

Attribute-Based Access Control: Insights and Challenges

Prof. Ravi Sandhu
Executive Director and Endowed Chair

DBSec
Philadelphia
July 19, 2017

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

**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**



**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

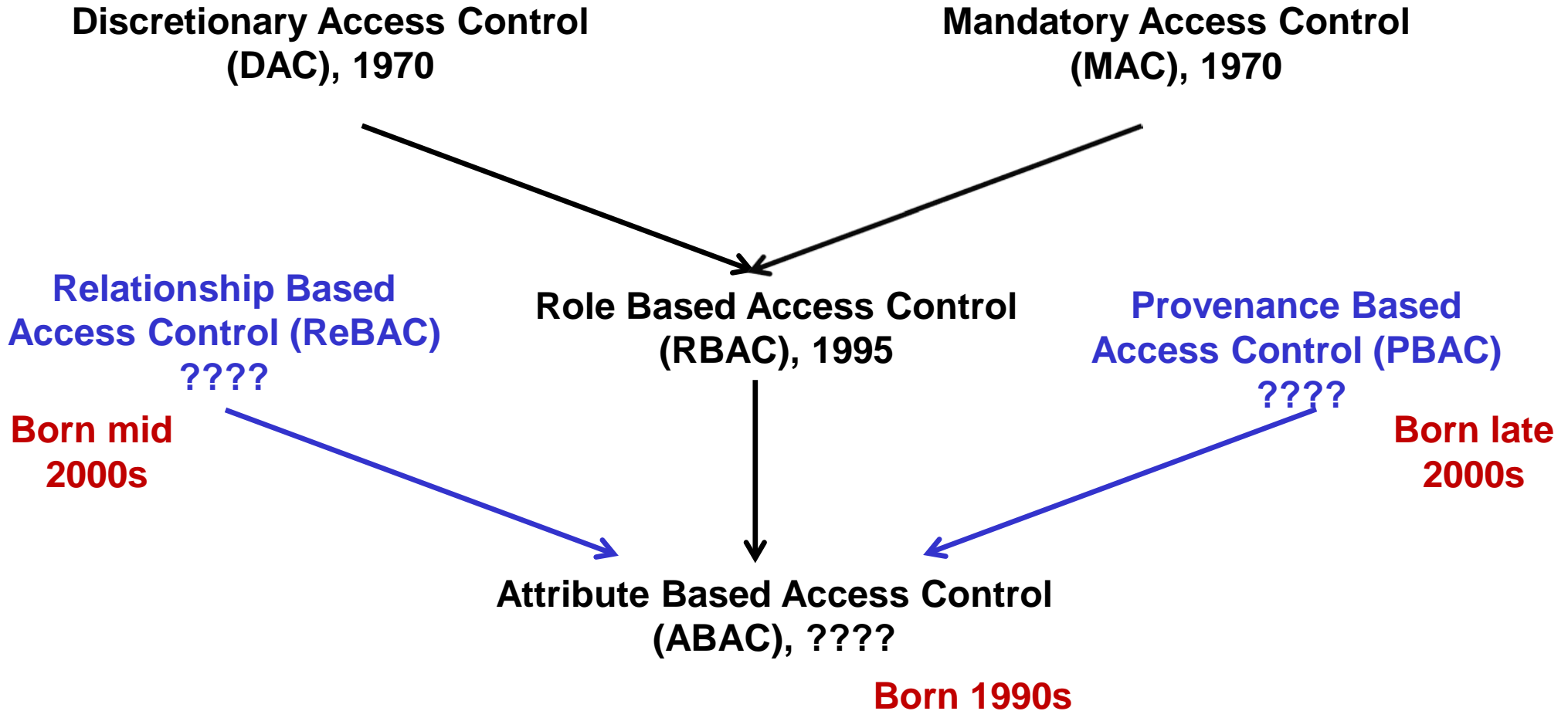


**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

Born 1990s



- NO!! Never!!

- Is ABAC the right word for the moment?
 - ❖ Certainly a strong candidate
 - ❖ Already too late?
 - ReBAC (relationship-based access control) not ABAC
 - Big Data, Analytics and AI will take care of everything

- What is lacking in ABAC?
 - ❖ Usage Control (UCON) concepts of attribute mutability, enforcement and obligation continuity, and post-obligations
 - ❖ Task-Based Access Control
 - ❖ Risk-Based Access Control
 - ❖ Policy-Based Access Control
 - ❖

- ABAC is orders of magnitude more complex than anything that has been an Access Control winner so far (DAC, MAC, RBAC)
 - ❖ We need the complexity, but need to manage it
 - ❖ If Google can index the web, we can do ABAC!!
- Cloud-enabled IoT may be the killer app

