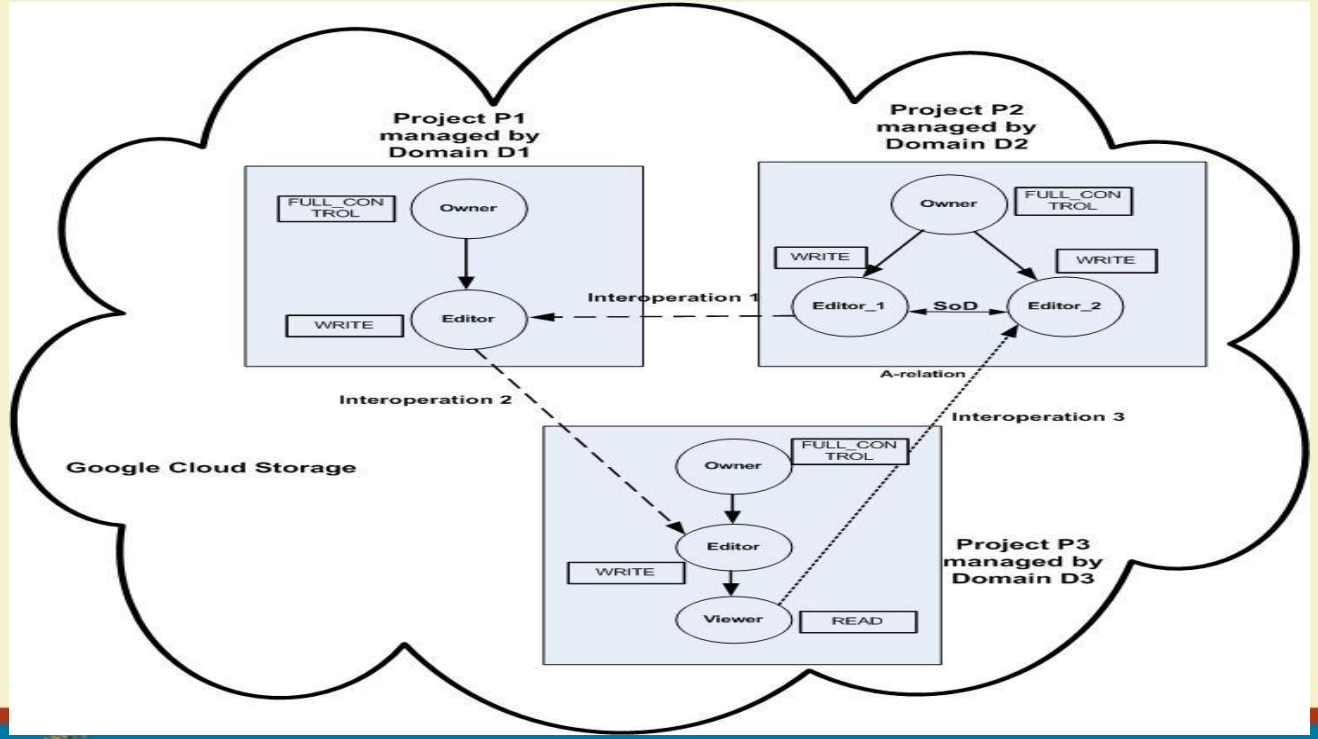
Conflict Removal

SoD Constraint Violation

- Two cases: similar to removal of inheritance conflict
  - Additional constraint: identifying *conflicting permission* between collaborating role and entry role in current domain
  - Conflicting permission
    - Objects are similar
    - Hierarchical relation exists between access modes
- Remove conflicting permission from permission set of collaborating role

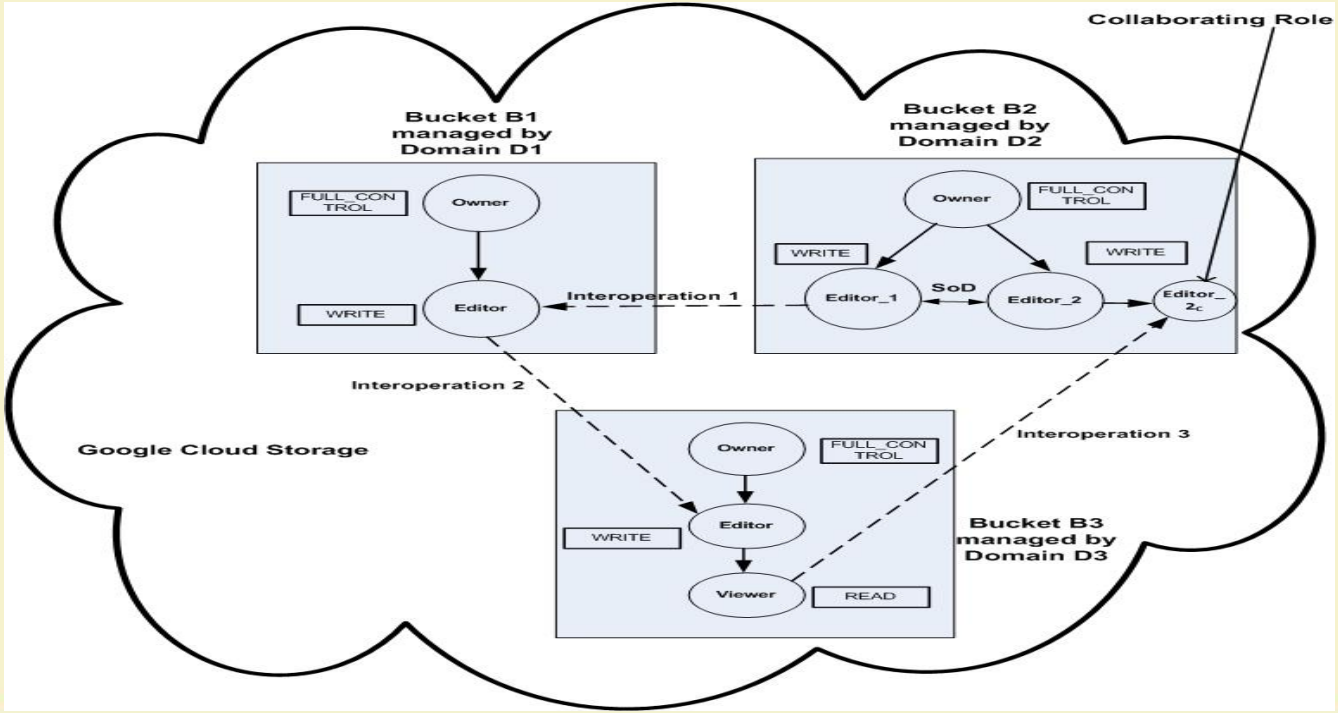
Conflict Removal

SoD Constraint Violation: SoD Conflict Removal Rule for Exactly Matched Role



Conflict Removal

SoD Constraint Violation: SoD Conflict Removal Rule for No-Exactly Matched Role



Summary

Secure Collaboration SaaS Clouds: A Typical Approach

- Selection of Trustworthy and Competent SaaS Cloud Provider for Collaboration
- Recommending Access Requests from Anonymous Users for Authorization
- Mapping of Authorized Permissions into Local Roles
- Dynamic Detection and Removal of Access Policy Conflicts

Thank You!