Attribute-Based Access and Communication Control Models for Cloud and Cloud-Enabled Internet of Things

Ph.D. Dissertation Defense:

Smriti Bhatt
Institute for Cyber Security (ICS)
Department of Computer Science
University of Texas at San Antonio

Ph.D. Dissertation Committee:

Dr. Ravi Sandhu, Chair
Dr. Murtuza Jadliwala
Dr. Palden Lama
Dr. Gregory White
Dr. Rohit Valecha

Introduction

Cloud-Enabled IoT (CE-IoT)

Security and Privacy

Internet of Things (IoT) [*]

*Source: https://en.wikipedia.org/wiki/Internet_of_things#/media/File:Internet_of_Things.jpg

Introduction

Access Control
Secure data, information, and resources from unauthorized entities

Communication Control
Secure communication and data flow from one component to other

Traditional Access Control Models:
Discretionary Access Control (DAC) – Ownership,
Mandatory Access Control (MAC) – Security Levels,
Role-Based Access Control (RBAC) – Roles,
Attribute-Based Access Control (ABAC) – Attributes, …

Communication Control Examples:
Firewall, Routing Tables, Guards, …
Formal models ???

Introduction

Cloud & CE-IoT

Access Control
Secure data, information, and resources from unauthorized entities

Communication Control
Secure communication and data flow from one component to other

Attribute-Based Approach

Attribute-Based Access Control (ABAC)

Attribute-Based Communication Control (ABCC)

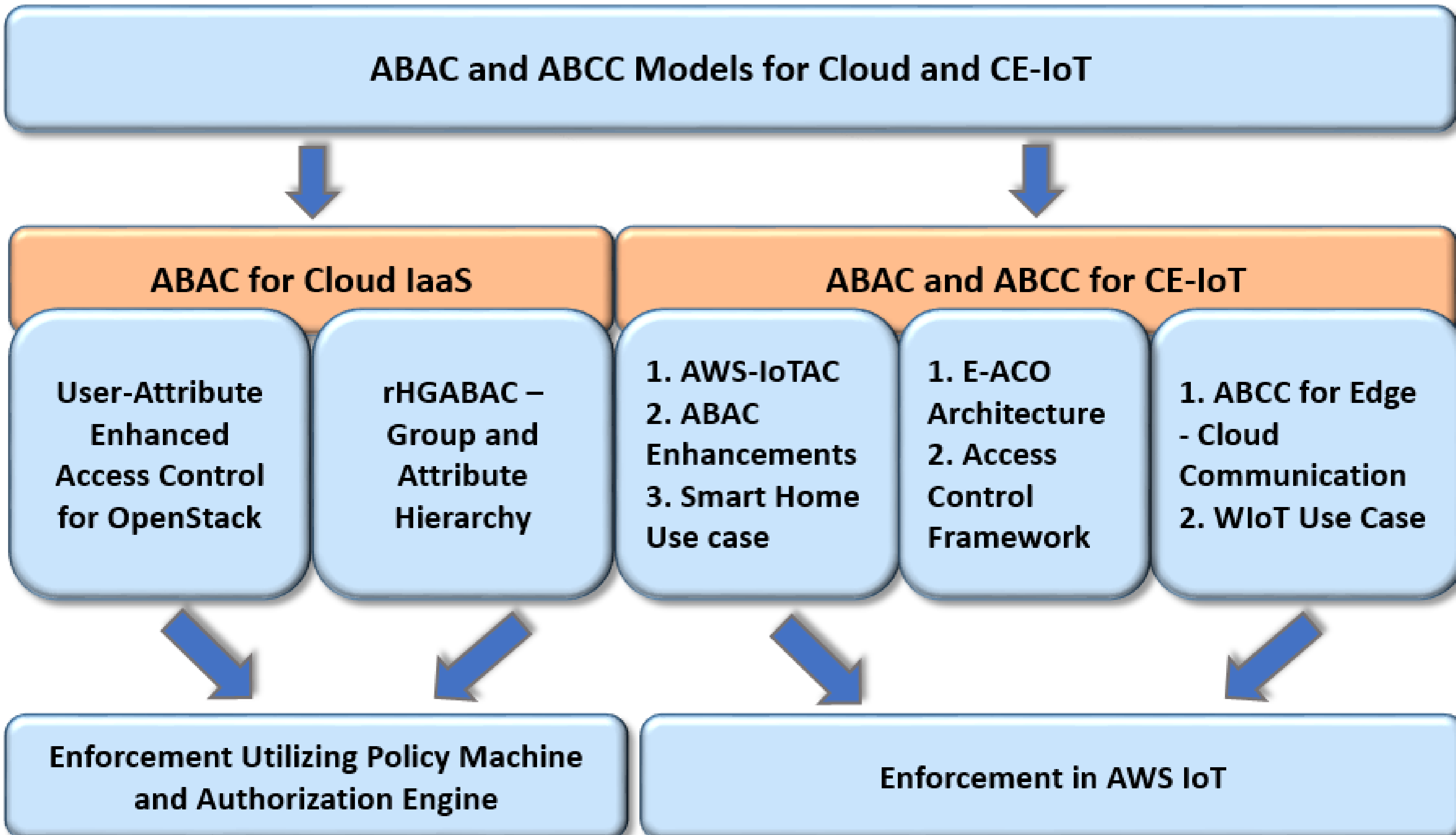
Problem Statement

- Significant gap between theoretical *ABAC* models and their application in real-world Cloud and CE-IoT platforms
- Fundamental lack of knowledge and academic literature on *Attribute-Based Communication Control (ABCC),* a novel concept
- Lack of ABCC models focused on CE-IoT context

Thesis Statement:

A flexible attribute-based approach can be utilized to address security and privacy issues in the dynamic and rapidly progressive Cloud Computing and CE-IoT architectures. A detailed exploration of ABAC and ABCC, their formal models, and implementation in different contexts concerning Cloud Computing and CE-IoT can ultimately strengthen the access, authorization, and communication framework in these domains.

Summary of Contributions



Attribute-Based Approach

Entities

User

File

IoT Devices

Attributes

name,
title,
type,
created_by,
owner,
…

Policies

Rule 1,
Rule 2,
…

Operations

read, write, send, …

Decision Function

Example: *Attribute-Based Authorization*

User (u)

name: Alice
title: Manager

Object (o)

type: Sensitive
created_by: Alice

Auth_{read} (u, o)

$\text{Auth}_{read} \equiv$ *title(u) = Manager* $\wedge$ *type(o) = Sensitive*
$\text{Auth}_{write} \equiv$ *name(u) = created_by(o)*

Background

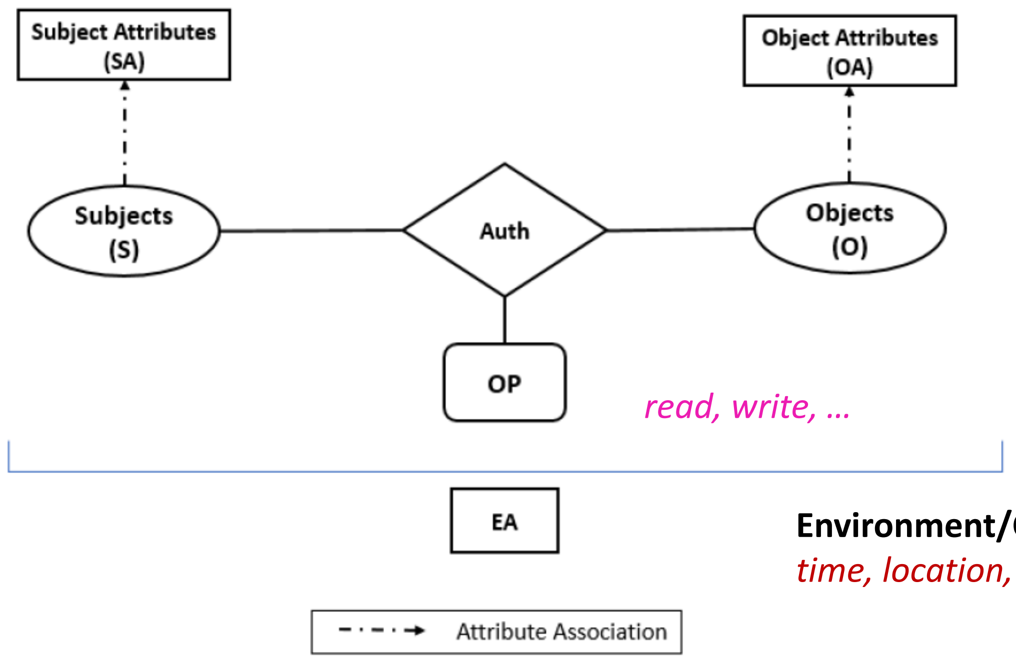
Attribute-Based Access Control

name, title, …

type, created_by, …

users, processes, …

files, databases, …

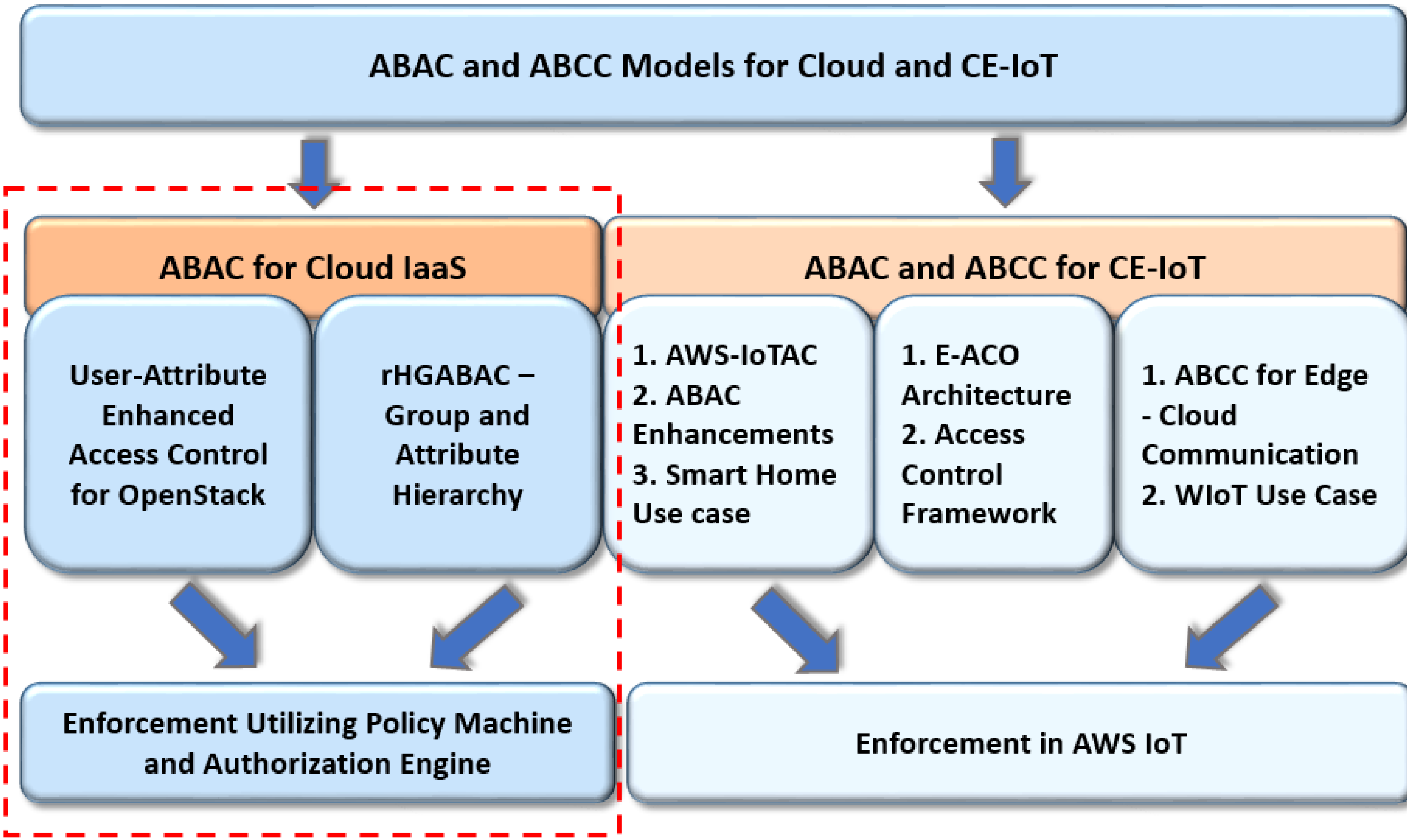


read, write, …

Environment/Context Attribute:
time, location, trust_level, …

- Next-Generation Access Control (NGAC) – By NIST
- Gartner predicts 2014 – "*By 2020, 70 percent of enterprises will use ABAC as the dominant mechanism to protect critical assets*" [source: https://www.tripwire.com/state-of-security/security-data-protection/security-controls/rbac-is-dead-now-what/]