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

2. Core ABAC Models

1. Foundational Principles and Theory

Based on RBAC experience

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

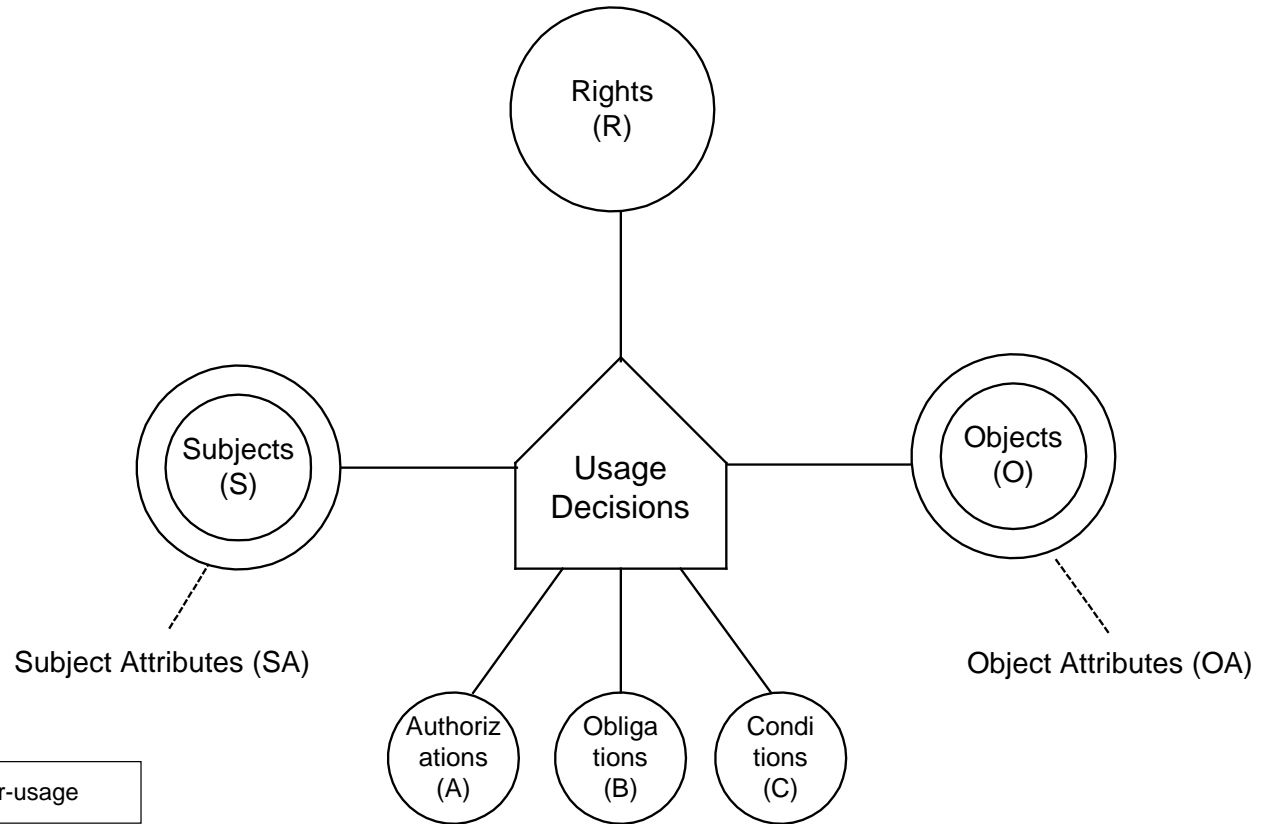
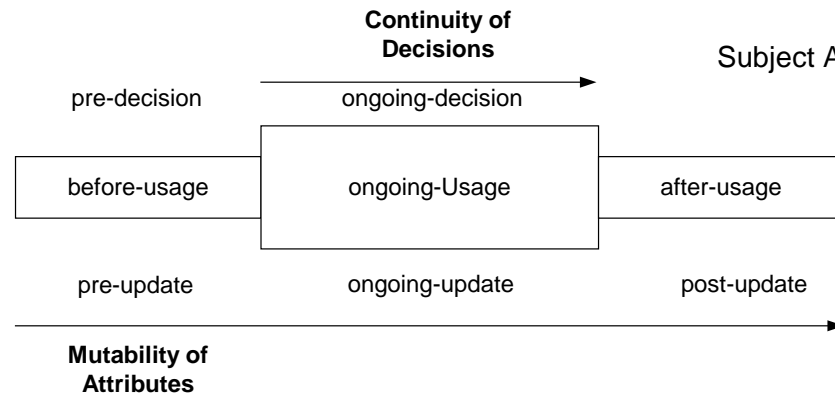
4. Extended ABAC Models

6. ABAC Enforcement Architectures

2. Core ABAC Models

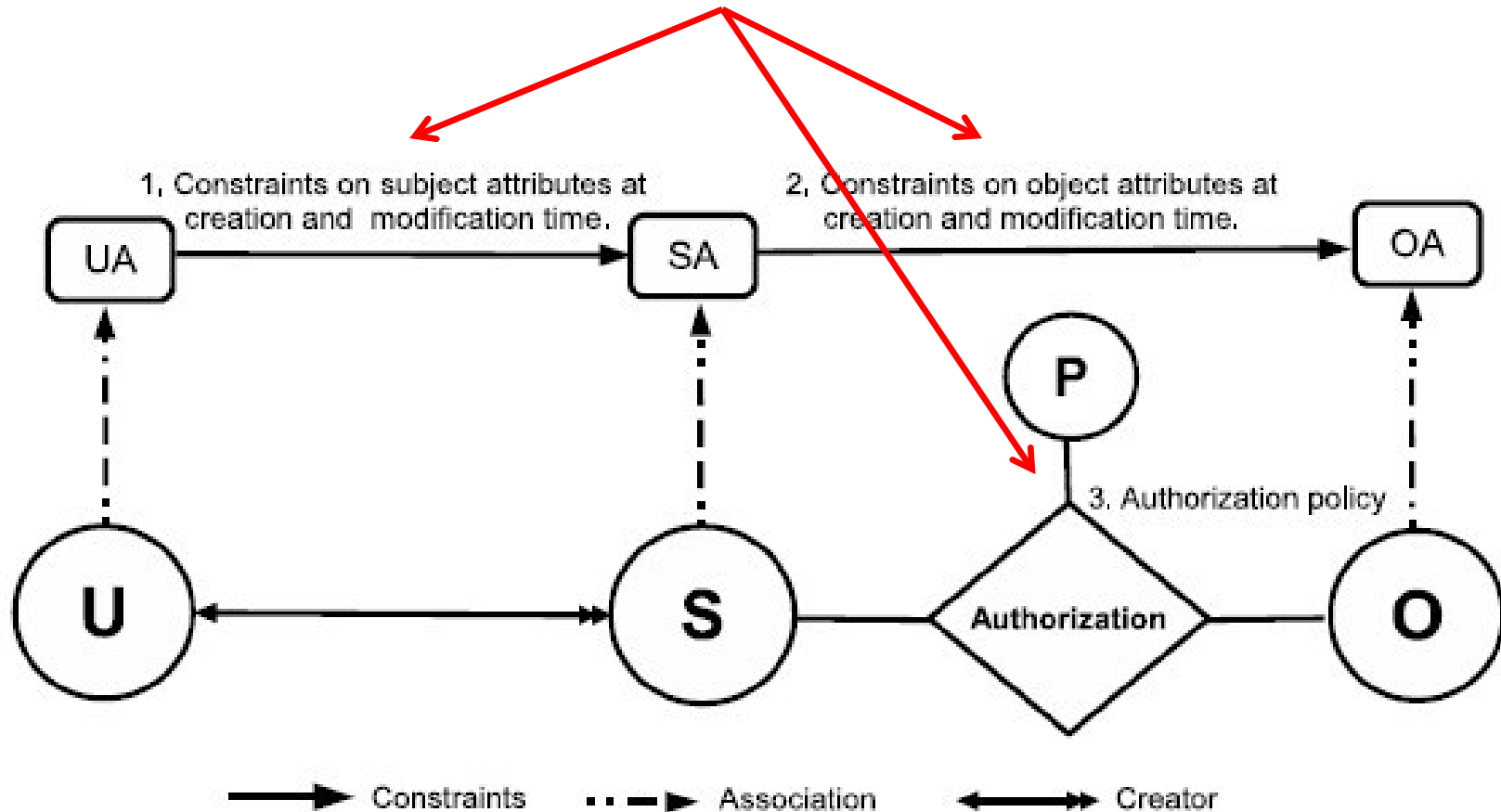
1. Foundational Principles and Theory

- unified model integrating
 - authorization
 - obligation
 - conditions
- and incorporating
 - continuity of decisions
 - mutability of attributes

