ABAC with Group Attributes and Attribute Hierarchies Utilizing the Policy Machine

2nd ACM Workshop on Attribute-Based Access Control (ABAC)
March 24, 2017

By
Smriti Bhatt, Farhan Patwa and Ravi Sandhu
Department of Computer Science
University of Texas at San Antonio

Outline

- Introduction
- Motivation
- Background & Related Work
- A Restricted HGABAC (*rHGABAC*) Model
- Policy Machine (PM) and its Architecture
- Authorization Architecture
- *rHGABAC* Utilizing Policy Machine
- Use Cases
- Policy Evaluation in PM
- Conclusion

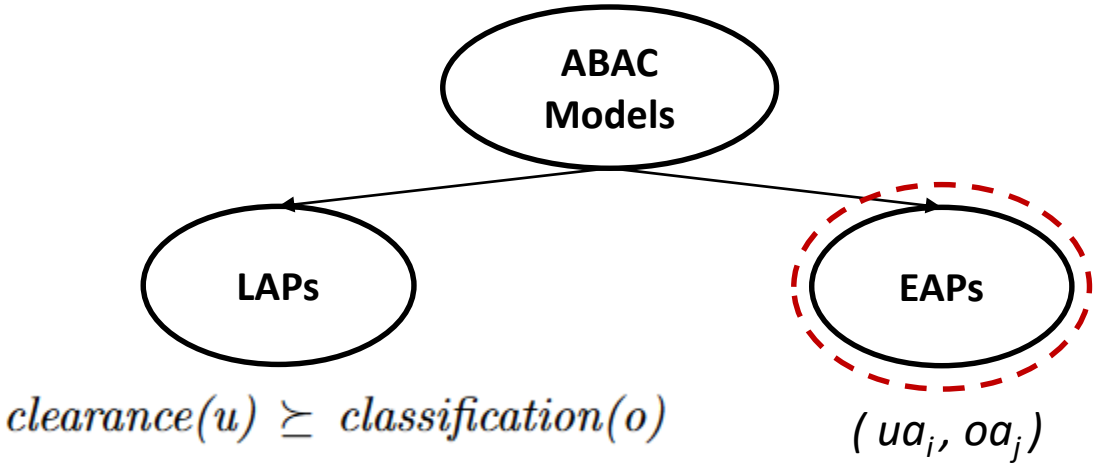
Introduction

❖ Attribute-Based Access Control (ABAC)

- ❖ Access control based on attributes of users and objects
- ❖ Flexible and fine grained access control model
- ❖ Core Entities:
  - ❖ Users
  - ❖ Objects
  - ❖ Attributes (Users & Objects)
  - ❖ Permissions/Actions
  - ❖ Authorization Policy

Introduction

- Many different ABAC models
- Authorization policy specification in ABAC Models



LAPs – Logical-Formula Authorization Policy

EAPs – Enumerated Authorization Policy

- Additional components and capabilities in ABAC
  - User and Object Groups
  - Group Attributes and Group Hierarchy
  - Attribute Hierarchy

Motivation

- ABAC models and policies in real-world applications
- Enforcement of ABAC policies through existing ABAC frameworks and tools
  - XACML 

  - Policy Machine 

- Ease of policy and attribute administration and management

Background & Related Work

- *HGABAC* – A hierarchical attribute-based access control model
  - User and Object Groups
  - Group Attributes and Hierarchies
- *HABE* – A hierarchical attribute-based encryption mechanism
- *LaBAC*$_H$ – Label-based access control model with hierarchy
  - Hierarchical relationship among attribute values