Summary of Contributions



OpenStack Access Control (OSAC) Model

Users ←→ Roles ←→ Permissions on Objects

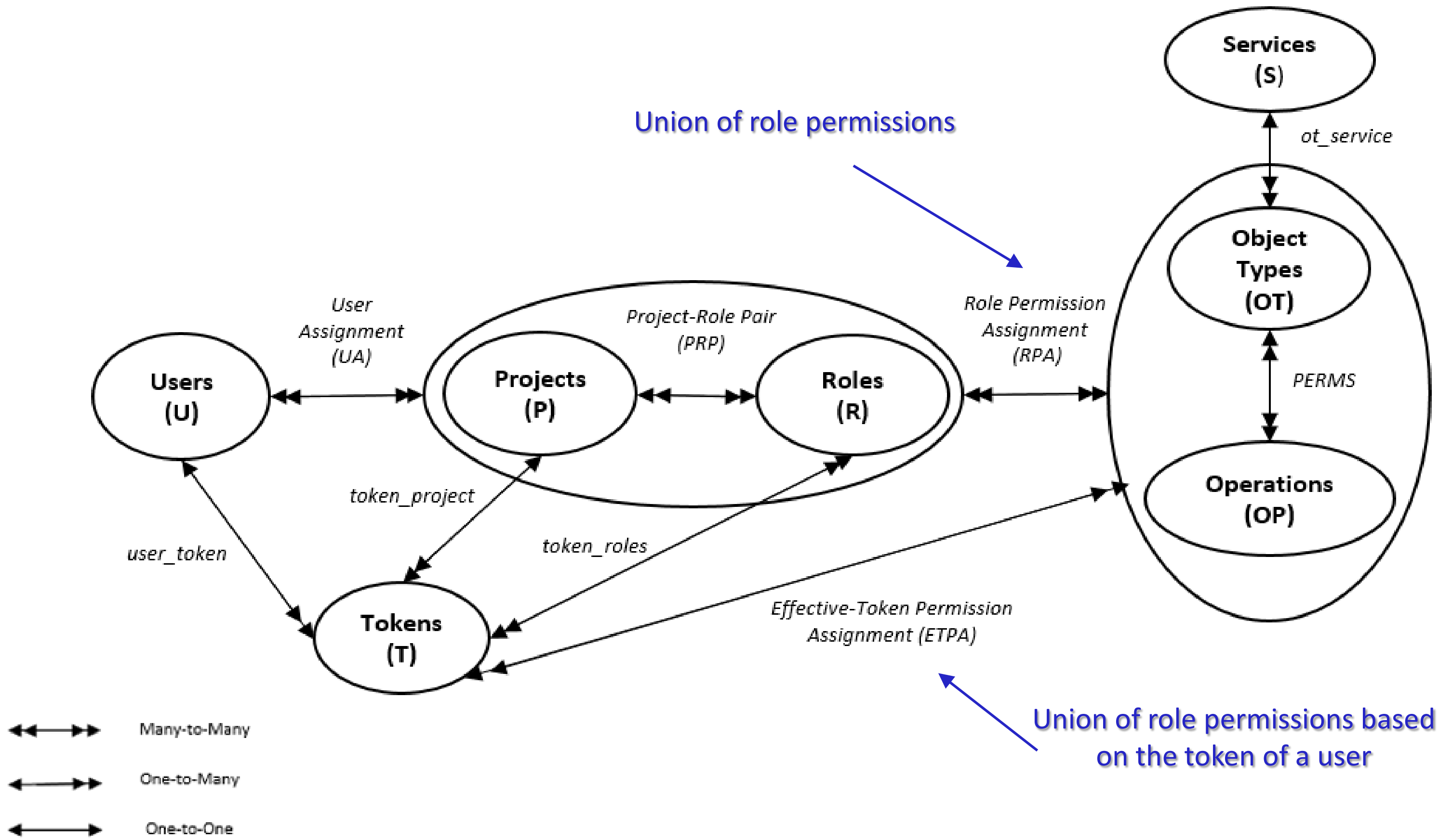
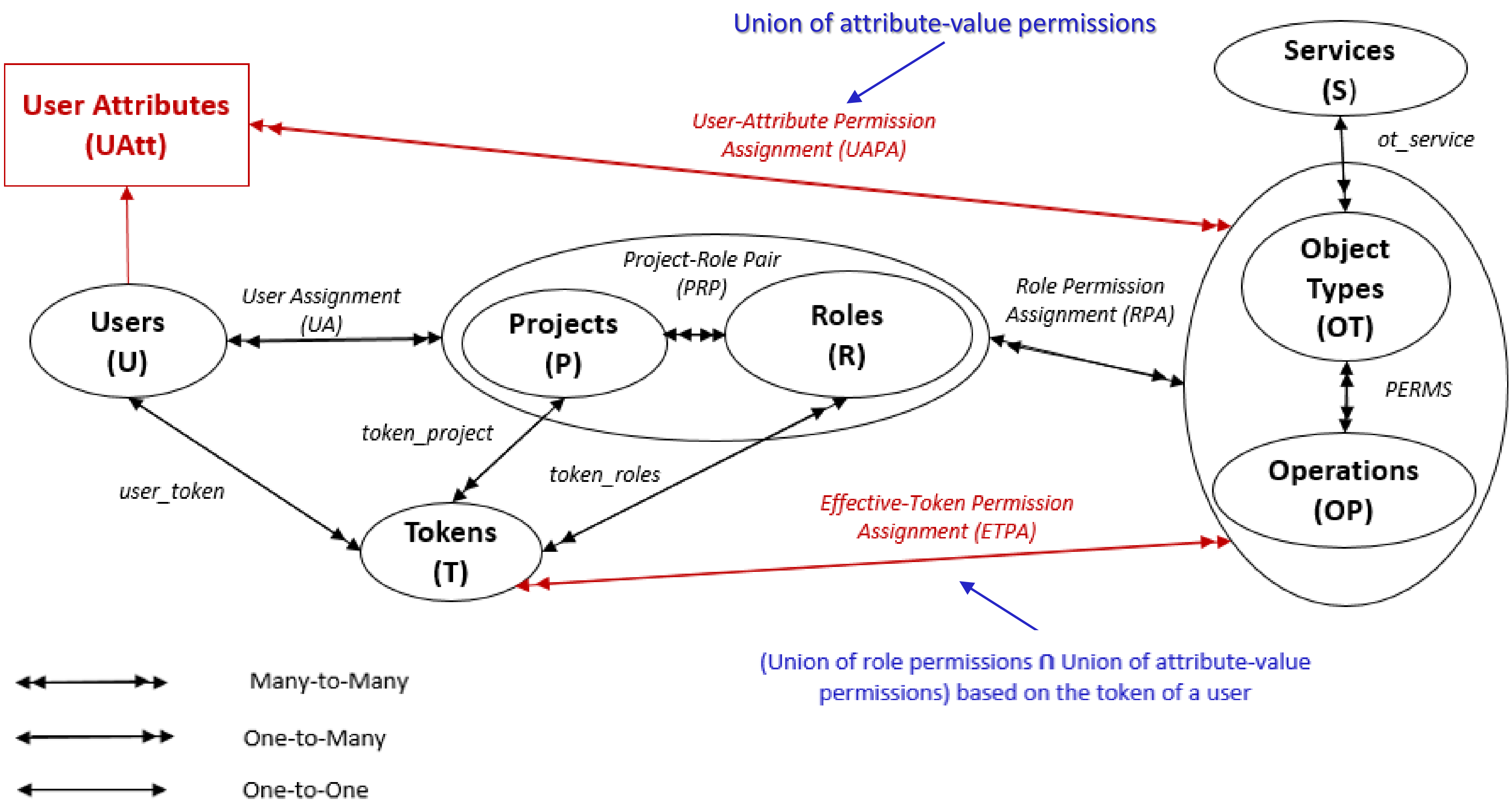


Fig. 1: Simplified OSAC Model (Adapted from Tang et al., 2014)

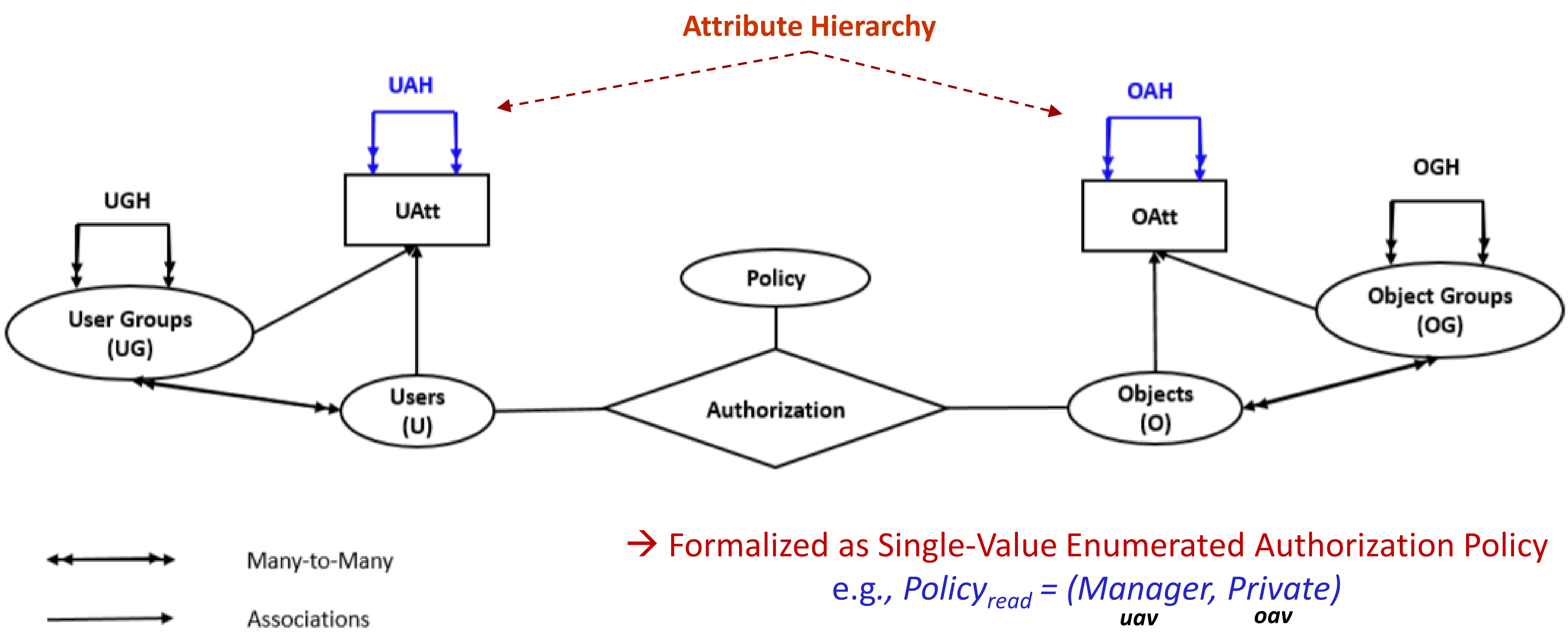
User-Attribute Enhanced OSAC Model

Role-Centric ABAC (Roles + Attributes)



rHGABAC Model

- Facilitate attribute assignment through Group and Attribute Hierarchy

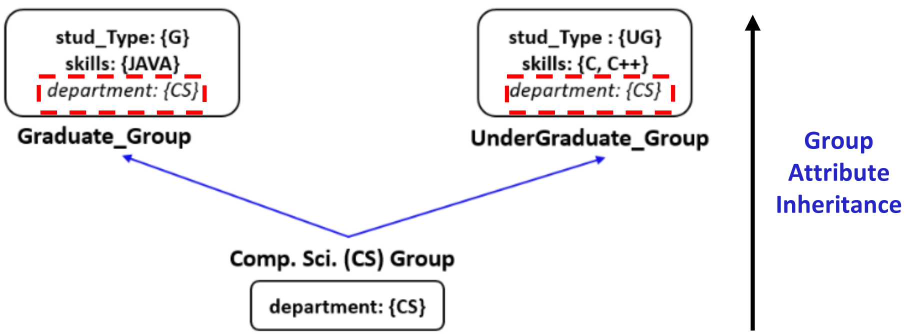


→ Formalized as Single-Value Enumerated Authorization Policy

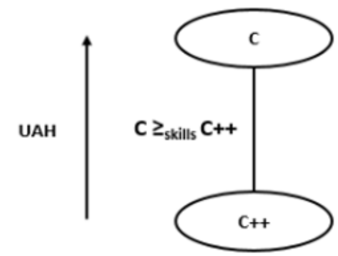
e.g., $Policy_{read} = (\underbrace{Manager}_{uav}, \underbrace{Private}_{oav})$