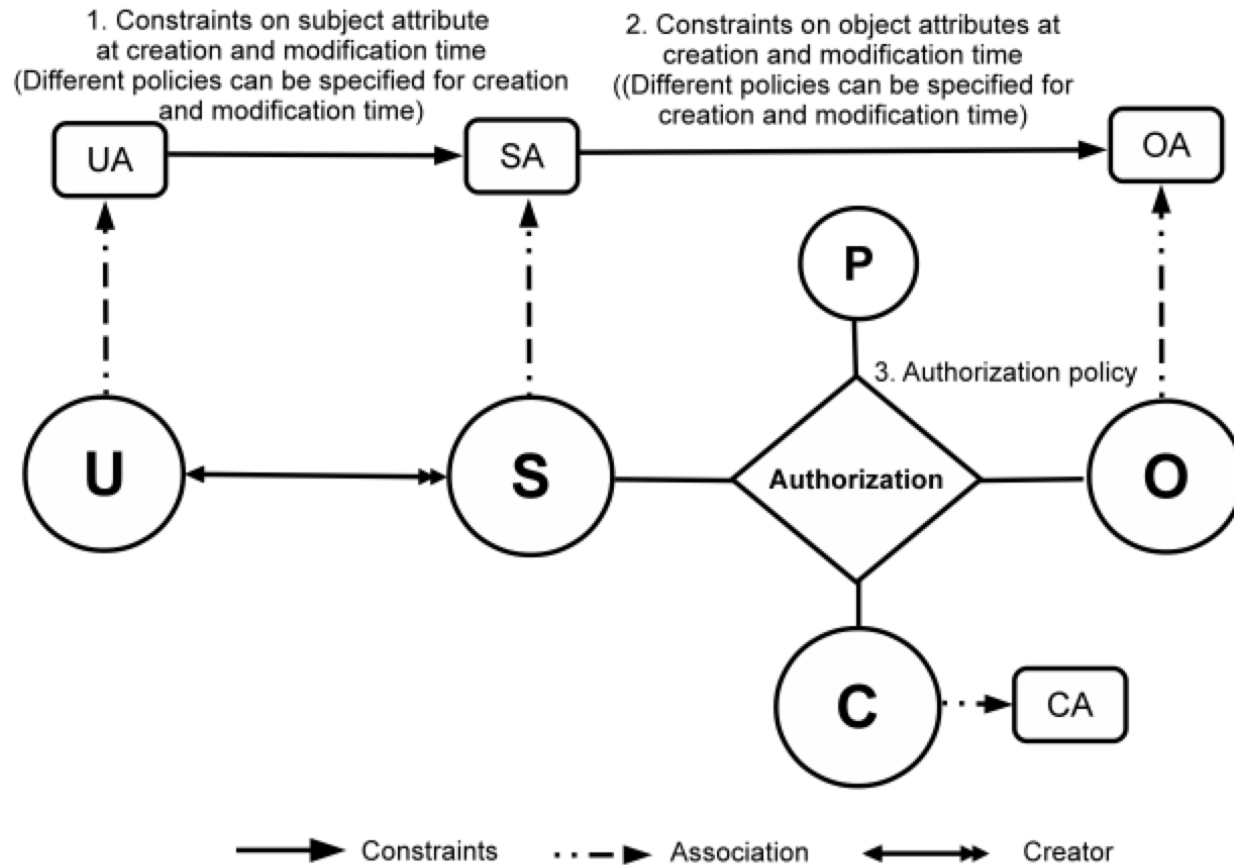


Usage Control Models, early 2000s
Park, Sandhu, Pretschner

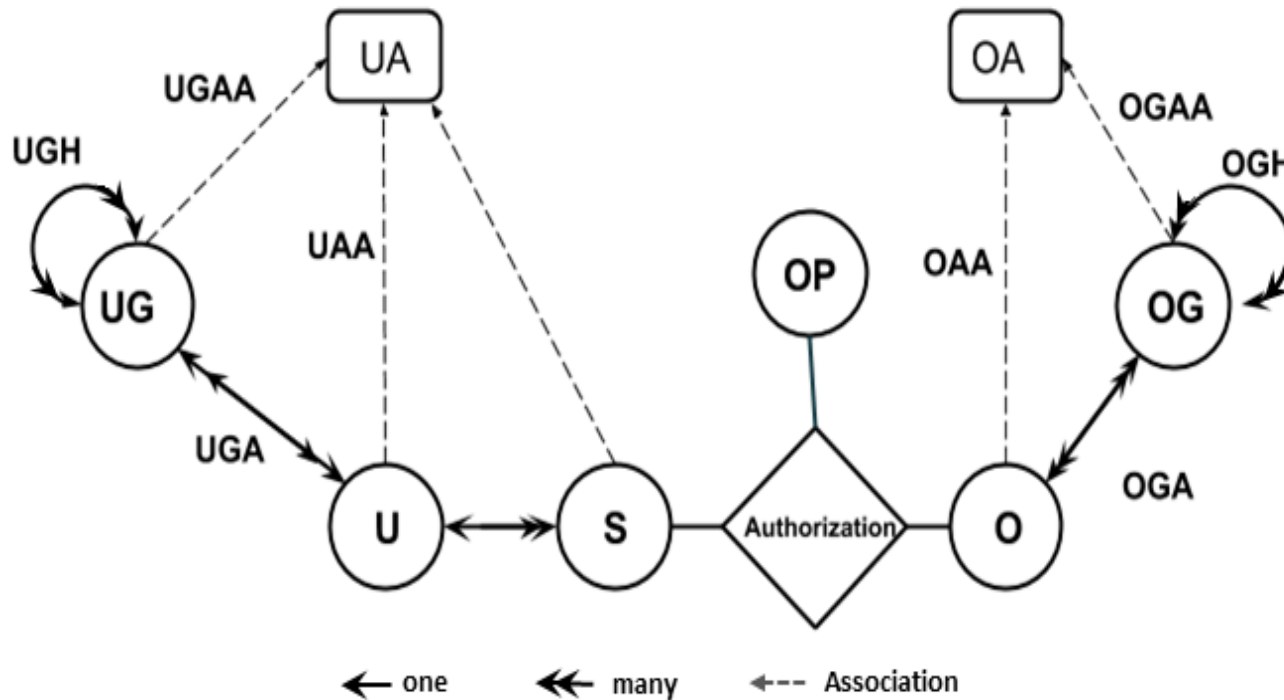
Policy Configuration Points



**Can be configured to do simple forms of
DAC, MAC, RBAC
Jin, Krishnan, Sandhu 2012**



**Can further be configured to do many
RBAC extensions
Jin, Krishnan, Sandhu 2014**



U: User
UG: User-Group
S: Subject
UA: User Attributes
O: Object
OG: Object-Group
OA: Object Attributes
OP: Operations

➤ Hierarchical Group and Attribute Based Access Control (HGABAC)

- ❖ Introduces the notion of User and Object Groups
- ❖ Core advantage is simplified administration of attributes
- ❖ User and Objects are assigned set of attributes in one go as compared to single assignment at a time.