Group Attributes and Hierarchies

- Group attributes
- Hierarchy among groups

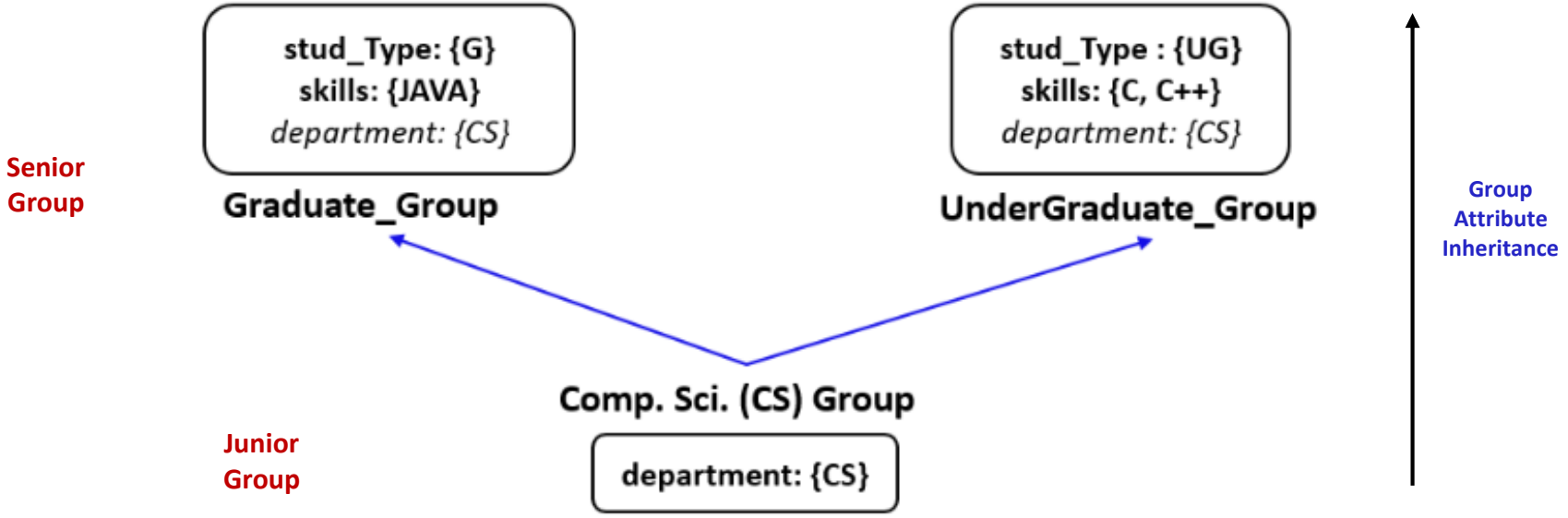
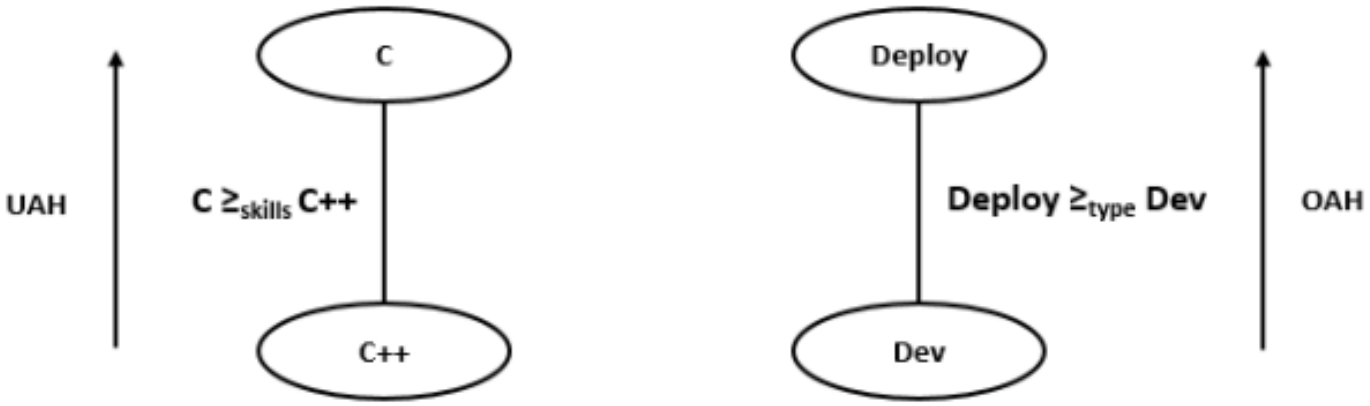


Fig 1. An Example of User Group Hierarchy Adapted from [*]

* Gupta, Maanak, and Ravi Sandhu. "The GURA_G Administrative Model for User and Group Attribute Assignment." *International Conference on Network and System Security*. Springer International Publishing, 2016.

Attribute Hierarchy

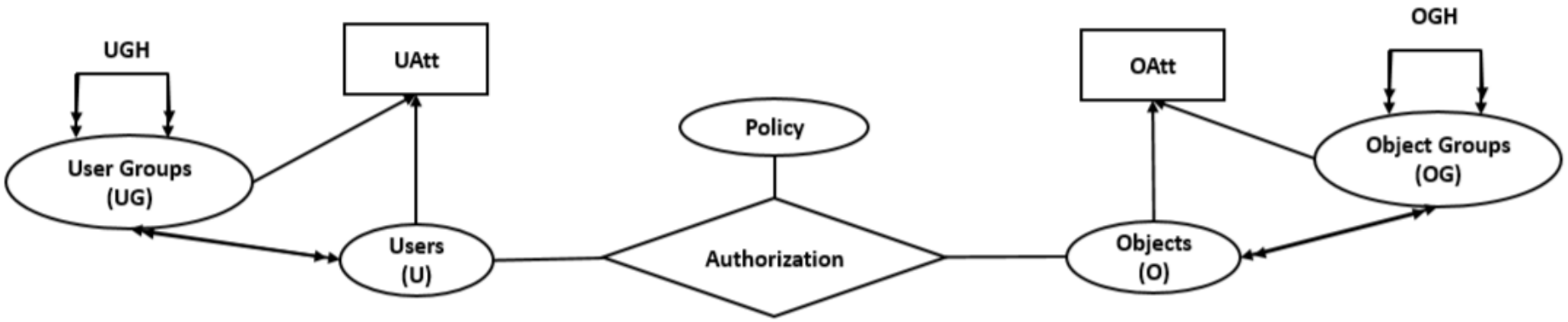
- A partial ordering of *Range* of attribute values



a. User Attribute-value Hierarchy **b. Object Attribute-value Hierarchy**

Fig 2. An Example of Attribute Hierarchy

A Restricted HGABAC (*rHGABAC*) Model



→ Formalized as Single-Value EAP

e.g. $Policy_{read} = (Manager, Private)$ (*uav*, *oav*)

Fig 3. *rHGABAC* Model Adapted from [1,2]

1. Servos, Daniel, and Sylvia L. Osborn. "HGABAC: Towards a formal model of hierarchical attribute-based access control." *International Symposium on Foundations and Practice of Security*. Springer International Publishing, 2014.
2. Gupta, Maanak, and Ravi Sandhu. "The GURA_G Administrative Model for User and Group Attribute Assignment." *International Conference on Network and System Security*. Springer International Publishing, 2016.