Fig. 2: Restricted Hierarchical Group and Attribute-Based Access Control (*rHGABAC*) Model Extended from HGABAC [Servos and Osborn, 2015]

Group and Attribute Hierarchy



a) An Example of User Group Hierarchy
(Adapted from [Gupta and Sandhu, 2016])



skills = {C, C++, Java}

b) User Attribute-value Hierarchy

Enforcement

- A *novel* enforcement architecture utilizing **Policy Machine** (by NIST) and **Authorization Engine** (our custom implementation component)
- Policy Machine (PM):
  - an open-source ABAC framework to express and enforce access control policies

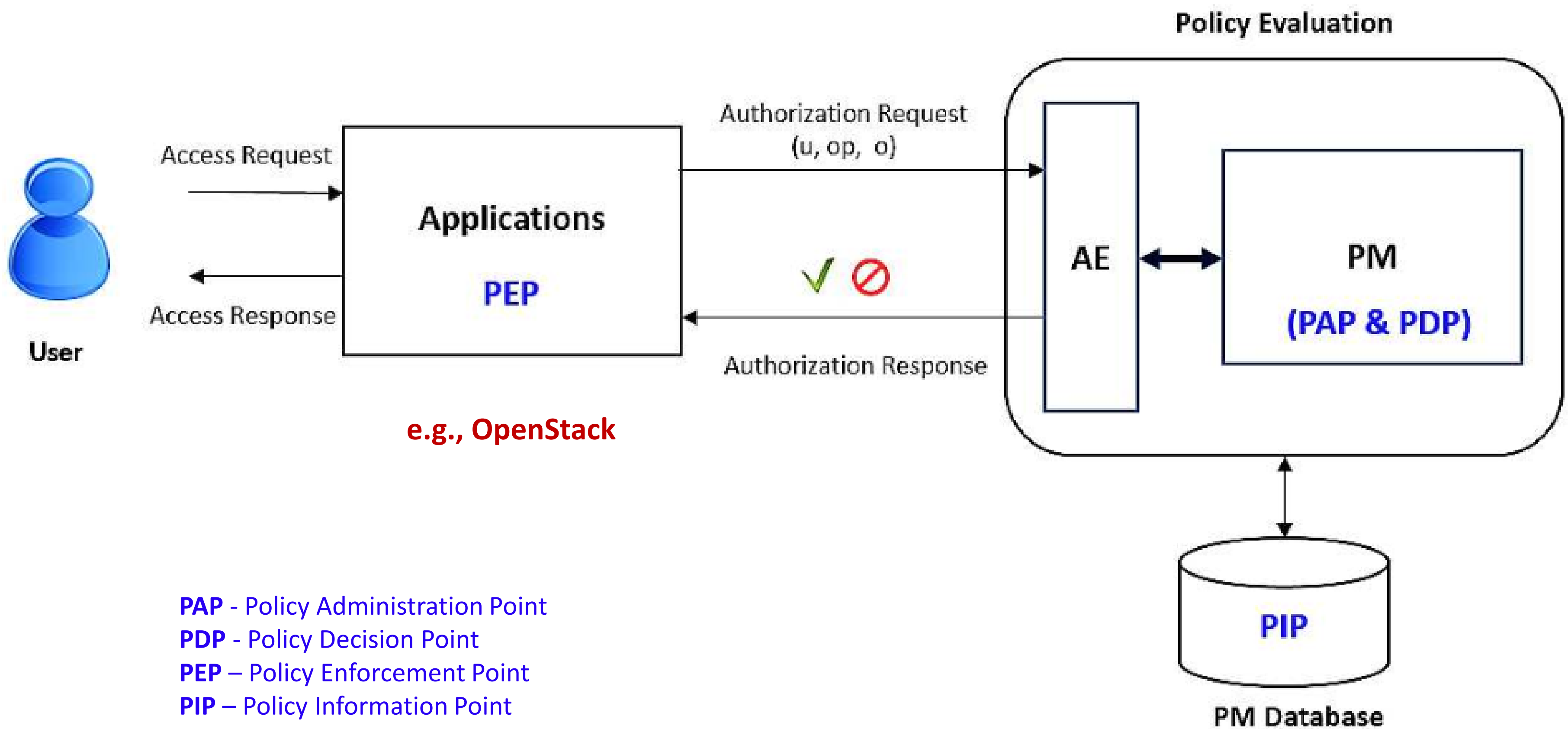
PM Core Elements
- Users
- Objects
- User Attributes
- Object Attributes
- Operations
- Policy Classes, …

PM Relations
- Assignment
- Association
- Prohibition
- Obligation

✓ **assignment**— relationships between policies, users and user attributes, objects and object attributes
✓ **association** – authorization policies based on attributes

- Authorization Engine (AE):
  - a RESTful service as an interface between PM and applications
  - provide authorization decisions (Allow/Deny)

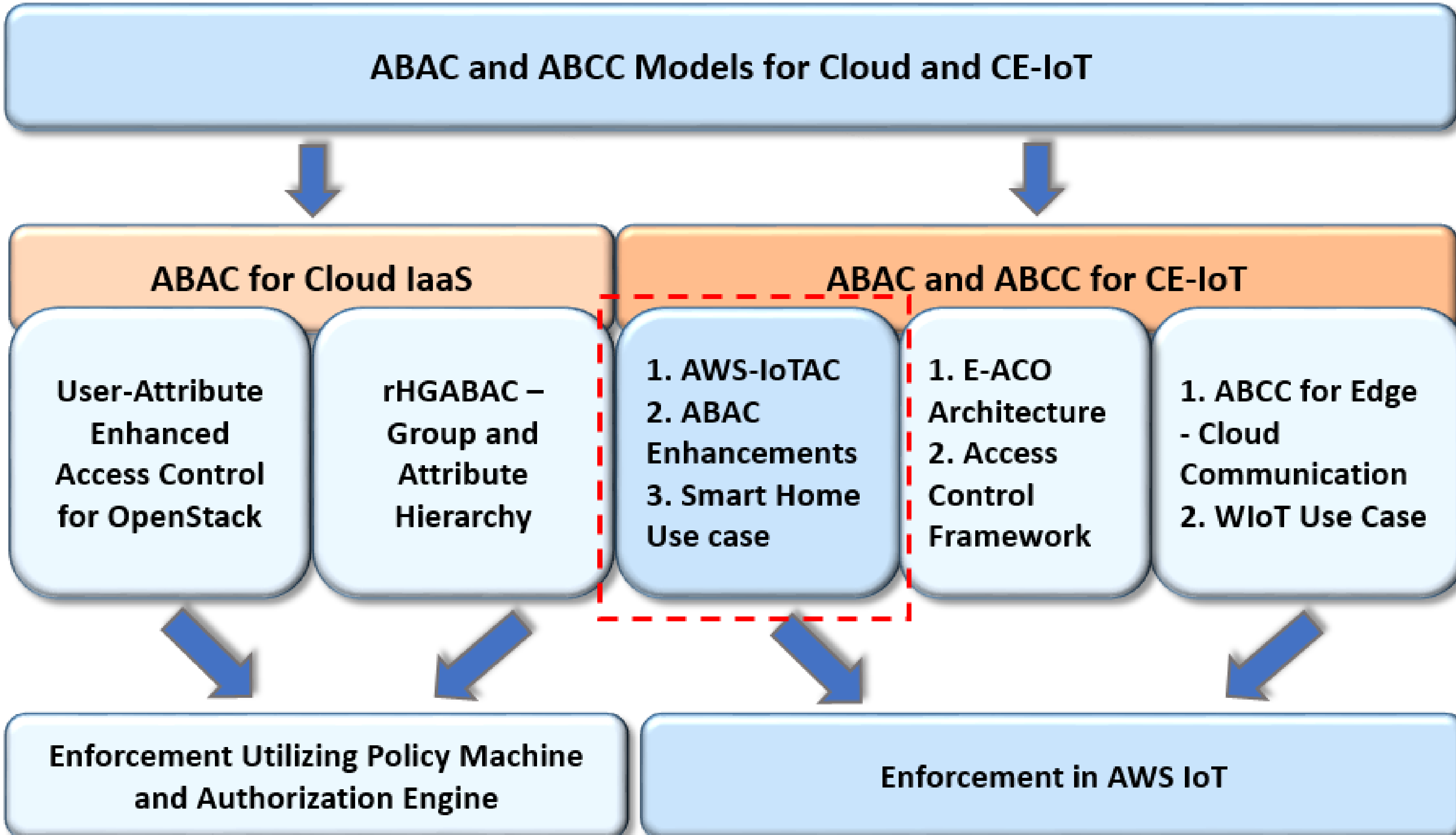
Enforcement Architecture



PAP - Policy Administration Point
PDP - Policy Decision Point
PEP – Policy Enforcement Point
PIP – Policy Information Point

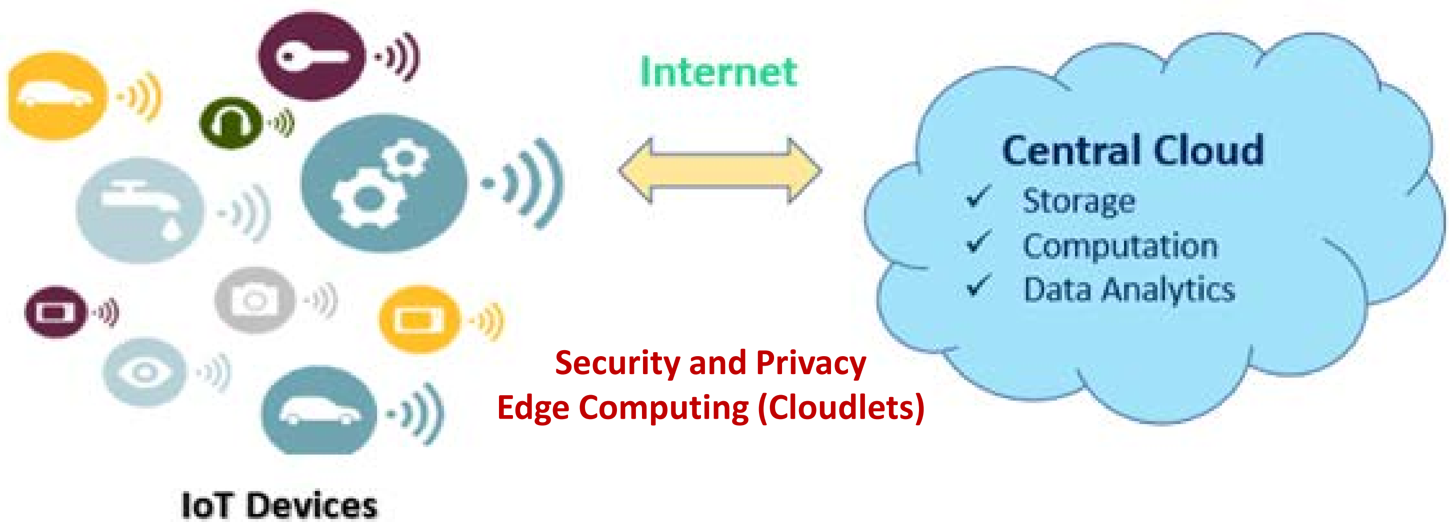
Fig. 3: Authorization Architecture Utilizing PM and AE