Servos and Osborn, 2015

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

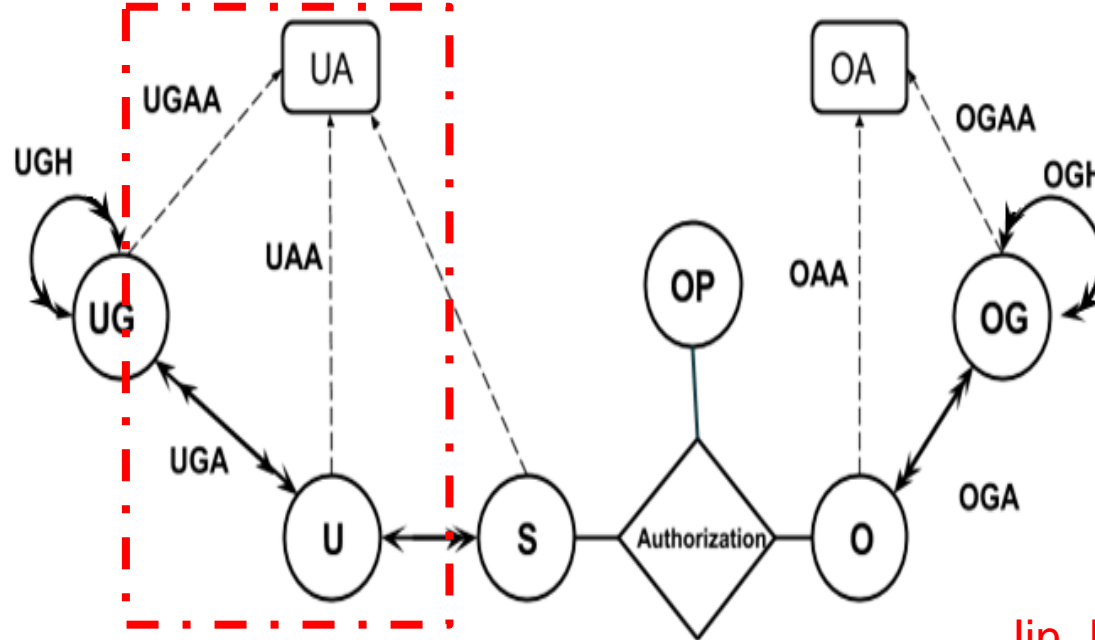
3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

2. Core ABAC Models

1. Foundational Principles and Theory



Jin, Krishnan, Sandhu, 2012
Gupta, Sandhu, 2016

Administrative Relations

– User Attribute Assignment (**UAA**) & User-Group Attribute Assignment (**UGAA**):

For each att_u in UA,

$$canAdd_{att_u} \subseteq AR \times \text{EXPR}(UA) \times 2^{\text{Range}(att_u)}$$

$$canDelete_{att_u} \subseteq AR \times \text{EXPR}(UA) \times 2^{\text{Range}(att_u)}$$

– User to User-Group Assignment (**UGA**):

$$canAssign \subseteq AR \times \text{EXPR}(UA \cup UG) \times 2^{UG}$$

$$canRemove \subseteq AR \times \text{EXPR}(UA \cup UG) \times 2^{UG}$$

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

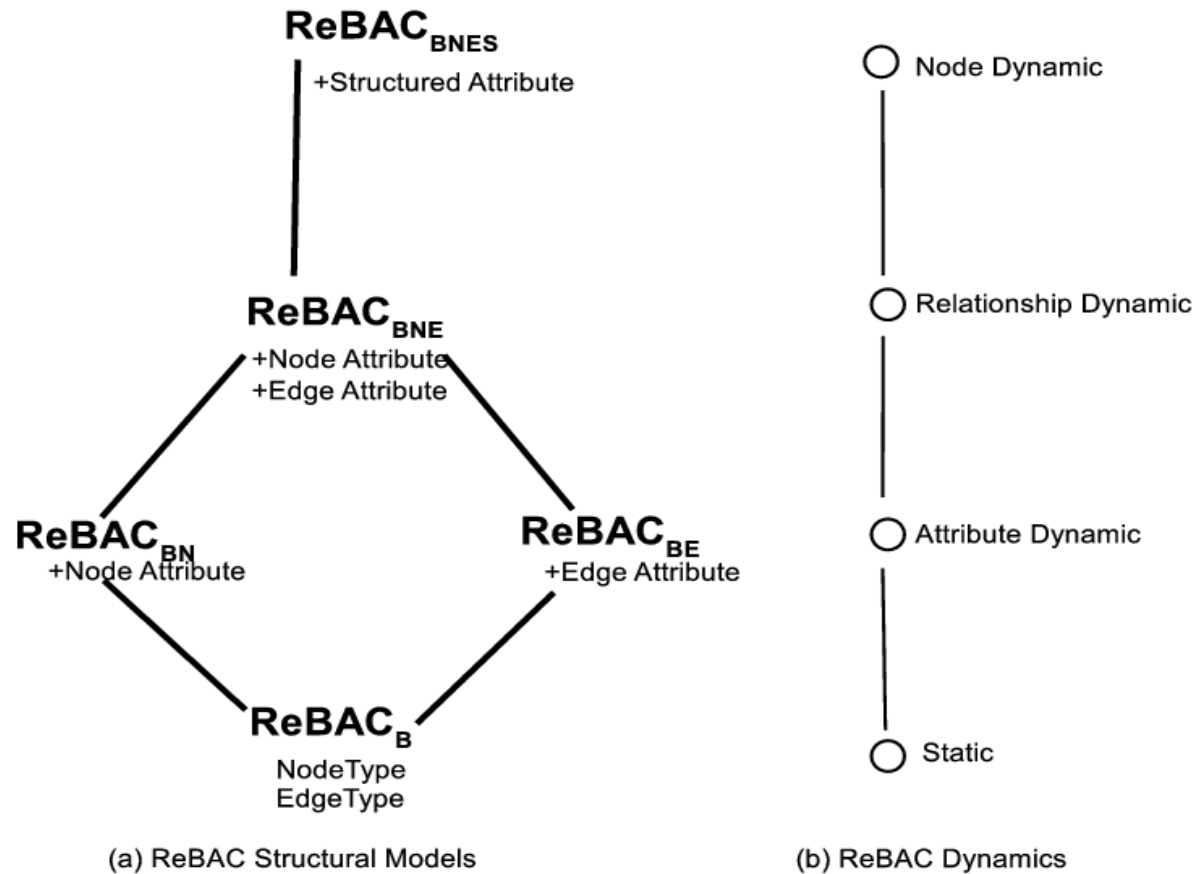
3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