rHGABAC Model with Attribute Hierarchy

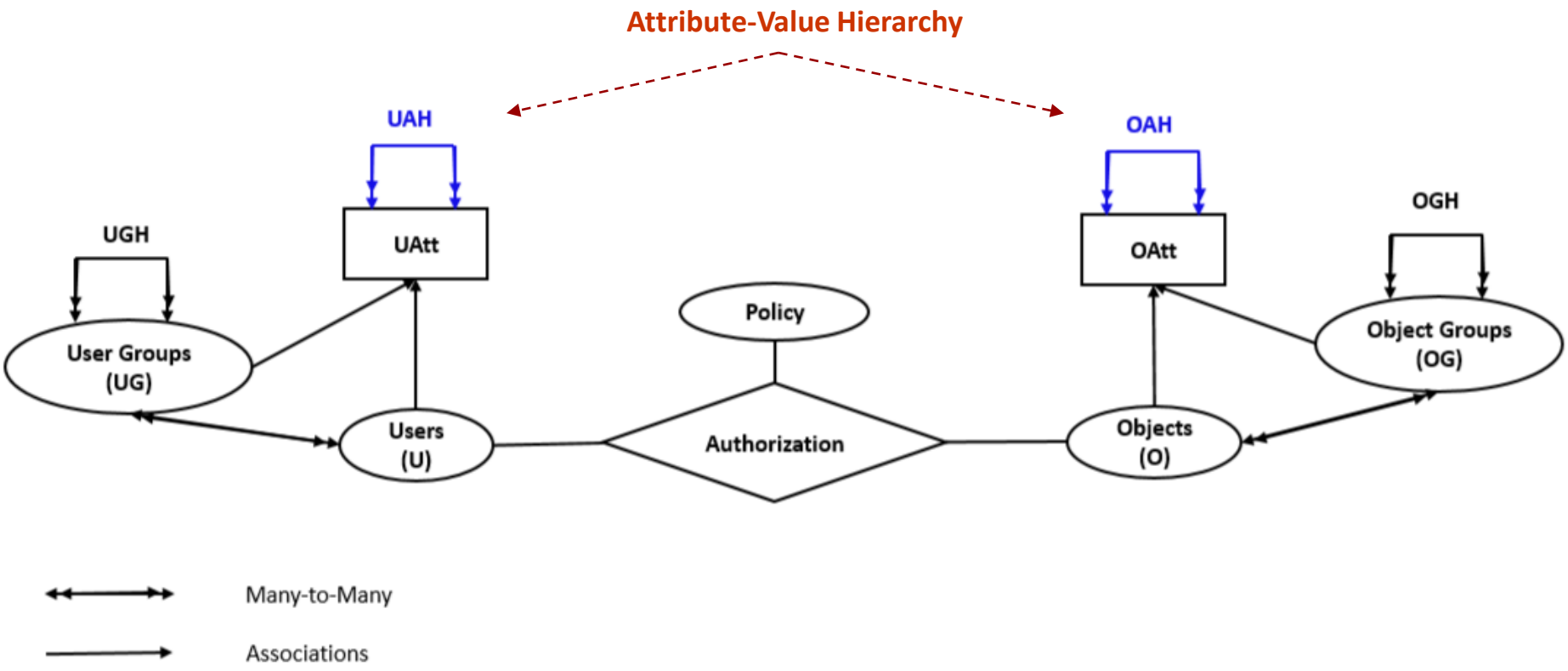


Fig 4. *rHGABAC* Model with Attribute Hierarchy

Policy Machine (PM)

- Unified attribute-based access control framework
- Express and enforce variety of access control policies utilizing PM Policy Configuration Points
  - Commonly known and implemented access control policies (DAC, MAC, RBAC)
  - Combinations of policies
  - New access control policies

PM Core Elements

- Users
- Objects
- User Attributes
- Object Attributes
- Operations, Access Rights
- Processes
- Policy Classes

PM Relations

- Assignment
- Association
- Prohibition
- Obligation

- ✓ **assignment**—for specifying relationships between policies, users, and user attributes, objects and object attributes
- ✓ **association** – for defining policies through associations between user attributes and object attributes or objects through some operations