Summary of Contributions



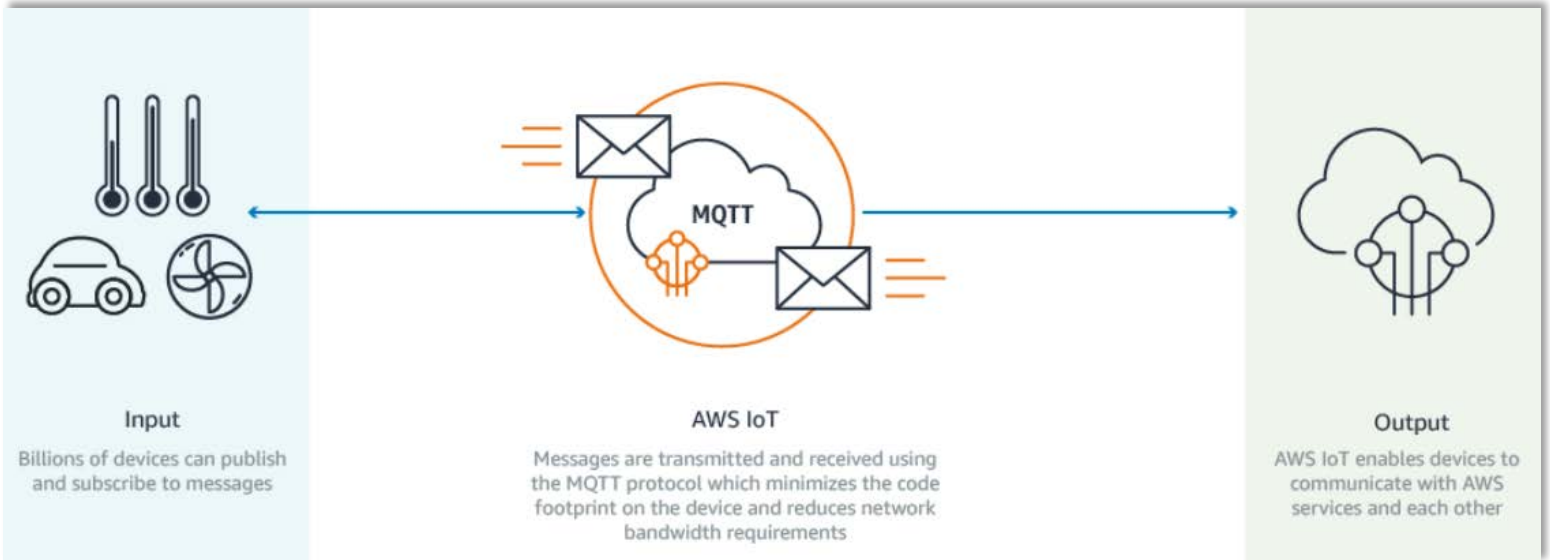
ABAC for Cloud-Enabled IoT

- **Cloud-Enabled IoT (CE-IoT)**
  - Seamless communication (devices-to-cloud, cloud-to-devices)
  - Unlimited resources → compute, storage, etc.
  - Meaningful insights → Data Analytics and Visualizations
  - Virtual things/devices management, access control management, …



AWS IoT Access Control Model

- Amazon Web Services (AWS) IoT – *a CE-IoT platform*



[Source: AWS Website]

- Currently utilize customized policy-based access control
- Lack a formal access control model for controlling access and authorization in cloud-enabled IoT

I·C·S
The Institute for Cyber Security

AWS-IoTAC Model

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

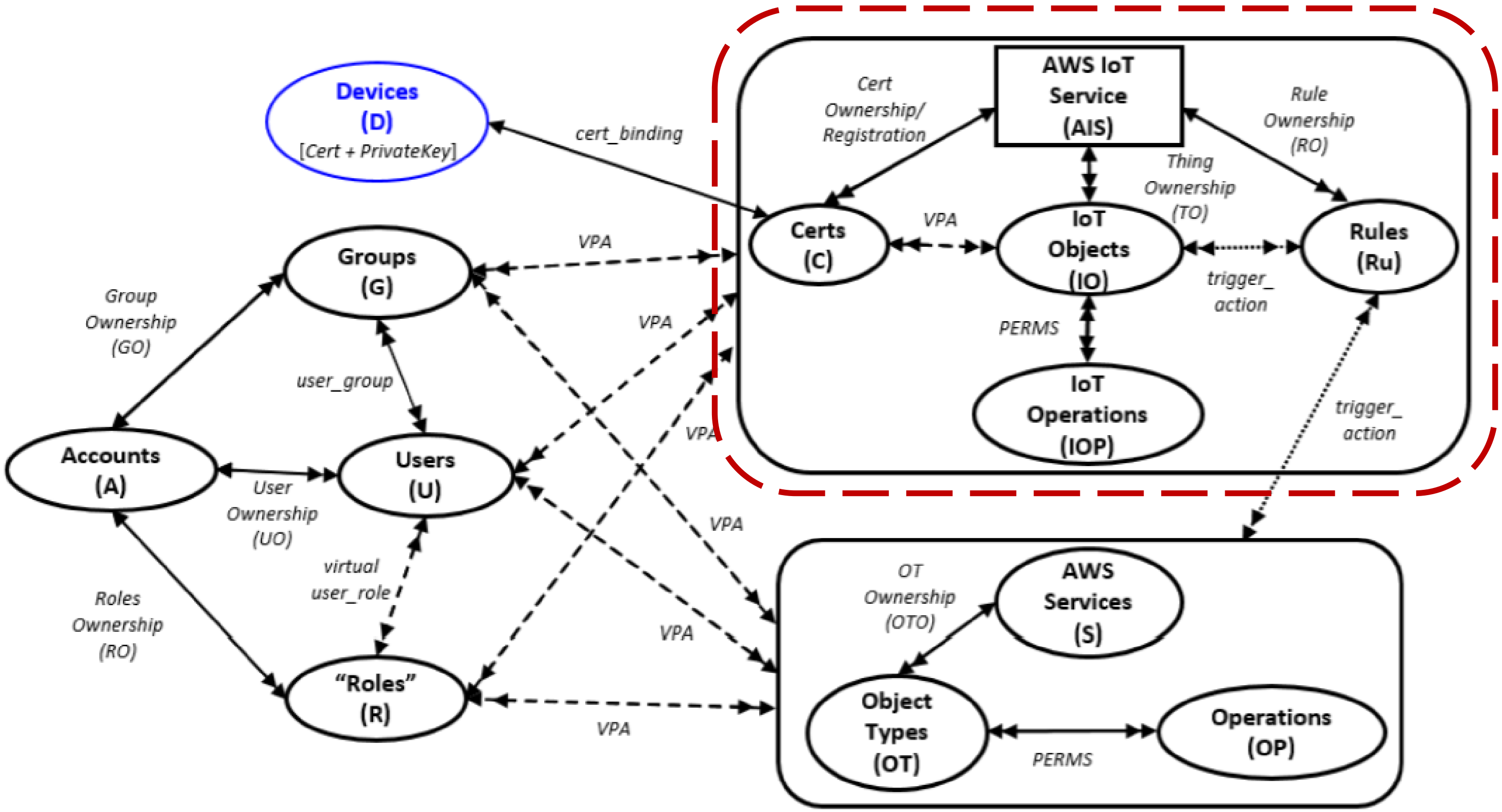


Fig. 4: AWS IoT Access Control (AWS-IoTAC) Model within a Single Account Extended from Zhang et al., 2015

Smart Home Use Case in AWS IoT

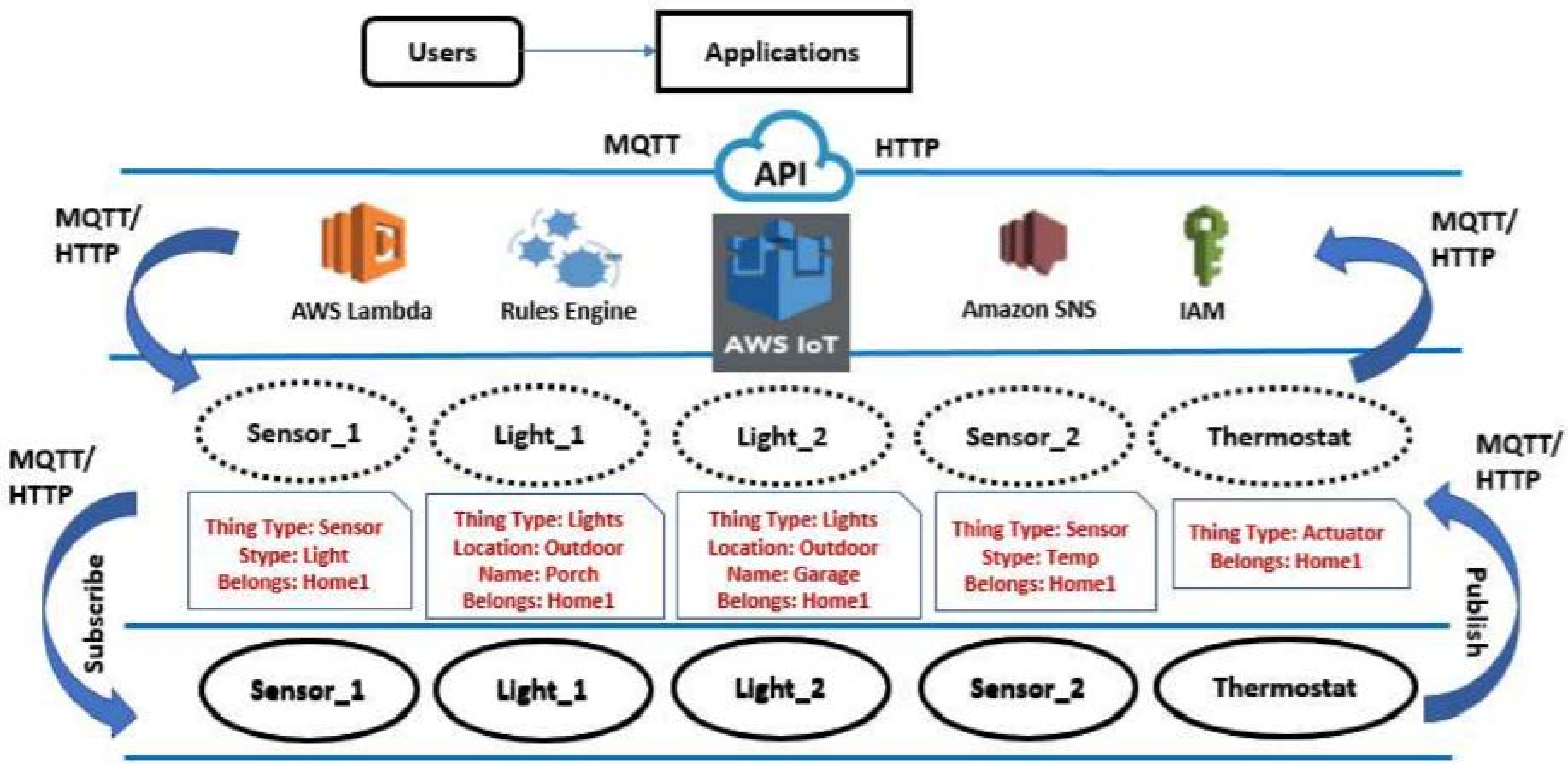
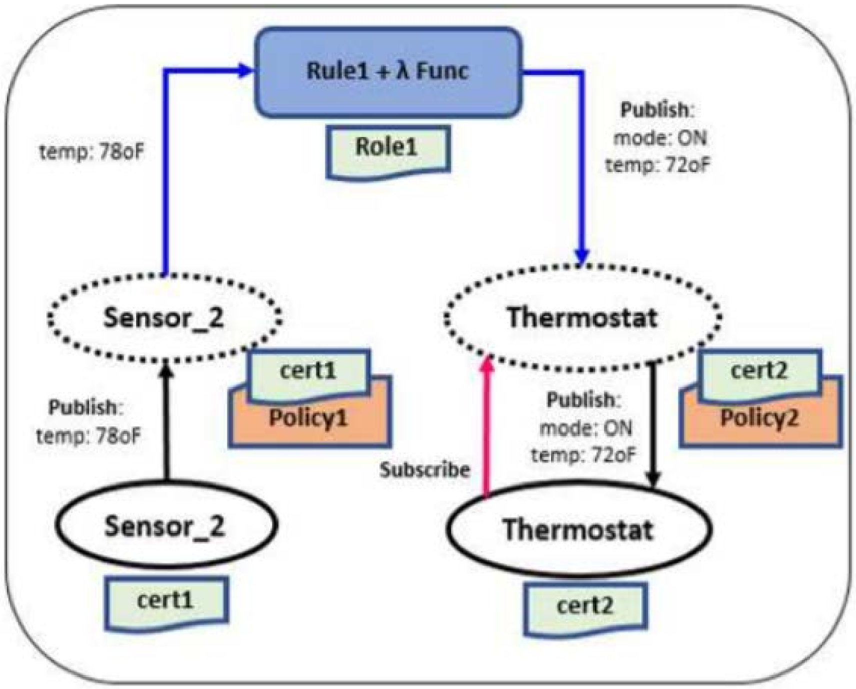