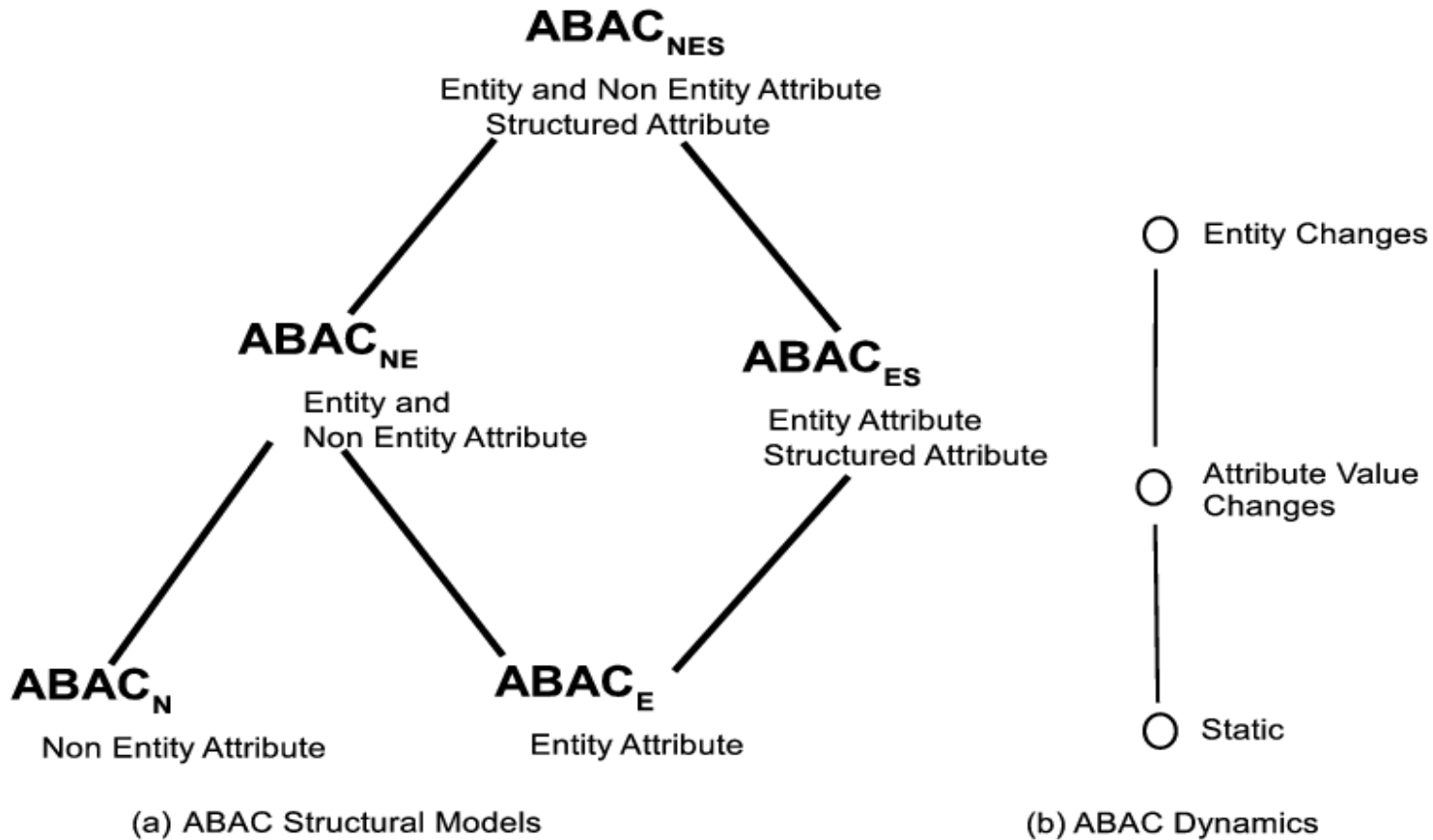
2. Core ABAC Models

1. Foundational Principles and Theory

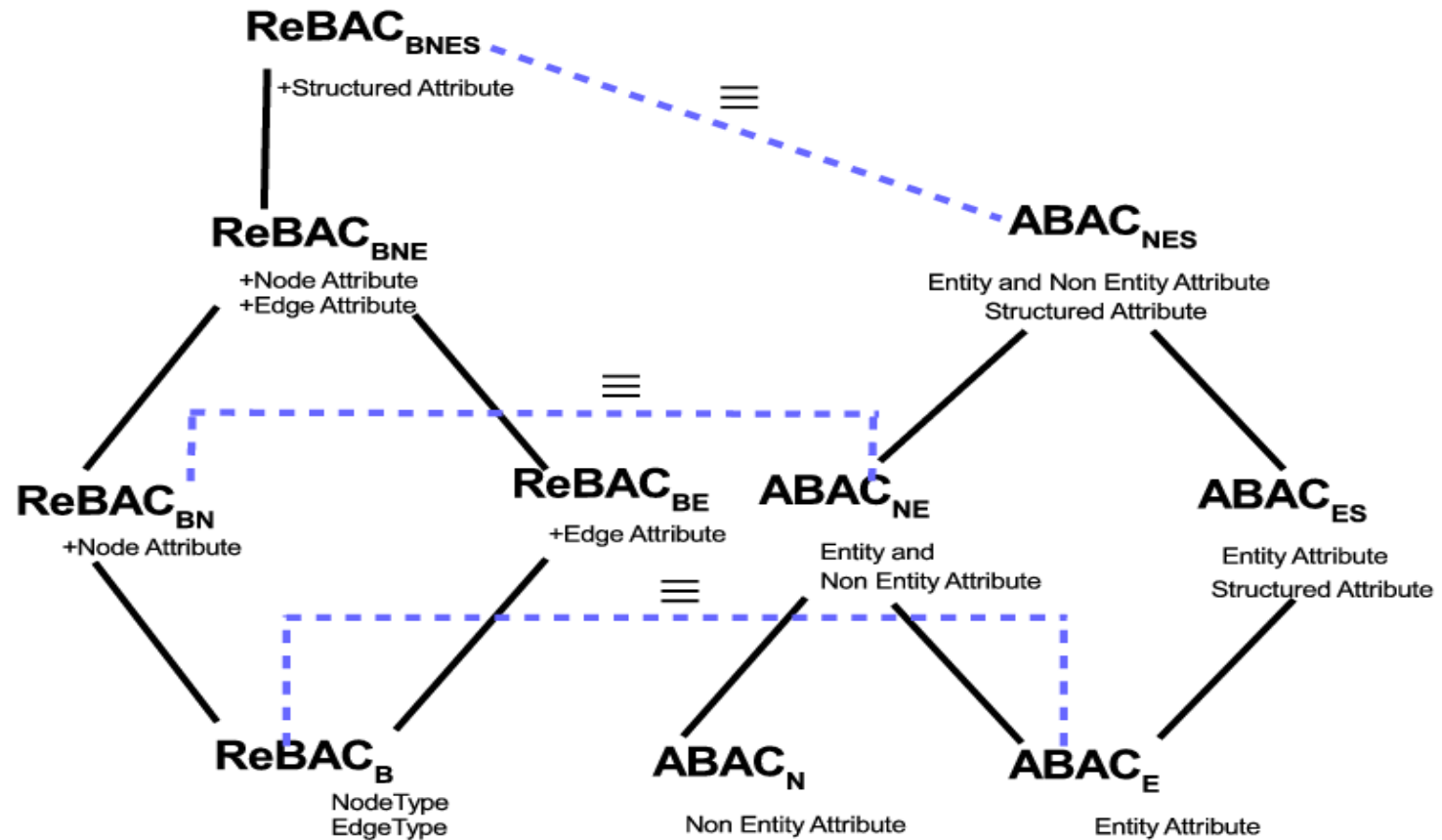


ReBAC Framework

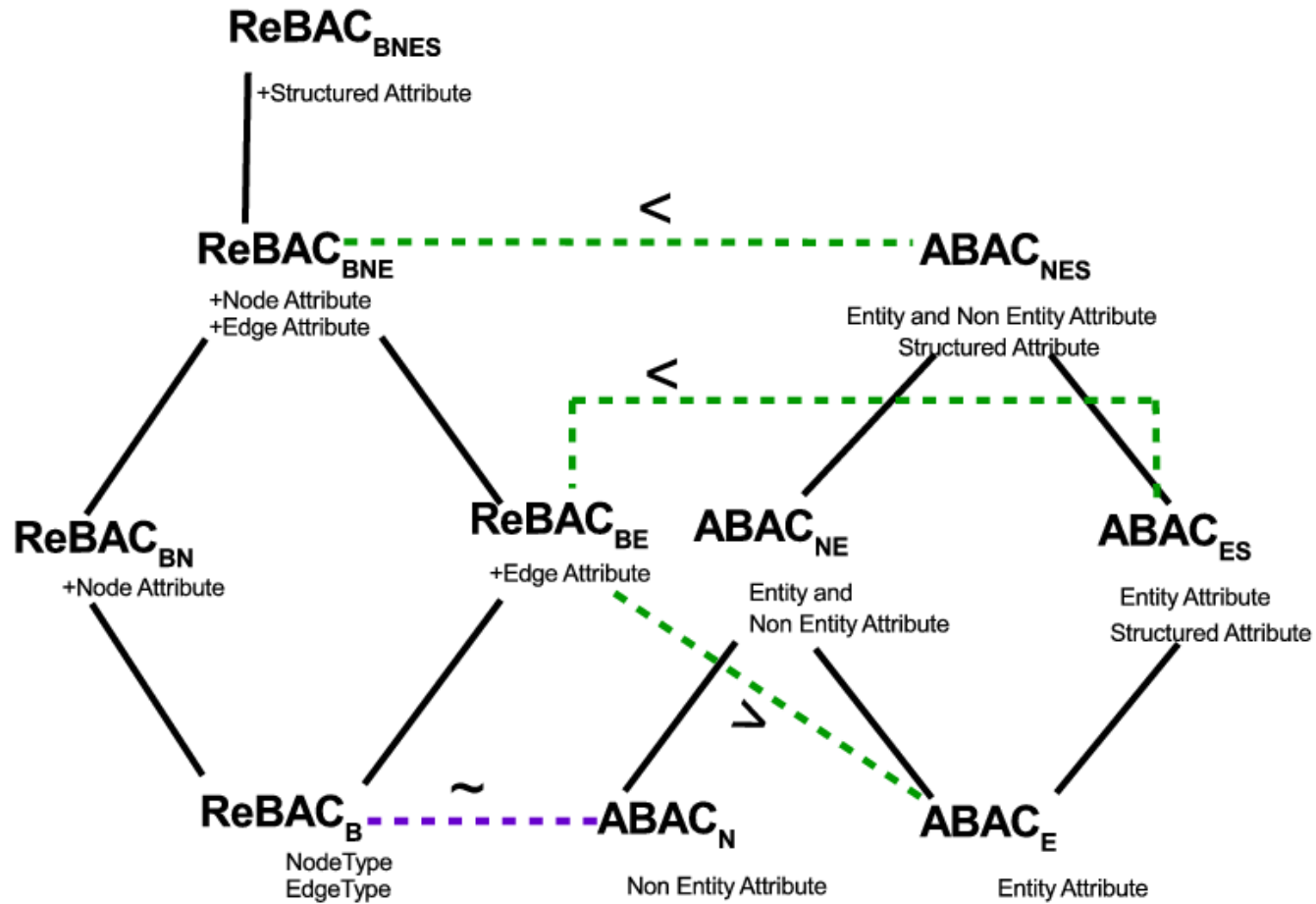
Ahmed and Sandhu, 2017



ABAC Framework



Equivalence of ReBAC and ABAC Structural Variants



Non-Equivalence of ReBAC and ABAC Variants

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

2. Core ABAC Models

1. Foundational Principles and Theory

- A single infinite attribute with no creation leads to undecidable safety. **Rajkumar 2012**
- Pre_UCON with finite attributes and unbounded creation has decidable safety. **Rajkumar, Sandhu 2016**
- ABAC_α has decidable safety. **Ahmed, Sandhu 2017**
- GURA has decidable safety/reachability. **Jin, Krishnan, Sandhu 2017**