PM Architectural Components

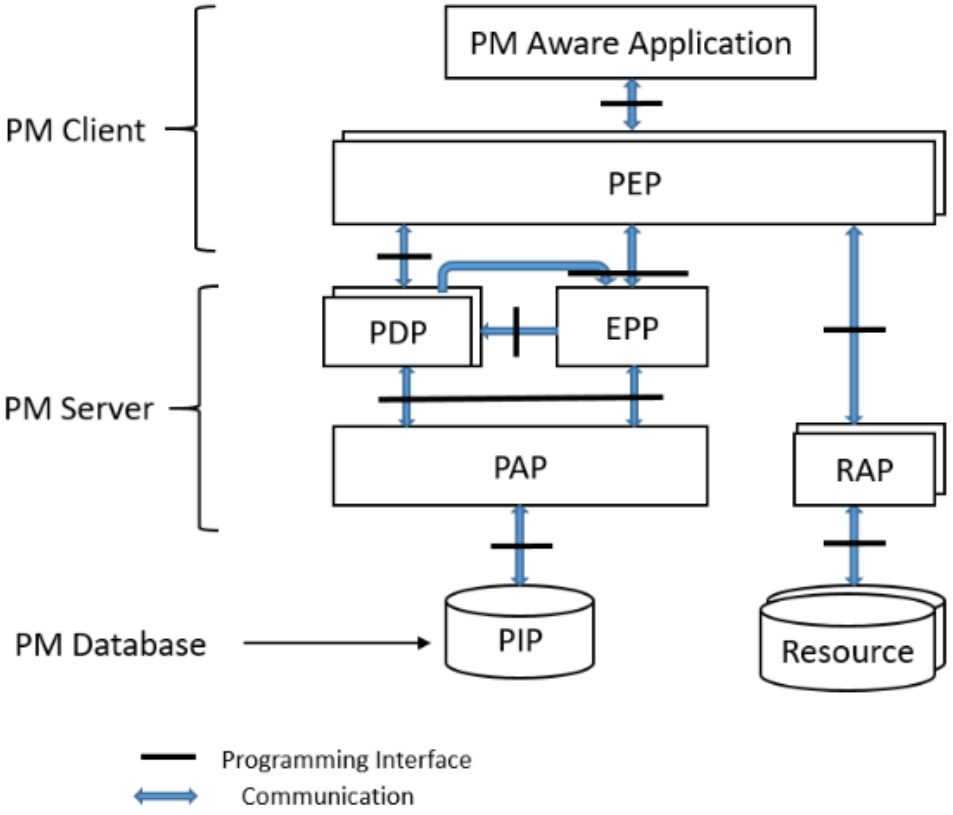


Fig 5. Architectural Components of PM Adapted from [*]

* D. Ferraiolo, S. Gavrila, and W. Jansen, "Policy Machine: Features, architecture, and specification," National Institute of Standards and Technology Internal Report 7987, 2014.

PM Architectural Components

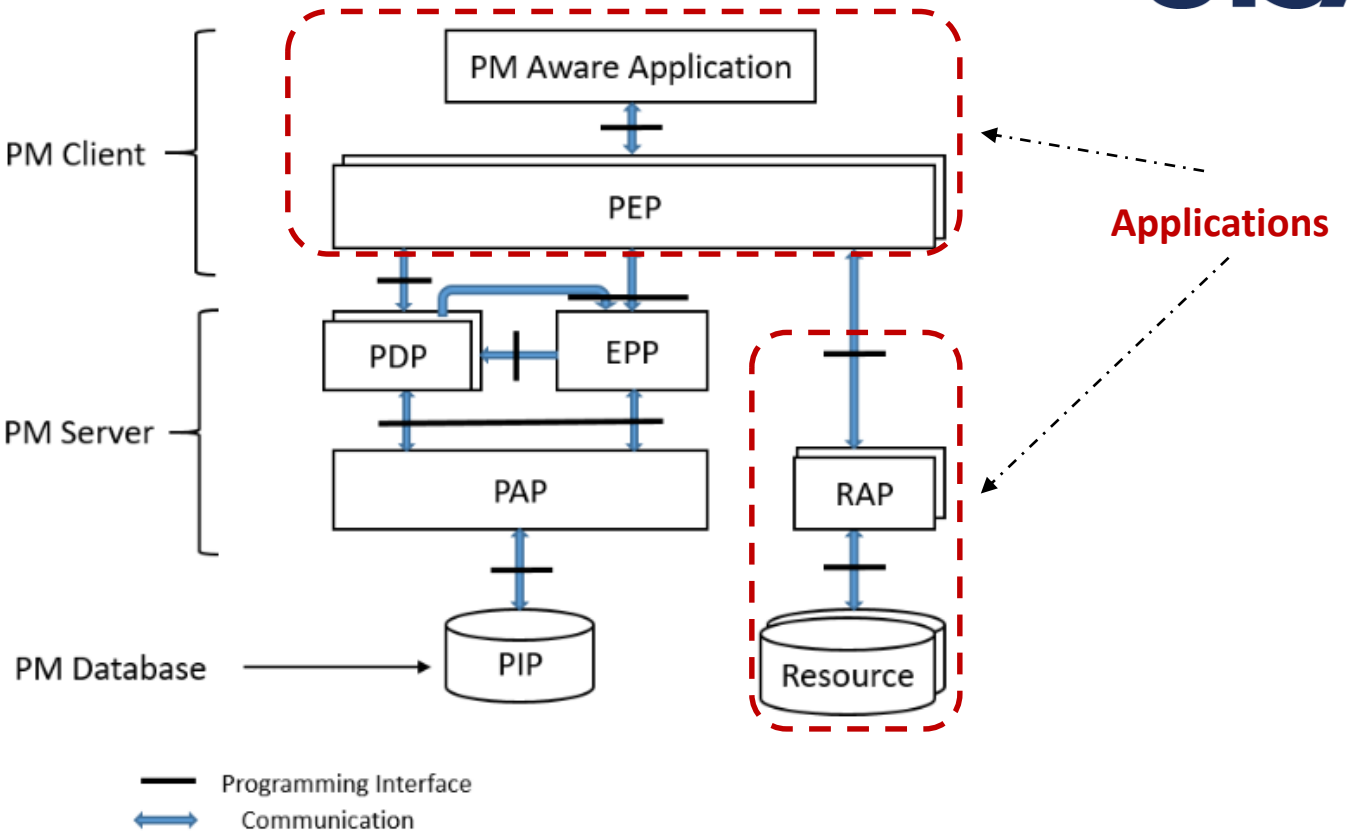


Fig 5. Architectural Components of PM Adapted from [*]

* D. Ferraiolo, S. Gavrila, and W. Jansen, "Policy Machine: Features, architecture, and specification," National Institute of Standards and Technology Internal Report 7987, 2014.