Fig. 5: Smart-Home Use Case Utilizing AWS IoT and Cloud Services

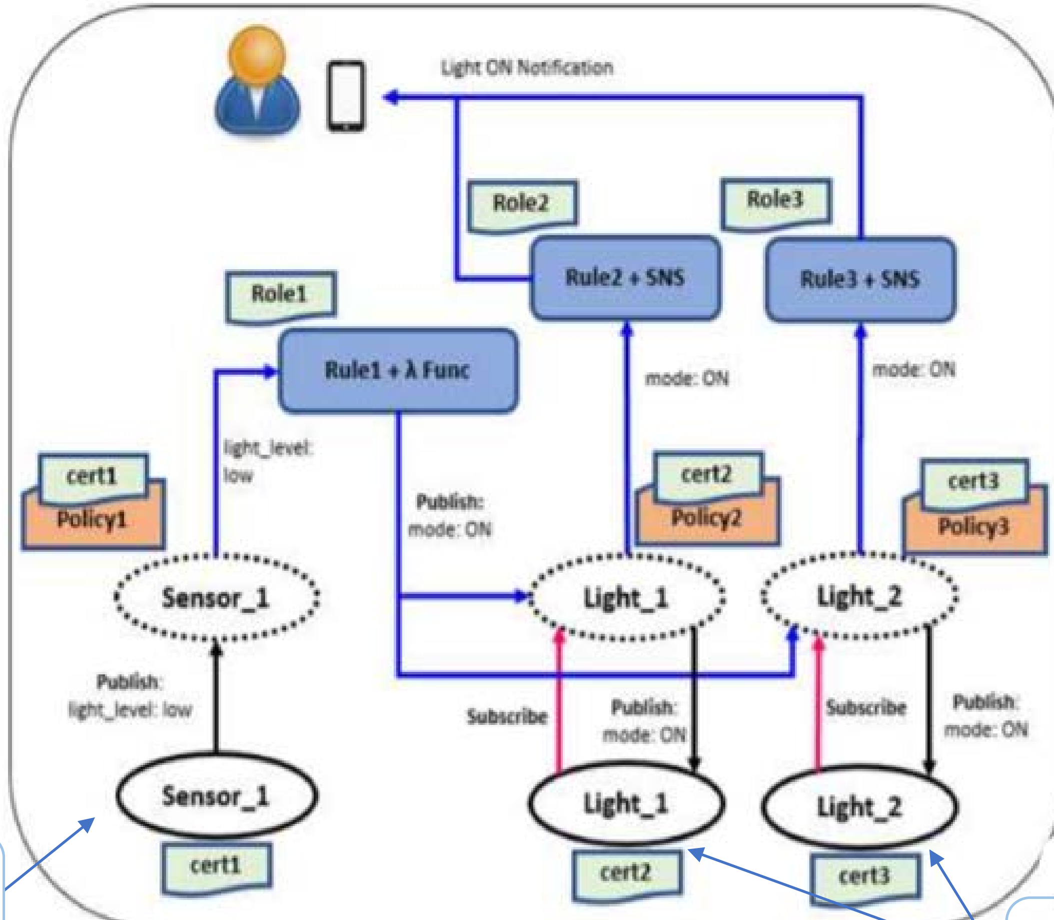
Use Case – Scenario 1



A temperature sensor and thermostat use case

Existing AWS Policy Structure:
Allows all the IoT operations on any resource in AWS IoT

Use Case – Scenario 2



Sensor Attribute:
Belongs = Home1

Light Attributes:
Location = Outdoor
Belongs = Home1

ABAC Policy – Scenario 2

❖ Utilizing target things attributes through AWS Lambda function

```
...
var params2 = {attributeName: 'Location',
               attributeValue: 'Outdoor'
 };
 iot.listThings(params2, function(err, data) {
   ...
     for (i in data.things) {
          x = data.things[i].thingName;

          var params3 = {
          topic: '$aws/things/'+x+'/shadow/update',
          payload: new Buffer('{"state": {"desired" : {"light" : "ON"}}}'),
          qos: 0
          };

        iotdata.publish(params3, function(err, data){
          ...
```

AWS Lambda Function

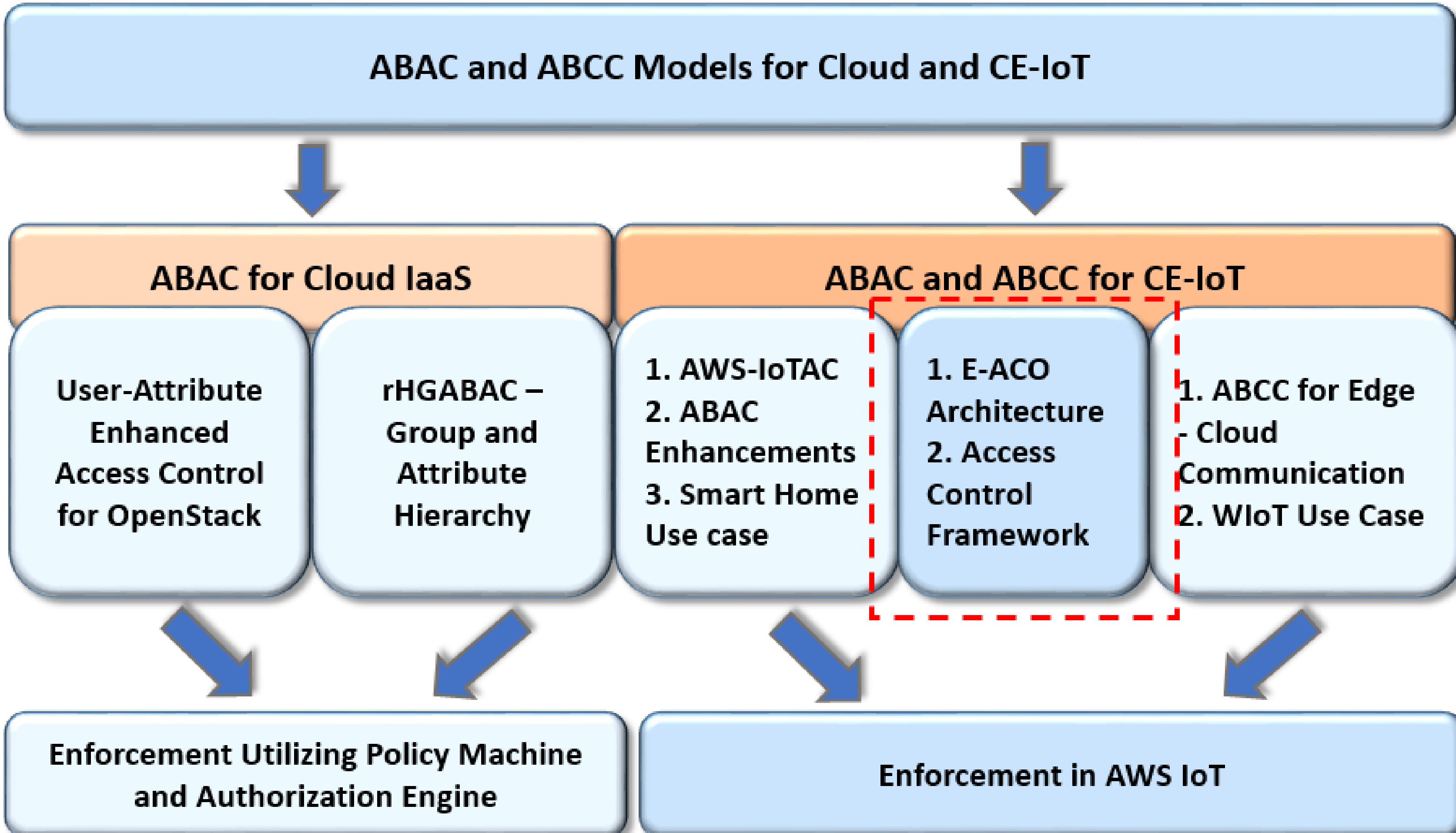
Search and list things with attribute name = *Location* & attribute value = *Outdoor*

Publish update on all thing shadows (outdoor lights here) that has attribute *"Location = Outdoor"* to turn on outdoor lights

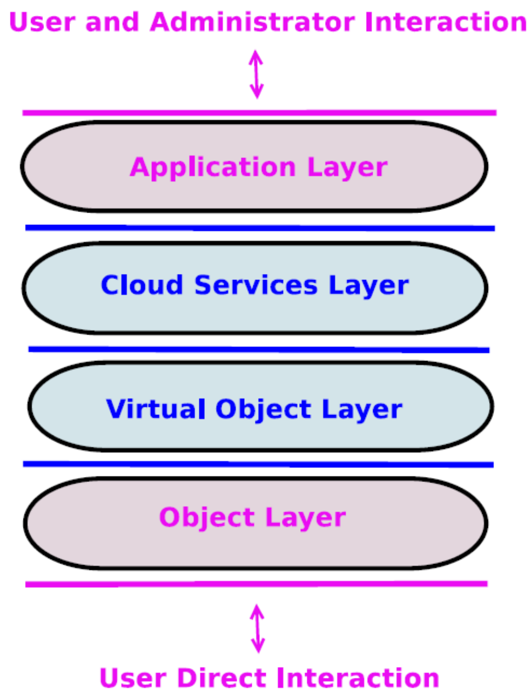
ABAC Enhancements for AWS-IoTAC

- ABAC Including Attributes of Target Resources
  - Attributes of source and target things
- ABAC Including User and Group Attributes
  - Attributes besides thing attributes in access control policies
- Policy Management Utilizing the Policy Machine
  - Policy-Explosion
  - Customized policy management for enterprises