7. ABAC Design, Engineering and Applications

**5. ABAC Policy
Architectures
and Languages**

3. Administrative
ABAC Models

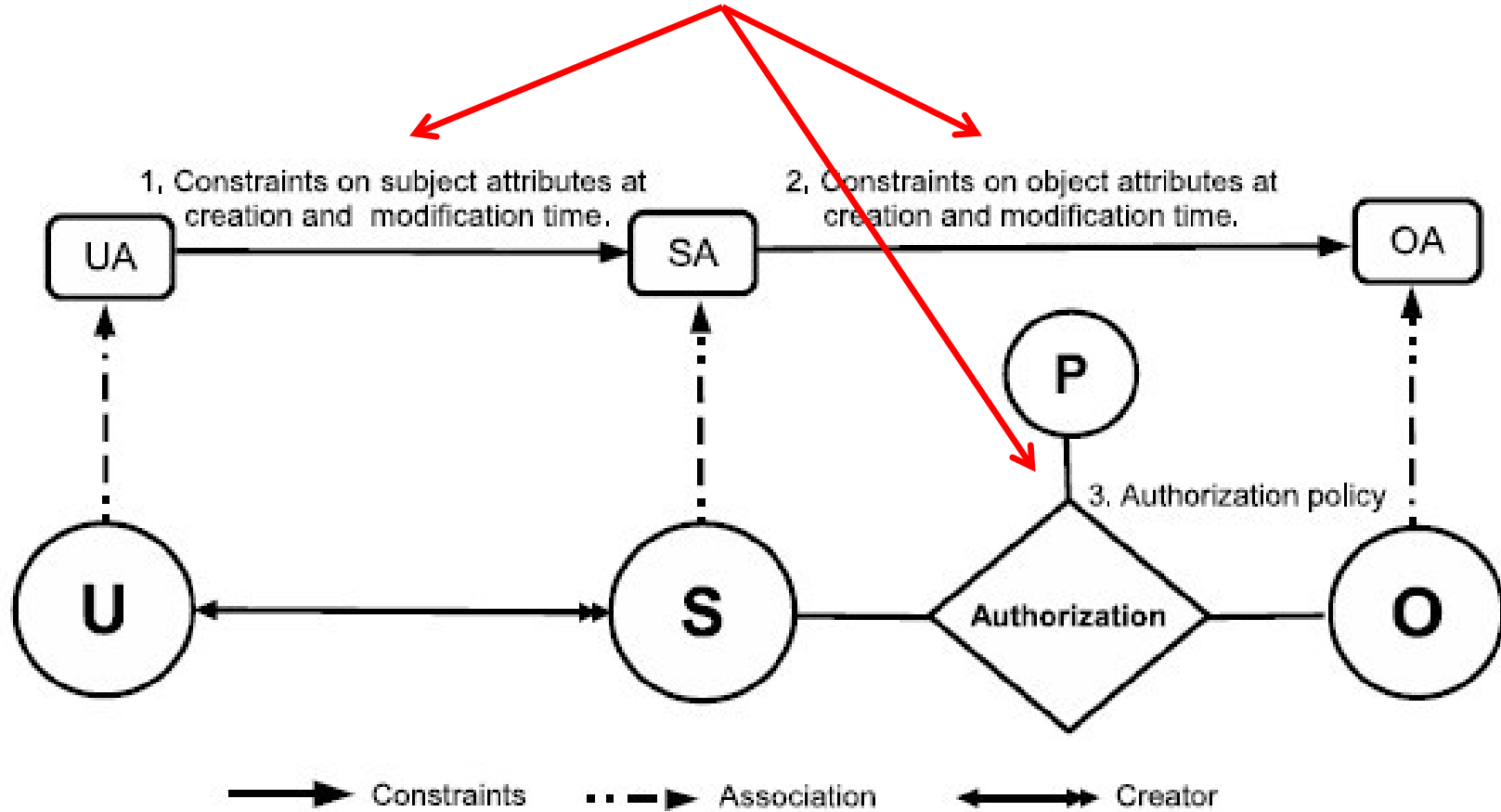
4. Extended
ABAC Models

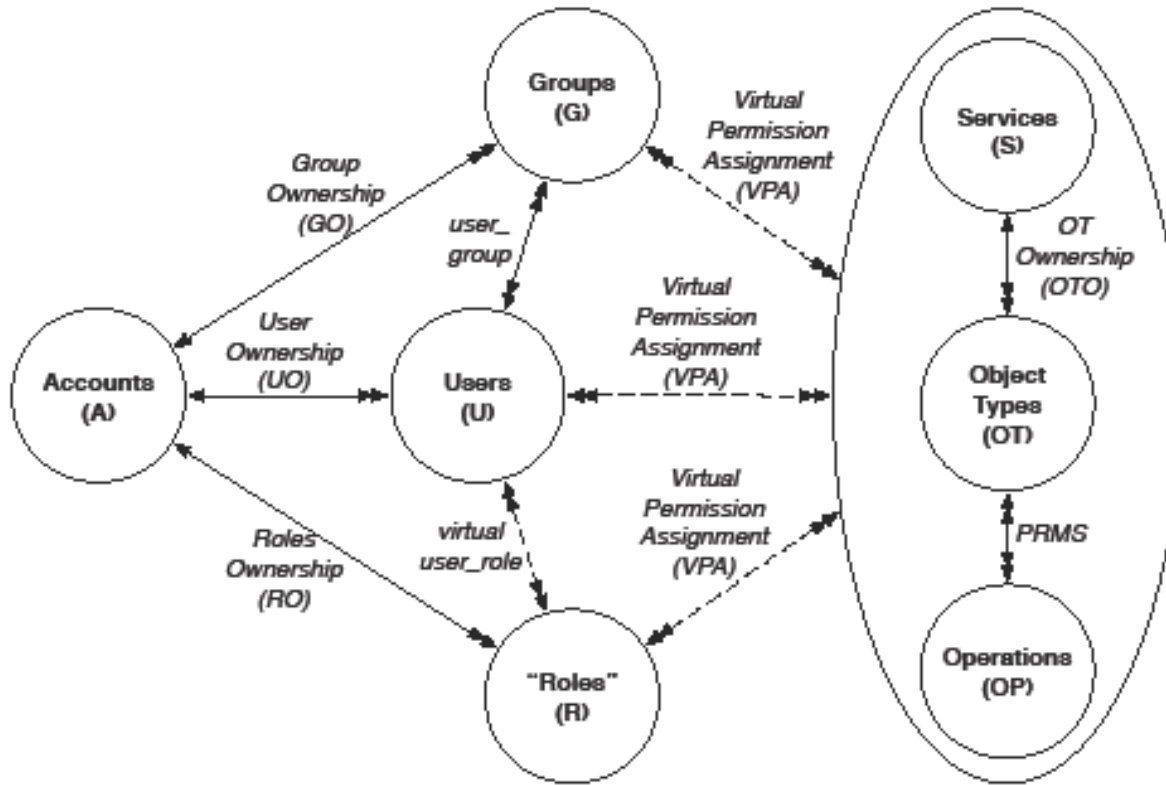
6. ABAC
Enforcement
Architectures

2. Core ABAC Models

1. Foundational Principles and Theory

Policy Configuration Points





7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

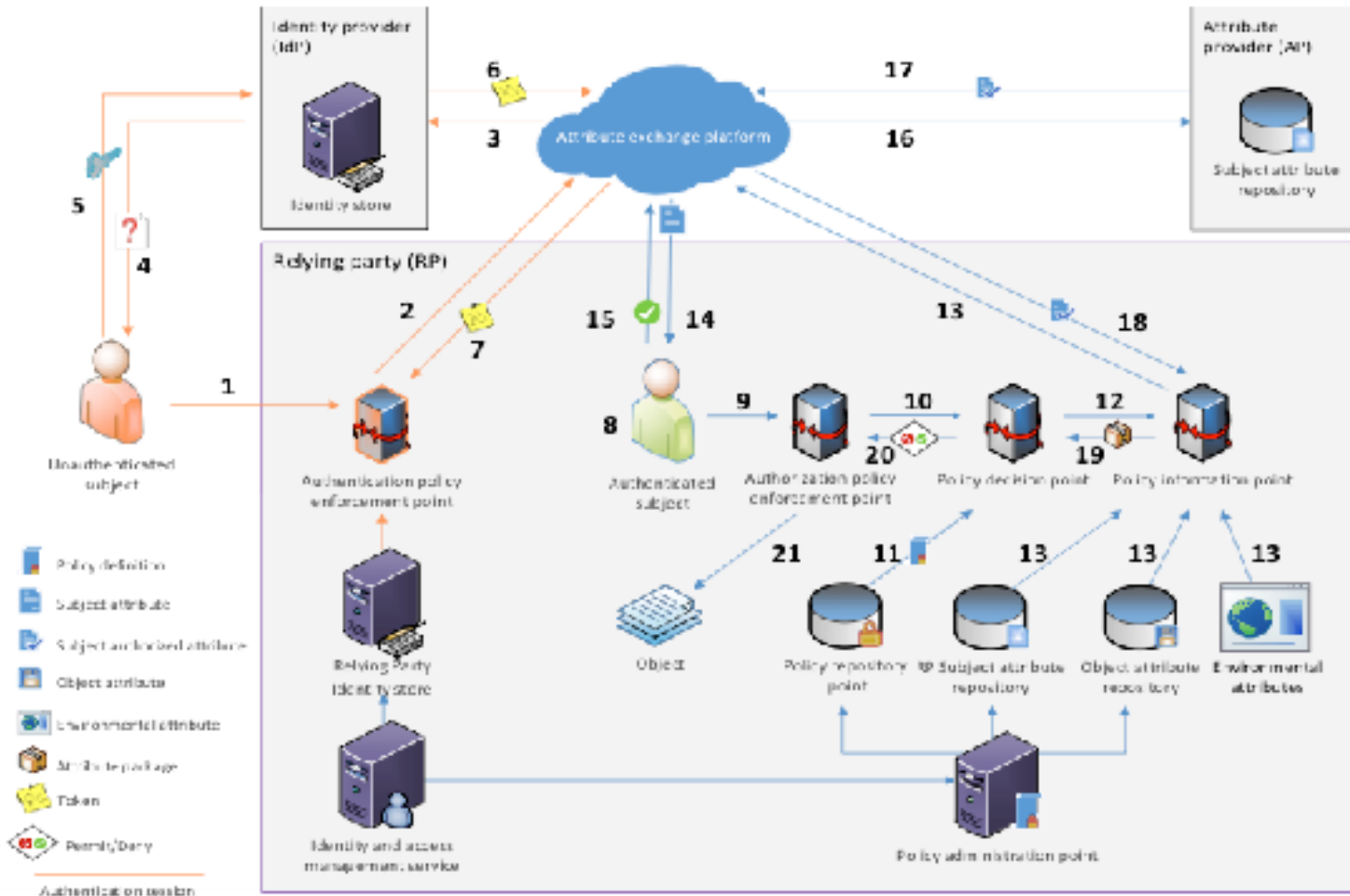
3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

2. Core ABAC Models

1. Foundational Principles and Theory



Fisher 2015
NCCOE, NIST, Building Block