Authorization Architecture

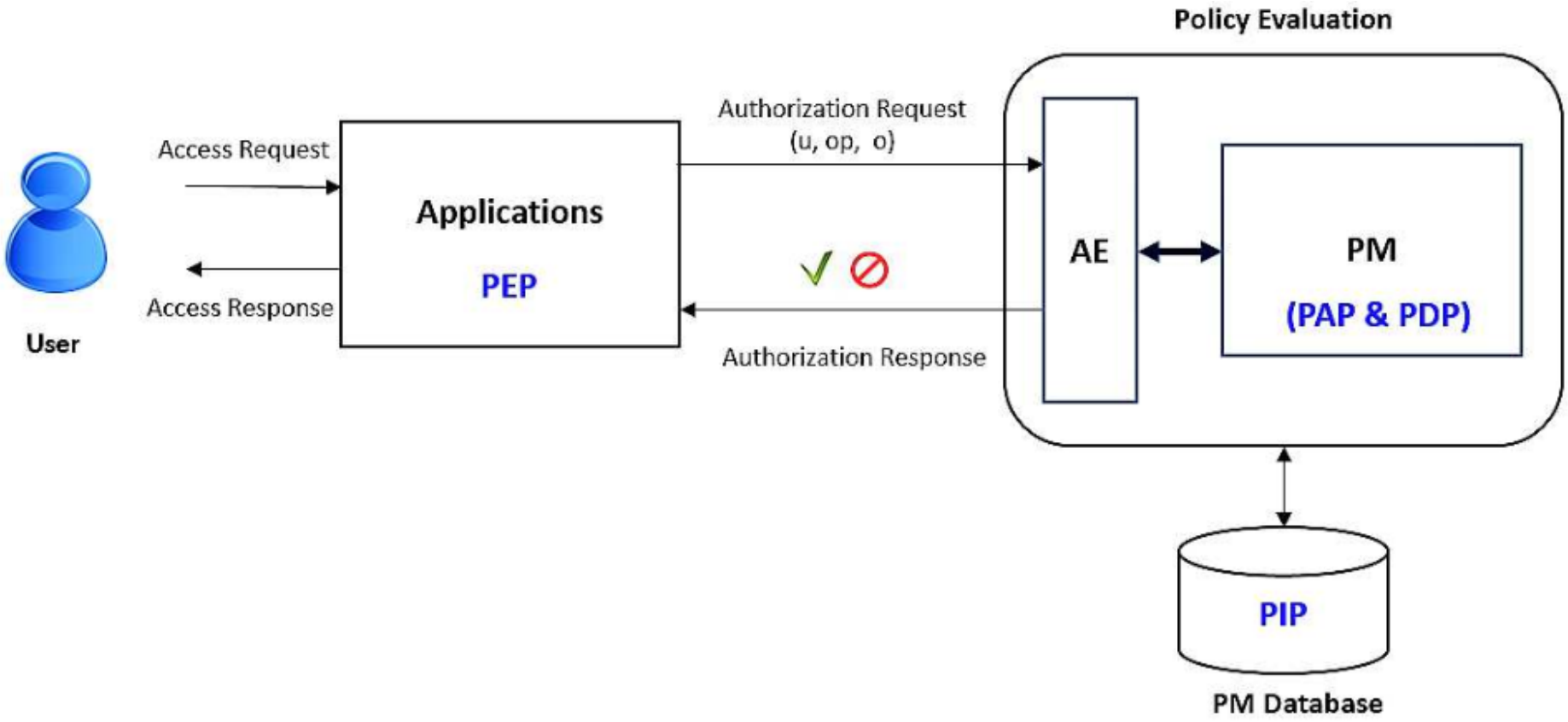


Fig 6. Authorization Architecture Utilizing PM and AE

rHGABAC Utilizing Policy Machine

Implementation

- PM Version 1.5
- Utilized PM Server (PAP + PDP) and PM Database (Active Directory)
- PM Agnostic Applications
- Need support for RESTful API in order to communicate to our **Authorization Engine (AE)***
- Resources and their access points are abstracted within applications

* S. Bhatt, F. Patwa, and R. Sandhu, "An attribute-based access control extension for OpenStack and its enforcement utilizing the Policy Machine," in IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). IEEE, 2016, pp. 37–45.