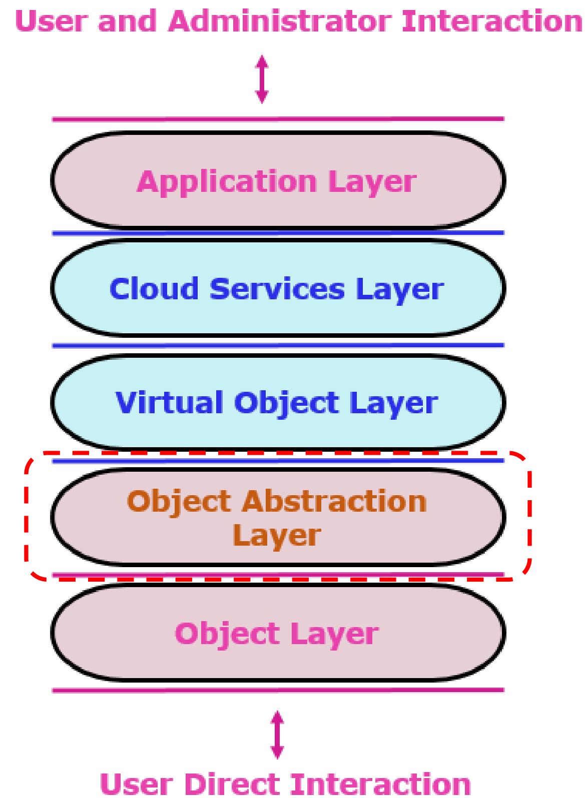
Summary of Contributions



Enhanced ACO Architecture for CE-IOT



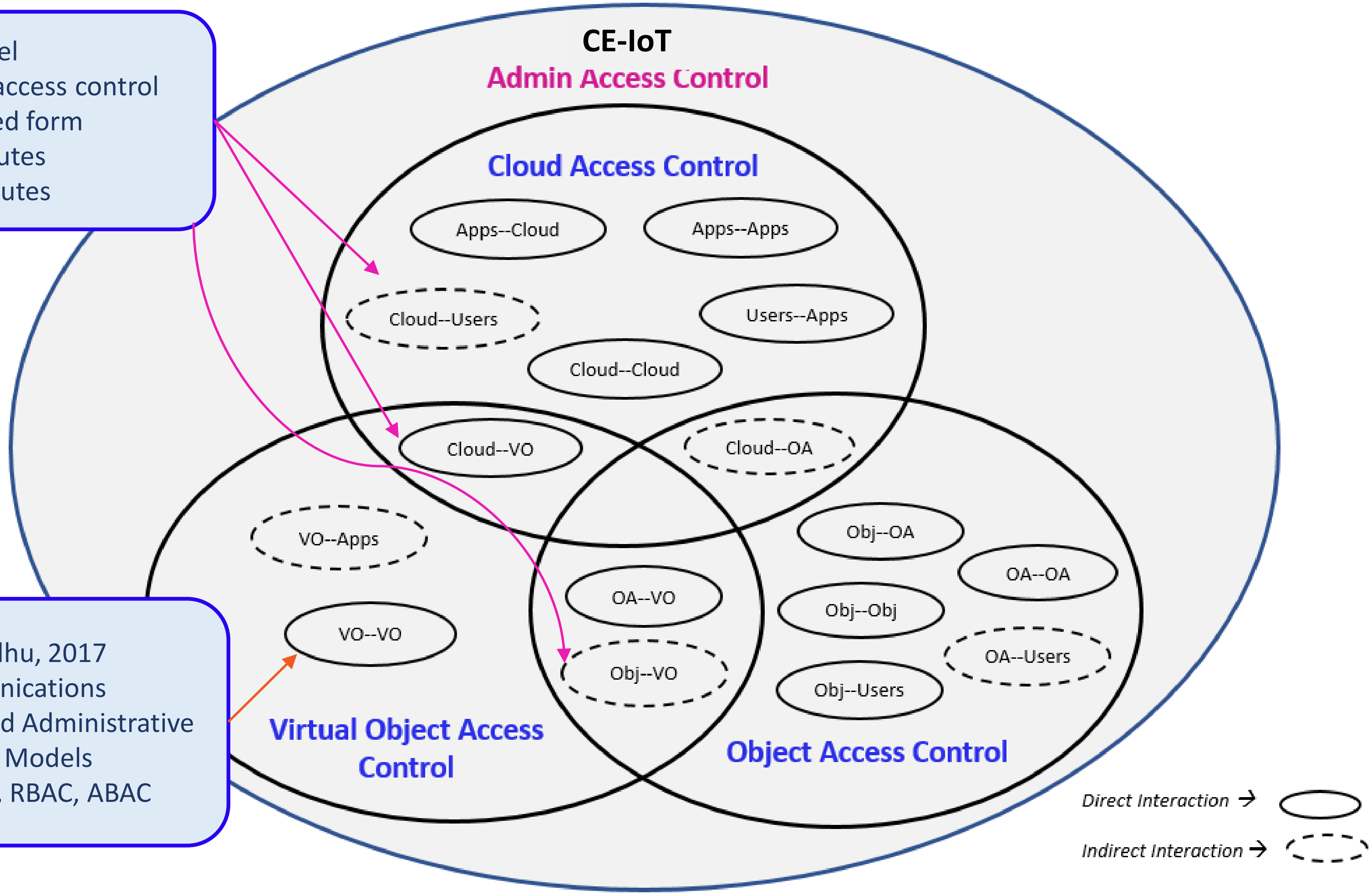
a) Access Control Oriented (ACO) Architecture [Alshehri and Sandhu, 2016]



b) Enhanced ACO (E-ACO) Architecture

Access Control Framework

AWS-IoTAC Model
- Policy-based access control
- ABAC in limited form
  - Client Attributes
  - Target Attributes



Alshehri and Sandhu, 2017
- VO-VO communications
- Operational and Administrative Access Control Models
  - ACLs, CapBAC, RBAC, ABAC

Wearable IoT Use Case

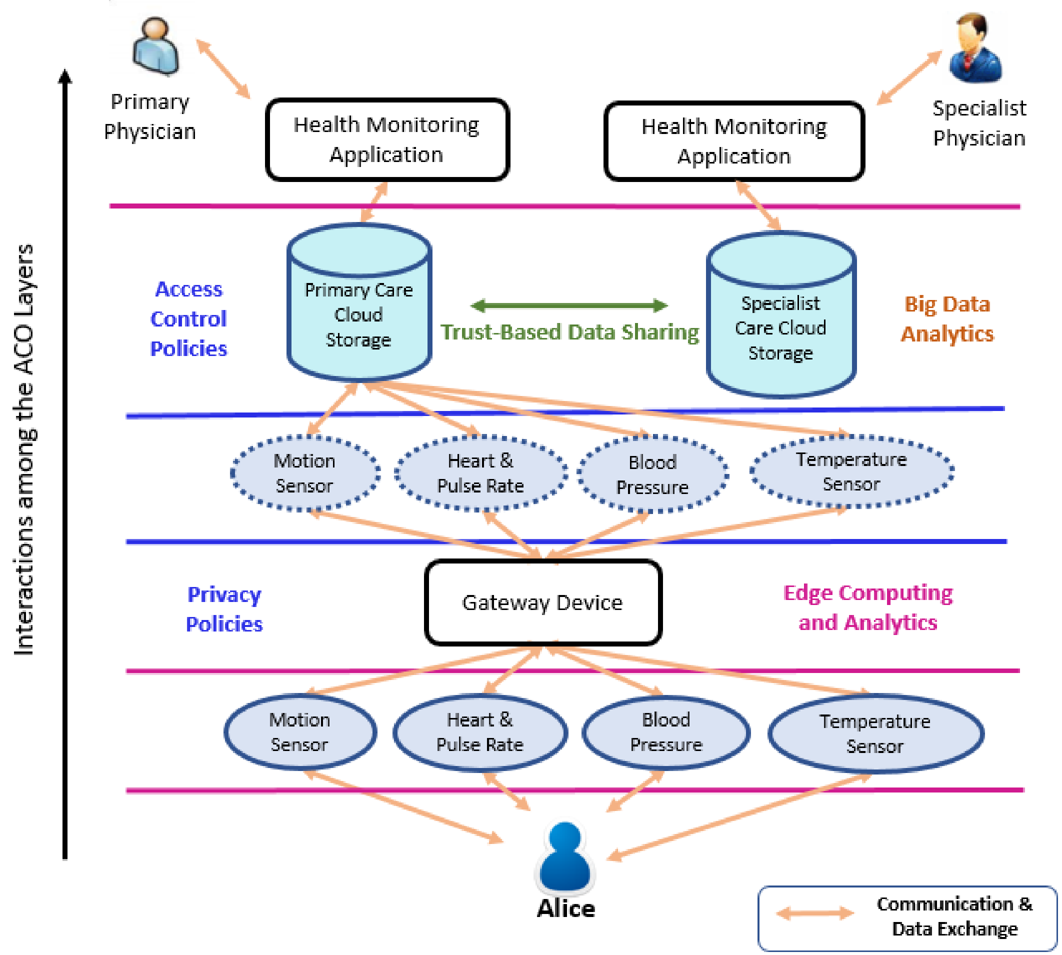


Fig. 6: Remote Health and Fitness Monitoring (RHFM) Example

Summary of Contributions

I·C·S The Institute for Cyber Security

C·SPECC Center for Security and Privacy Enhanced Cloud Computing

ABAC and ABCC Models for Cloud and CE-IoT

ABAC for Cloud IaaS

User-Attribute Enhanced Access Control for OpenStack

rHGABAC – Group and Attribute Hierarchy

ABAC and ABCC for CE-IoT

1. AWS-IoTAC
2. ABAC Enhancements
3. Smart Home Use case

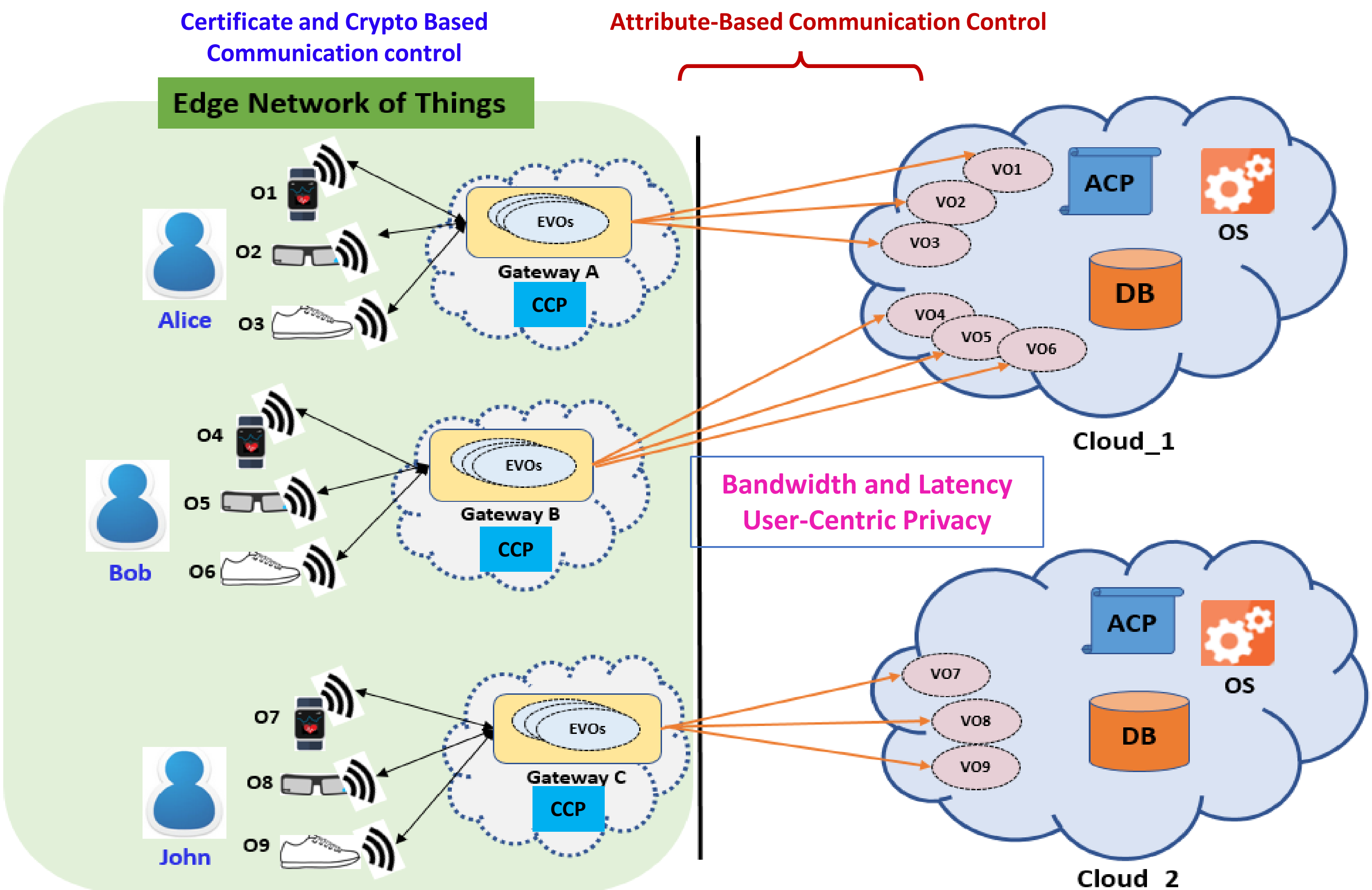
1. E-ACO Architecture
2. Access Control Framework

1. ABCC for Edge - Cloud Communication
2. WIoT Use Case

Enforcement Utilizing Policy Machine and Authorization Engine

Enforcement in AWS IoT

Communication Control in CE-IoT



Objects → **O** | Virtual Objects → **VO** | Edge virtual objects → **EVOs** | Access Control Policies → **ACP** | Communication Control Policies → **CCP** | Database → **DB** | Other Services → **OS**