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

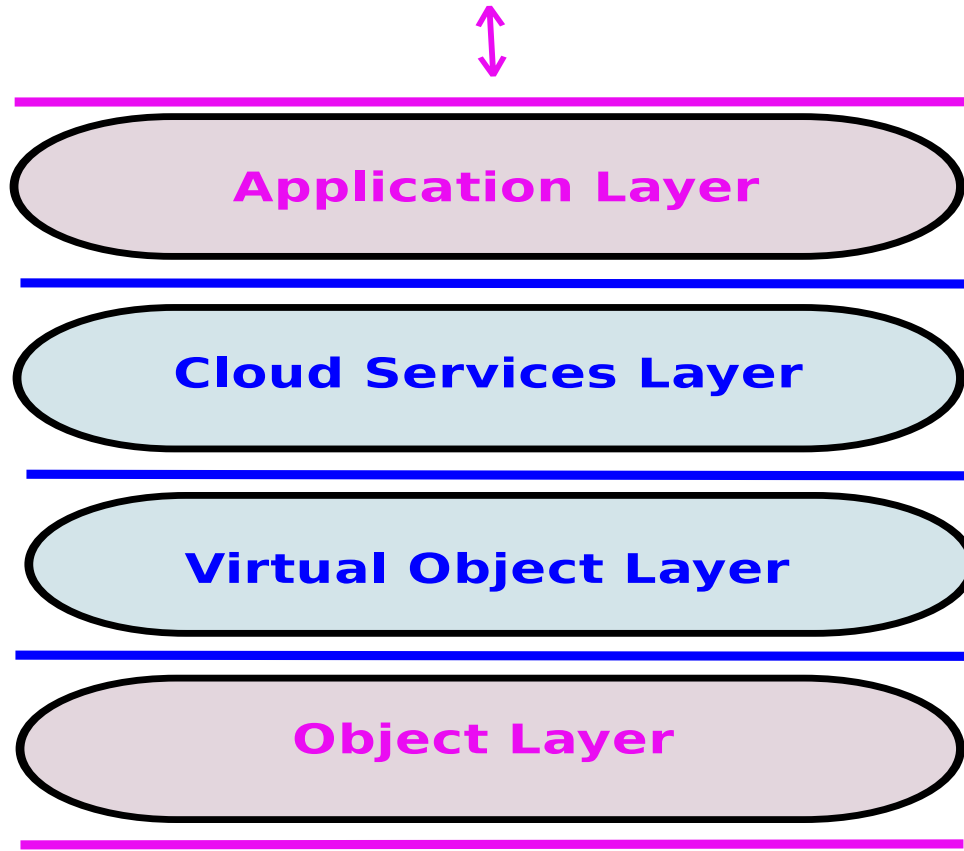
2. Core ABAC Models

1. Foundational Principles and Theory

- Cloud Computing IaaS
 - ❖ Single tenant
 - ❖ Multi tenant
 - ❖ Multi cloud

Jin, Tang, Dang, Bijon, Pustchi, Zhang, Biswas, Ahmed, Cheng,
Patwa, Krishnan, Sandhu
2012 onwards

User and Administrator Interaction



User Direct Interaction

Alsheri, Bhatt,
Patwa, Benson,
Sandhu
2016 onwards

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

4. Extended ABAC Models

6. ABAC Enforcement Architectures

2. Core ABAC Models

1. Foundational Principles and Theory