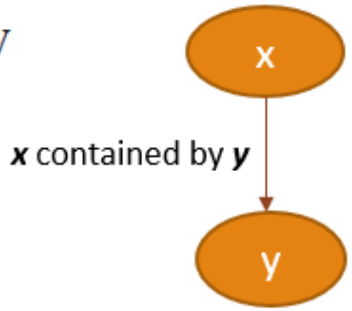
rHGABAC Utilizing Policy Machine

❖ *rHGABAC* Policy Configuration in PM

- ❖ User groups, user attributes and their values modeled as PM User Attributes
- ❖ Object groups, object attributes and their values modeled as PM Object Attributes
- ❖ Hierarchical relationships represented using PM's *assignment* relation and *containment* property

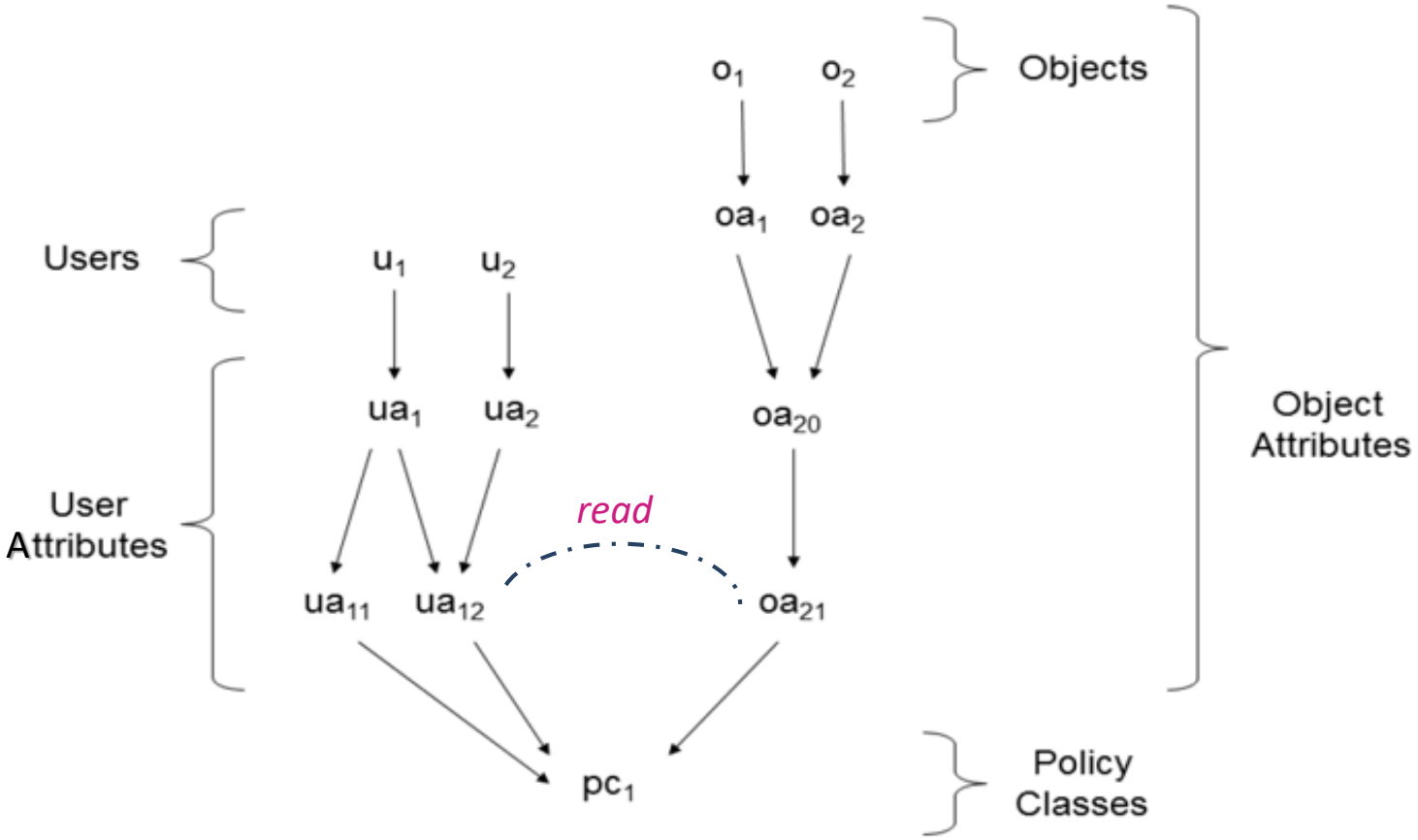
Containment Property:

$x \ ASSIGN^{+} \ y$

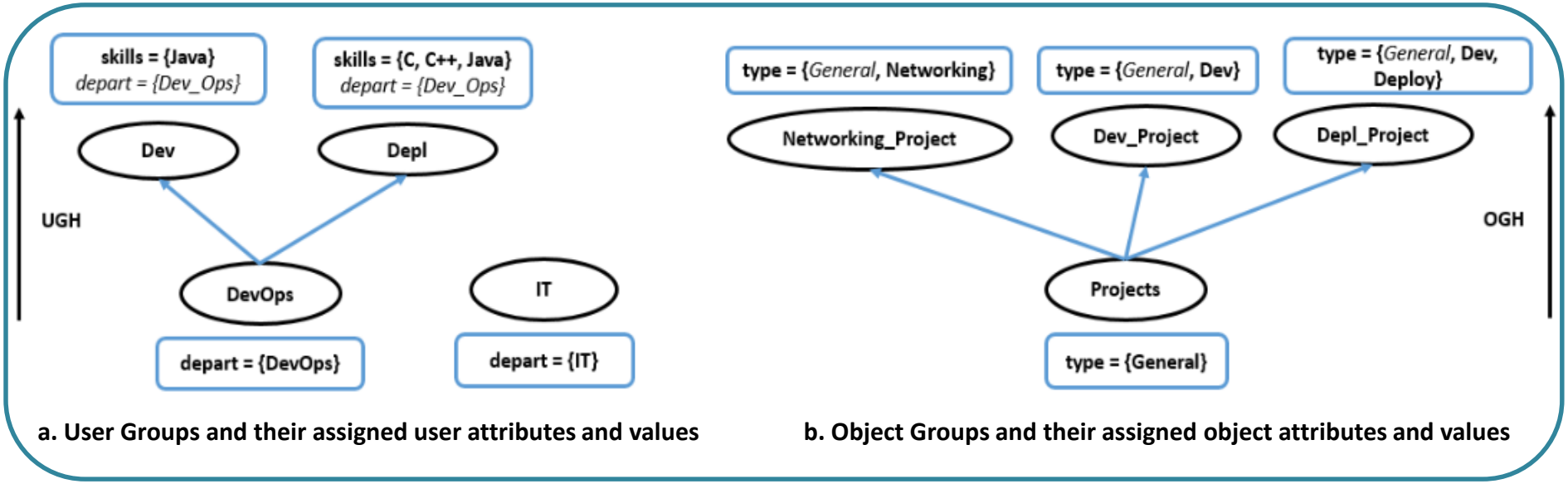


rHGABAC Utilizing Policy Machine

❖ A simplified Policy Element Diagram in Policy Machine



Use Case – Group Attributes and Hierarchy



a. User Groups and their assigned user attributes and values

b. Object Groups and their assigned object attributes and values

Use Case – PM Graph

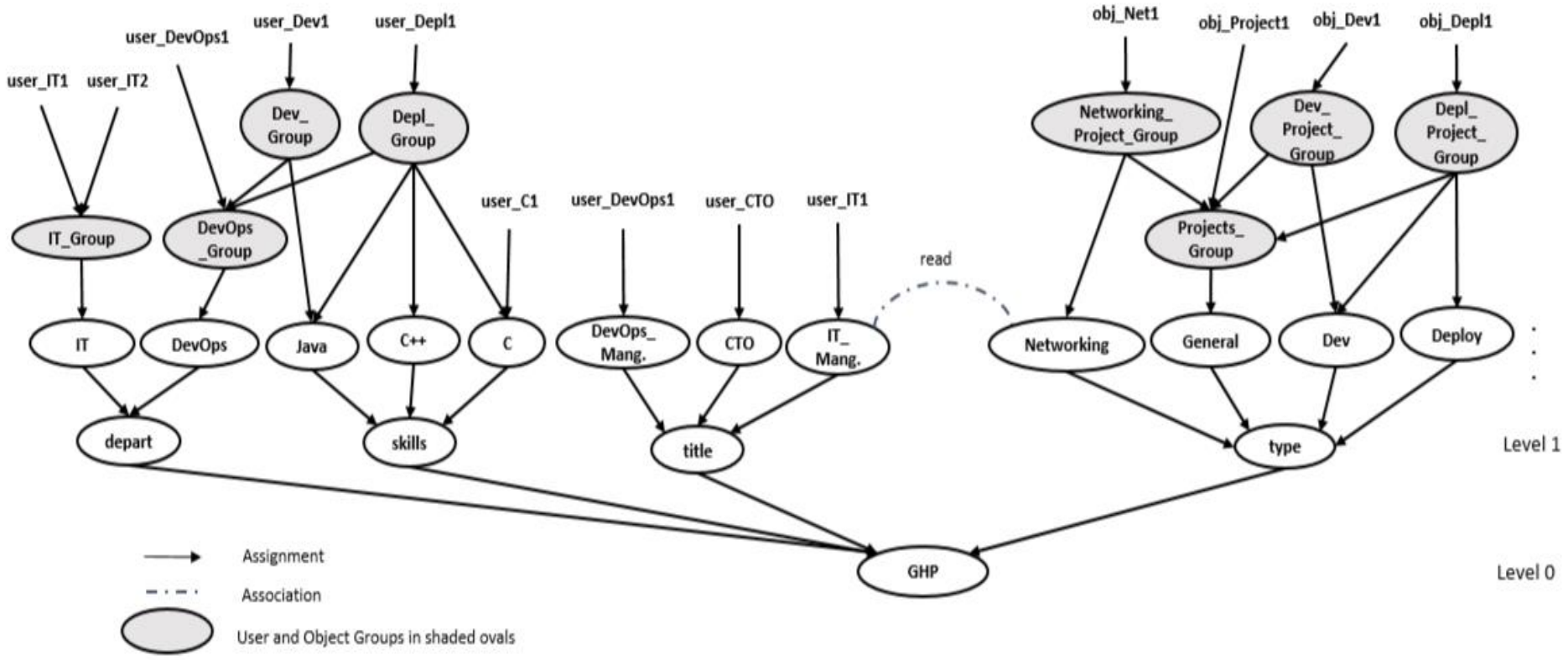


Fig 7. Group Hierarchy Policy Graph (Based on PM Graph Structure)