A Conceptual ABCC Model

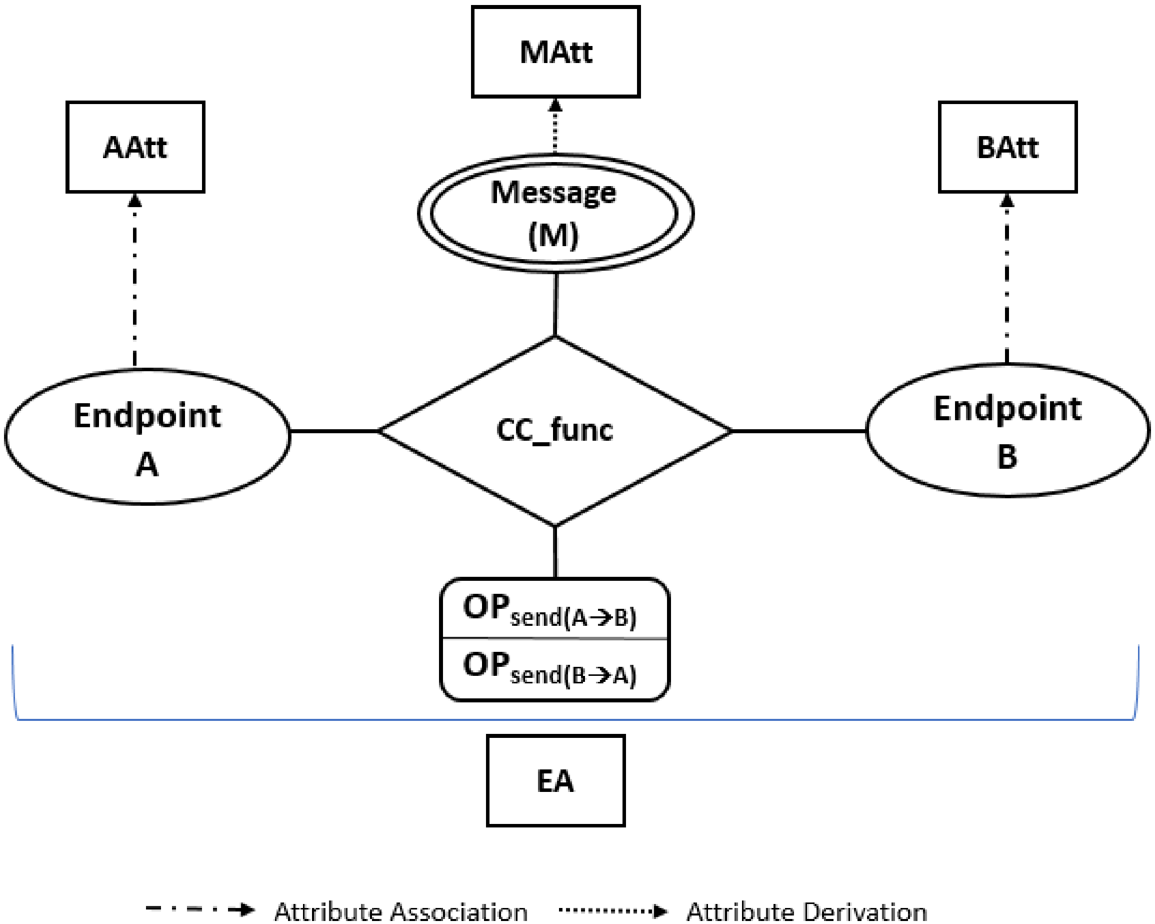
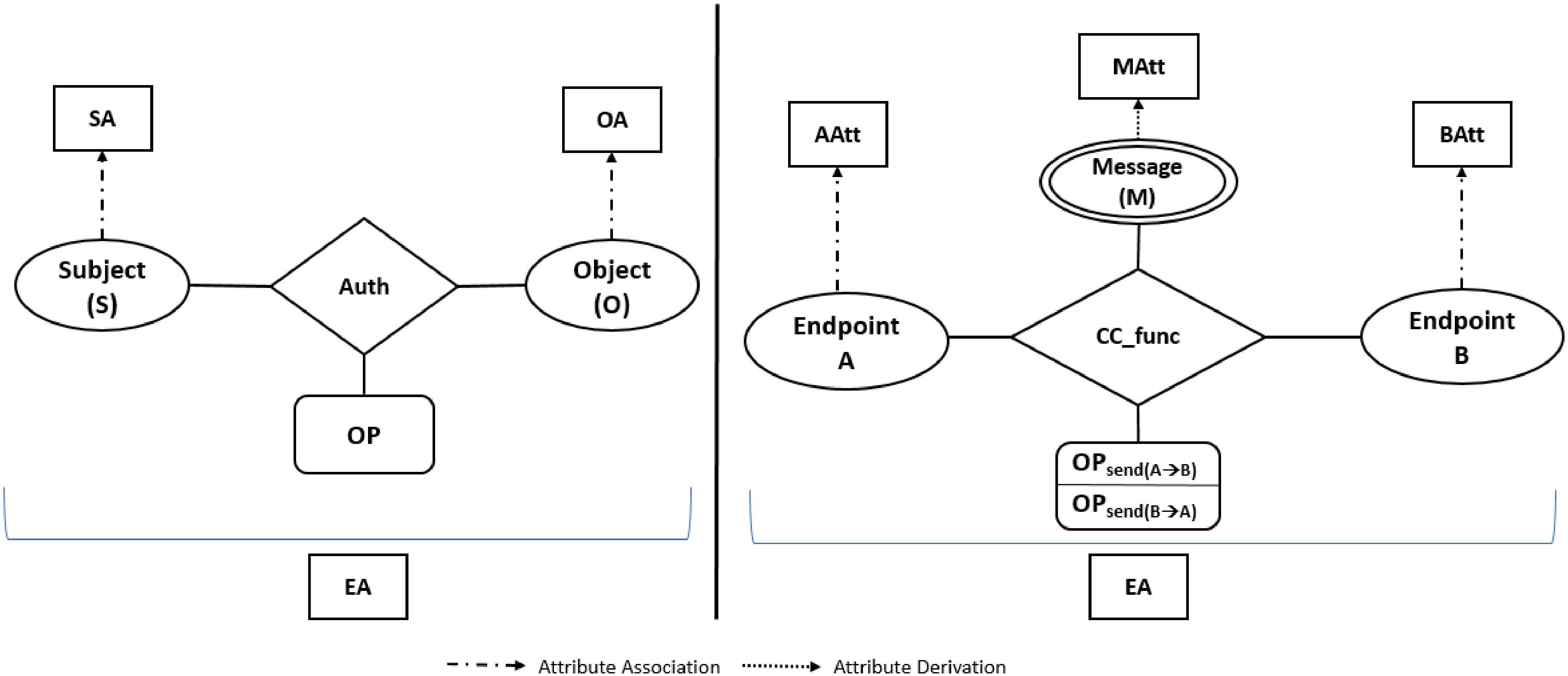


Fig. 7: A General Conceptual Attribute-Based Communication Control (ABCC) Model

ABAC vs. ABCC



a) Attribute-Based Access Control (ABAC) Model

b) Attribute-Based Communication Control (ABCC) Model

World-Leading Research with Real-World Impact!

ABCC for Edge and Cloud Communication

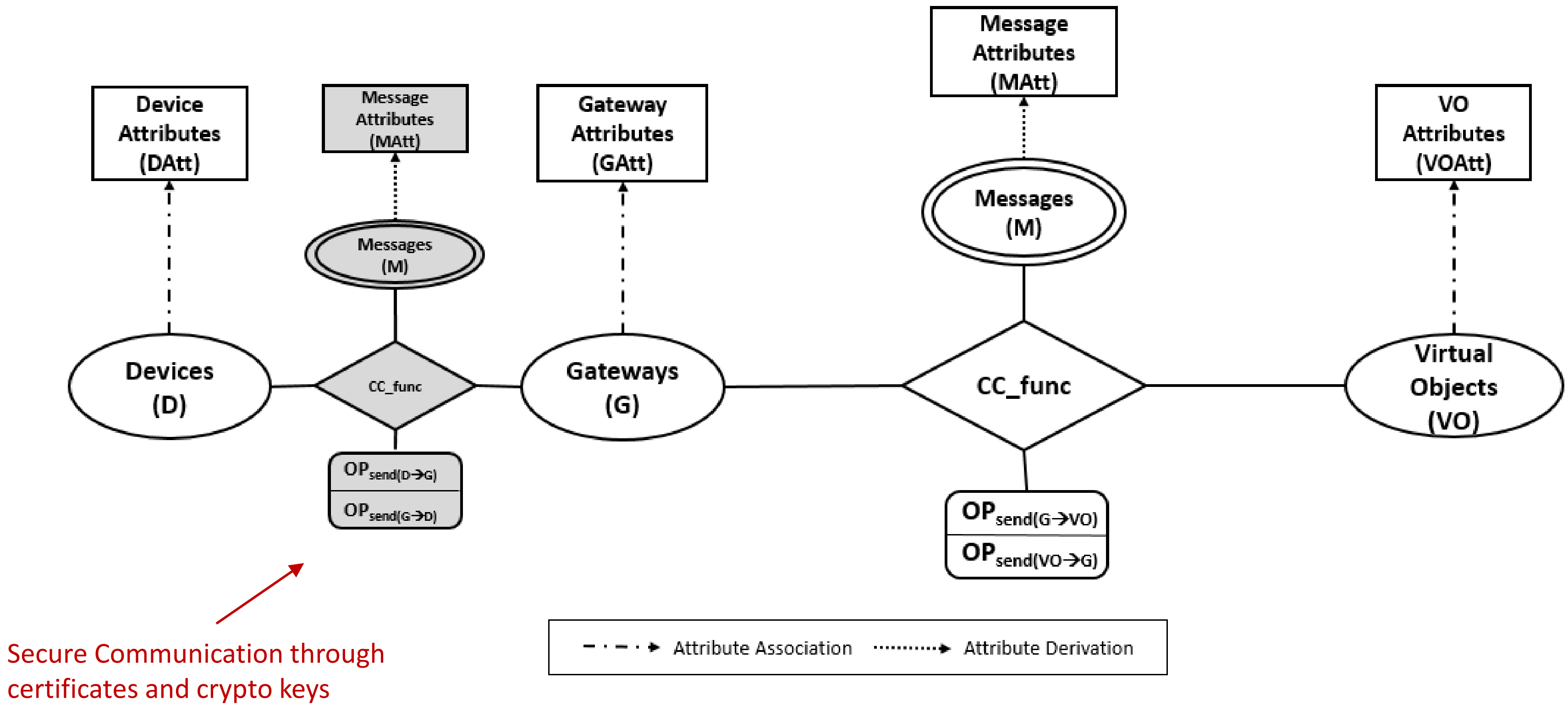


Fig. 8: ABCC for Edge and Cloud Communication Model

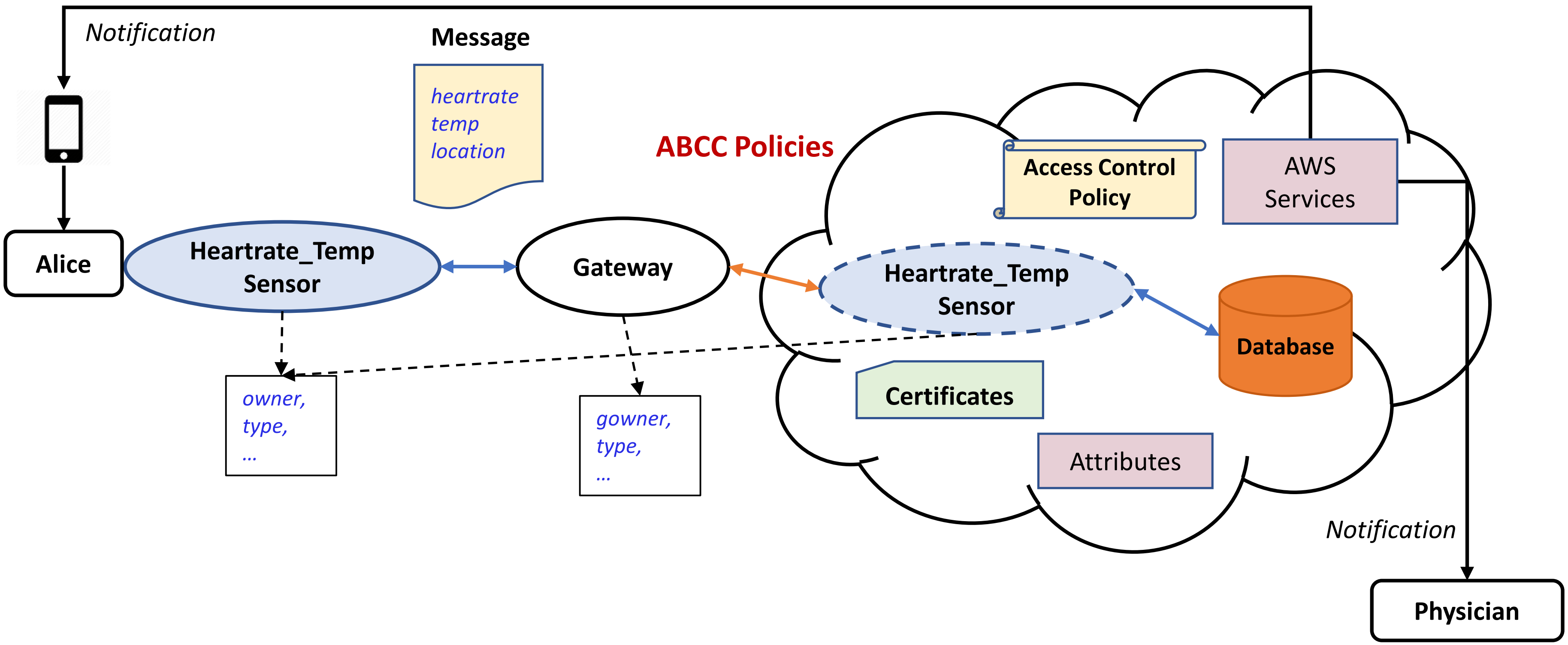
ABCC Components

- Basic Entities and Functions:
  - Two endpoints – *gateway* and *virtual object*
  - *Message* – the control unit (device data messages)
  - *Attributes* of entities (gateways, virtual objects, messages, contextual)
  - Message attributes within the message *(key, value(s))*
  - Operation – *send*
  - Communication Control Function
    - Communication Control Policies based on attributes

Communication Control Decision →

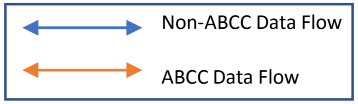
- ***Send Allow***
  send (m) → m
- ***Send Filtered***
  send (m) → m'
- ***Send Deny***
  send (m) → Ø

Use Case



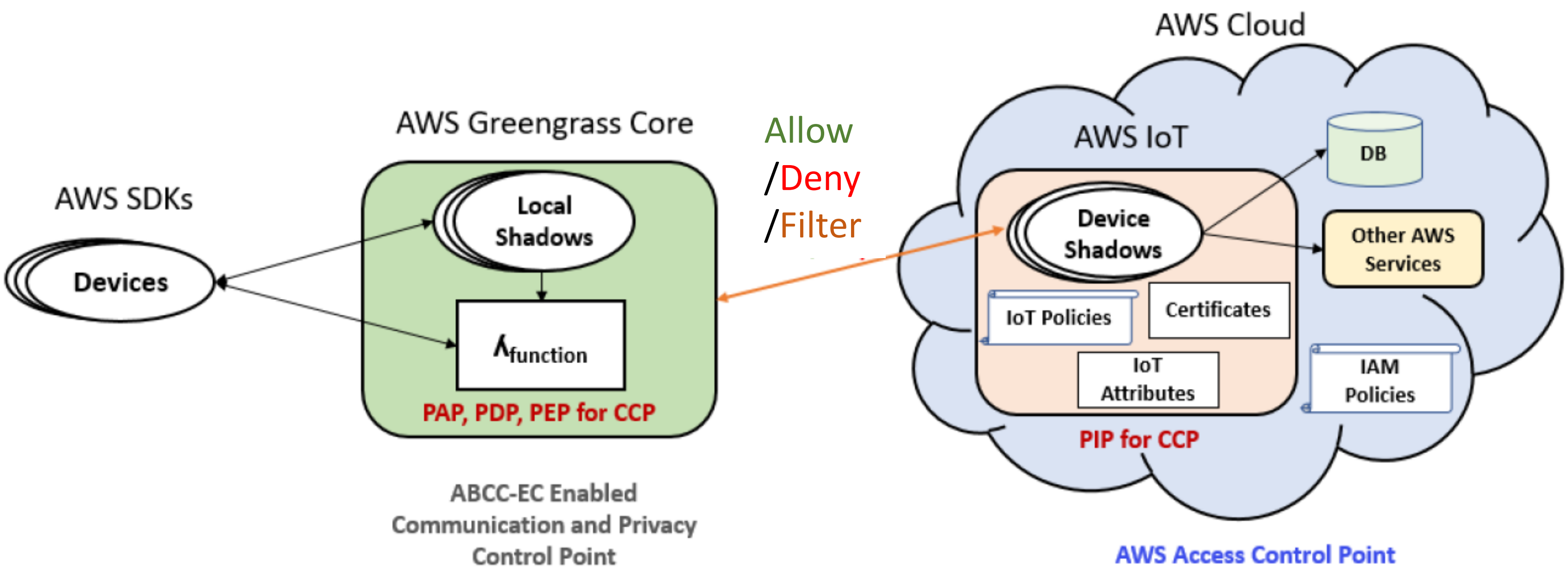
ABCC Policies

- Send Allow → *gowner(g) = owner(vo) ^ heartrate(m) >= 150 ^ temp(m) > 104*
- Send Filtered → *gowner(g) = owner(vo) ^ heartrate(m) <= 75 (filter location)*
- Send Deny → *If policy evaluation failed (e.g., gowner(g) ≠ owner(vo))*



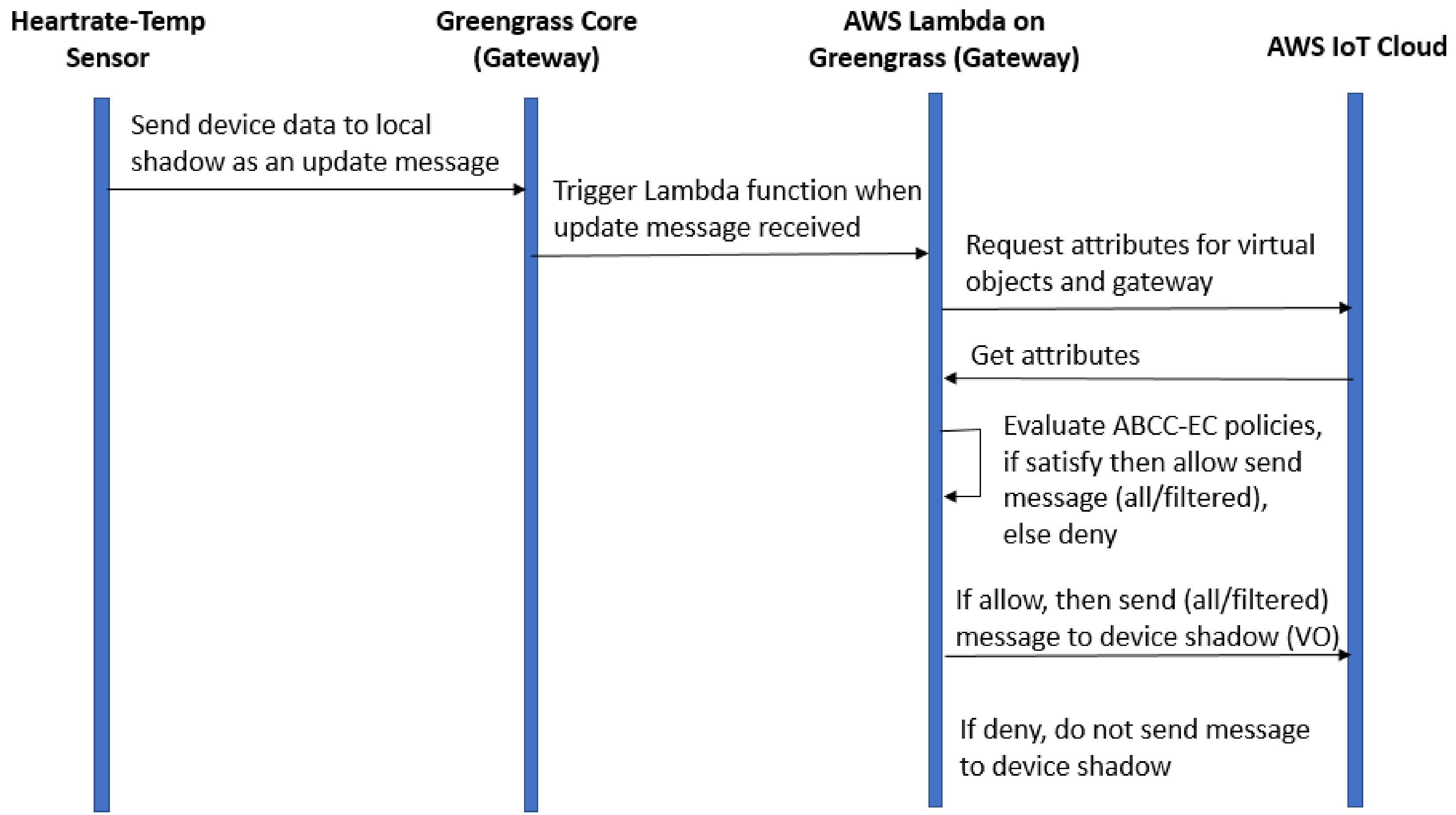
Enforcement in AWS IoT

- AWS IoT and AWS Greengrass (Edge Computing Service)



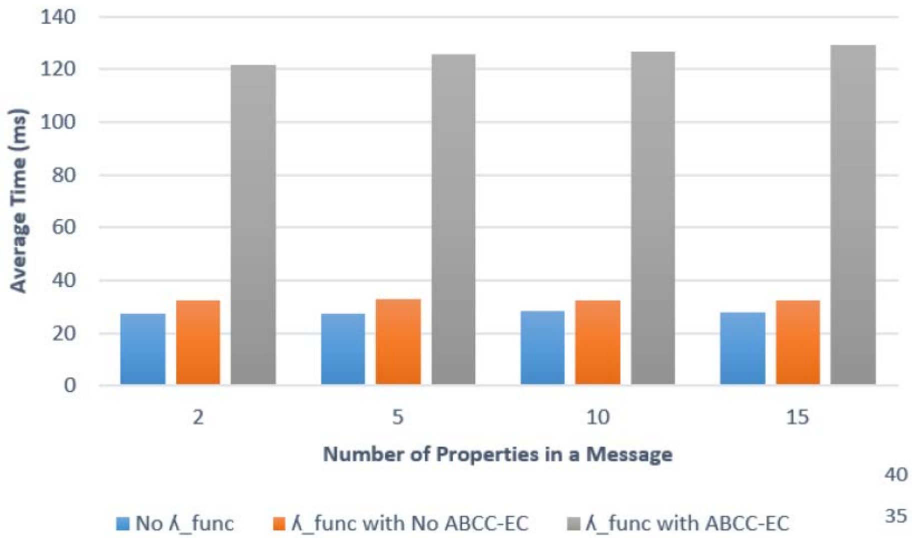
PAP – Policy Administration Point
PDP – Policy Decision Point
PEP – Policy Enforcement Point
PIP – Policy Information Point

Sequence Diagram

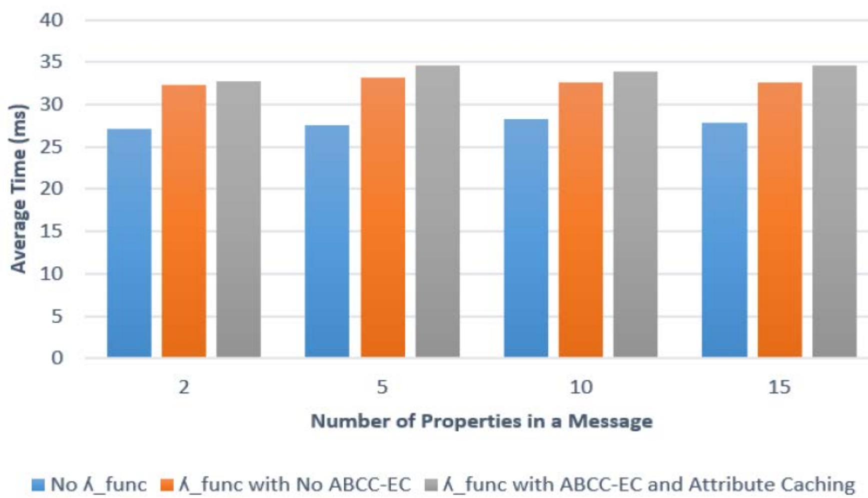


Evaluation

Device Shadow Update Time



Attribute Caching



Conclusion

- Developed and implemented ABAC and ABCC models in different context of Cloud and CE-IoT
- Presented novel enforcement frameworks to implement our models in real-world platforms
- Main goal of this research:
  - To depict the applicability and benefits of the attribute-based approach for access and communication control in Cloud and CE-IoT
  - To stimulate implementation and adoption of ABAC and ABCC models in real-world scenarios

Future Work

- ABAC and ABCC in context of Multi-Cloud architectures
- ABAC and ABCC in other application domains with additional capabilities (e.g., *Trust mechanisms*)
- Applicability of ABCC in critical domains: *Battlefield IoT, Medical/Healthcare IoT, and Vehicular IoT*

Dissertation Publications

Published:

- Smriti Bhatt, Farhan Patwa and Ravi Sandhu, An Access Control Framework for Cloud-Enabled Wearable Internet of Things. In Proceedings of the 3rd IEEE International Conference on Collaboration and Internet Computing (CIC), San Jose, CA, October 15-17, 2017, 11 pages.
- Smriti Bhatt, Farhan Patwa and Ravi Sandhu, Access Control Model for AWS Internet of Things. In Proceedings of the 11th International Conference on Network and System Security (NSS), Helsinki, Finland, August 21-23, 2017, 15 pages.
- Smriti Bhatt, Farhan Patwa and Ravi Sandhu, ABAC with Group Attributes and Attribute Hierarchies Utilizing the Policy Machine. In Proceedings of the 2nd ACM Workshop on Attribute-Based Access Control (ABAC), March 24, 2017, Scottsdale, Arizona, 12 pages.
- Smriti Bhatt, Farhan Patwa and Ravi Sandhu, An Attribute-Based Access Control Extension for OpenStack and its Enforcement Utilizing the Policy Machine. In Proceedings of the 2nd IEEE International Conference on Collaboration and Internet Computing (CIC), Pittsburgh, PA, November 1-3, 2016, 9 pages.

In preparation:

- Smriti Bhatt, Farhan Patwa and Ravi Sandhu, Attribute-Based Communication Control in Cloud-Enabled Internet of Things. Venue TBD.

Thank you!

Questions?