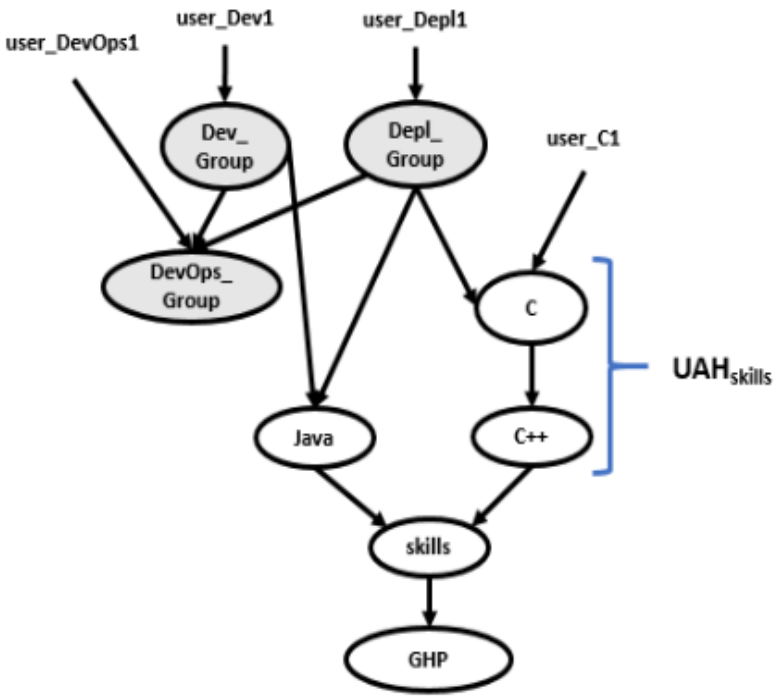
Use Case – Policy

$Policy_{read}$	
User Attribute Values	Object Attribute Values
IT_Manager	Networking
IT	Networking
DevOps_Manager	Dev
Java	Dev
DevOps_Manager	Deploy
Java	Deploy
C	Deploy
C++	Deploy
CTO	General

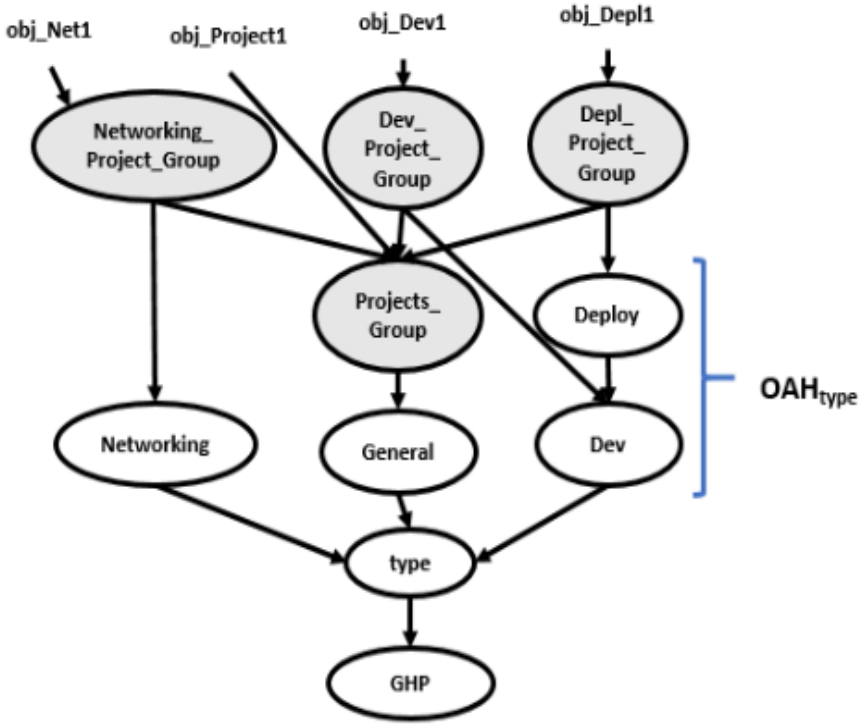
```
stack@pm-app1:/$ curl -s http:// 192.168.1.0:9000/echoGet -X GET -d
'{"type":"hierarchical",
 "user":"user_IT2",
 "operation":"read",
 "object":"obj_Net1"
}'
{"access":"granted"}
stack@pm-app1:/$
```

Authorization Policy Request and Response

Use Case Extended with Attribute Hierarchy



a. **Subgraph Showing Attribute Hierarchy in *skills* Attribute**



b. **Subgraph Showing Attribute Hierarchy in *type* Attribute**

Use Case Extended with Attribute Hierarchy

$Policy_{read}$	
User Attribute Values	Object Attribute Values
IT_Manager	Networking
IT	Networking
DevOps_Manager	Dev
Java	Dev
DevOps_Manager	Deploy
Java	Deploy
C	Deploy
C++	Deploy
CTO	General

Policy Without Attribute Hierarchy

$Policy_{read}$	
User Attribute Values	Object Attribute Values
IT_Manager	Networking
IT	Networking
DevOps_Manager	Dev
Java	Dev
C++	Deploy
CTO	General

Policy With Attribute Hierarchy

Policy Evaluation in PM

- Comparison of policy evaluation times for different ABAC policies in PM using our authorization architecture with AE

Average Policy Evaluation Time for ABAC Policies

Policy	Avg. Time (ms)
Role-Centric ABAC	26.04
rHGABAC	27.04
rHGABAC with AH	26.57

Conclusion

- A restricted HGABAC model (*rHGABAC*) presented and formalized as a single-value EAP
- Employed group attributes and group hierarchies, as well as attribute hierarchies in an ABAC model
- Presented a generalized authorization architecture for enforcement of ABAC policies
- *rHGABAC* simplifies Policy and Attribute management and administration in ABAC policies
- New versions of PM tool would provide better insights in new ways of expressing and enforcing ABAC policies

Thank you!!!

Questions???