Access Control Model for AWS Internet of Things

Prof. Ravi Sandhu
Executive Director and Endowed Chair

11th International Conference on Network and System Security (NSS)
Helsinki, Finland, 21-23 August, 2017

Smriti Bhatt, Farhan Patwa and Ravi Sandhu
Department of Computer Science

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

Outline

- Introduction
- Contribution
- AWS Access Control (AWSAC) Model
- Access Control Model for AWS IoT
- ACO Architecture for Cloud-Enabled IoT & AWS-IoTAC
- Use Case in AWS IoT
  - Use Case – Scenario 1
  - Use Case – Scenario 2
- ABAC Enhancements for AWS-IoTAC
- Conclusion and Future Work

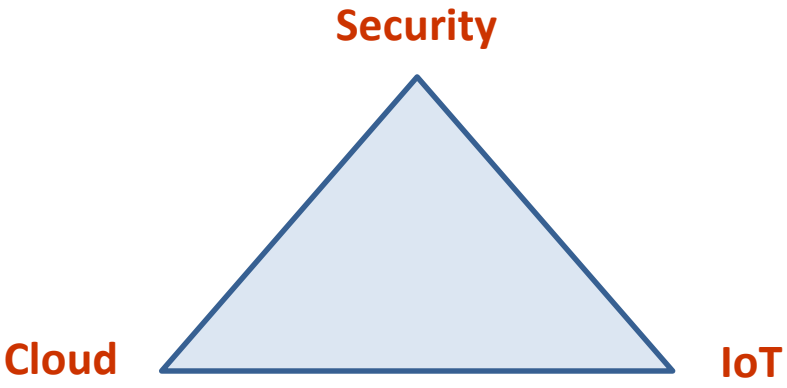
Introduction

❖ Internet of Things (IoT)

- ❖ Interconnection of people and things, and things and things
- ❖ Rapidly evolving concept with billions of connected devices/things

Introduction (Contd.)

- **Cloud-Enabled IoT**
  - Constrained IoT devices (limited resources)
  - Cloud Computing capabilities enable IoT
    - Seamless communication (devices-to-cloud, cloud-to-devices)
    - Unlimited resources → compute, storage, etc.
    - Meaningful insights → Analytics and Visualizations
    - Facilitate application development → APIs
    - Virtual things and management, Access Control policies, …



Access Control in Cloud-Enabled IoT

- Current industrial Cloud-Enabled IoT solutions/platforms
  - Amazon Web Services (AWS) IoT
  - Microsoft Azure IoT Suite
  - Google Cloud IoT
  - …
- Utilize some customized form of Role-Based Access Control (RBAC)
- RBAC insufficient to address dynamic IoT requirements
- Lack a formal access control model for controlling access and authorization in cloud-enabled IoT

Contributions

- Many access control models and architecture for IoT
  - Capability-Based Access Control (CAPBAC),
  - Role-Based Access Control (RBAC),
  - Attribute-Based Access Control (ABAC), …
- **Our Contributions:**
  - Develop a formal access control model for AWS IoT, known as AWS-IoTAC
  - Present a smart-home IoT use case depicting different access control points and authorizations in a cloud-enabled IoT platform
  - Propose some ABAC enhancements for the AWS-IoTAC model for more flexible and fine-grained access control policies

AWS Access Control (AWSAC) Model

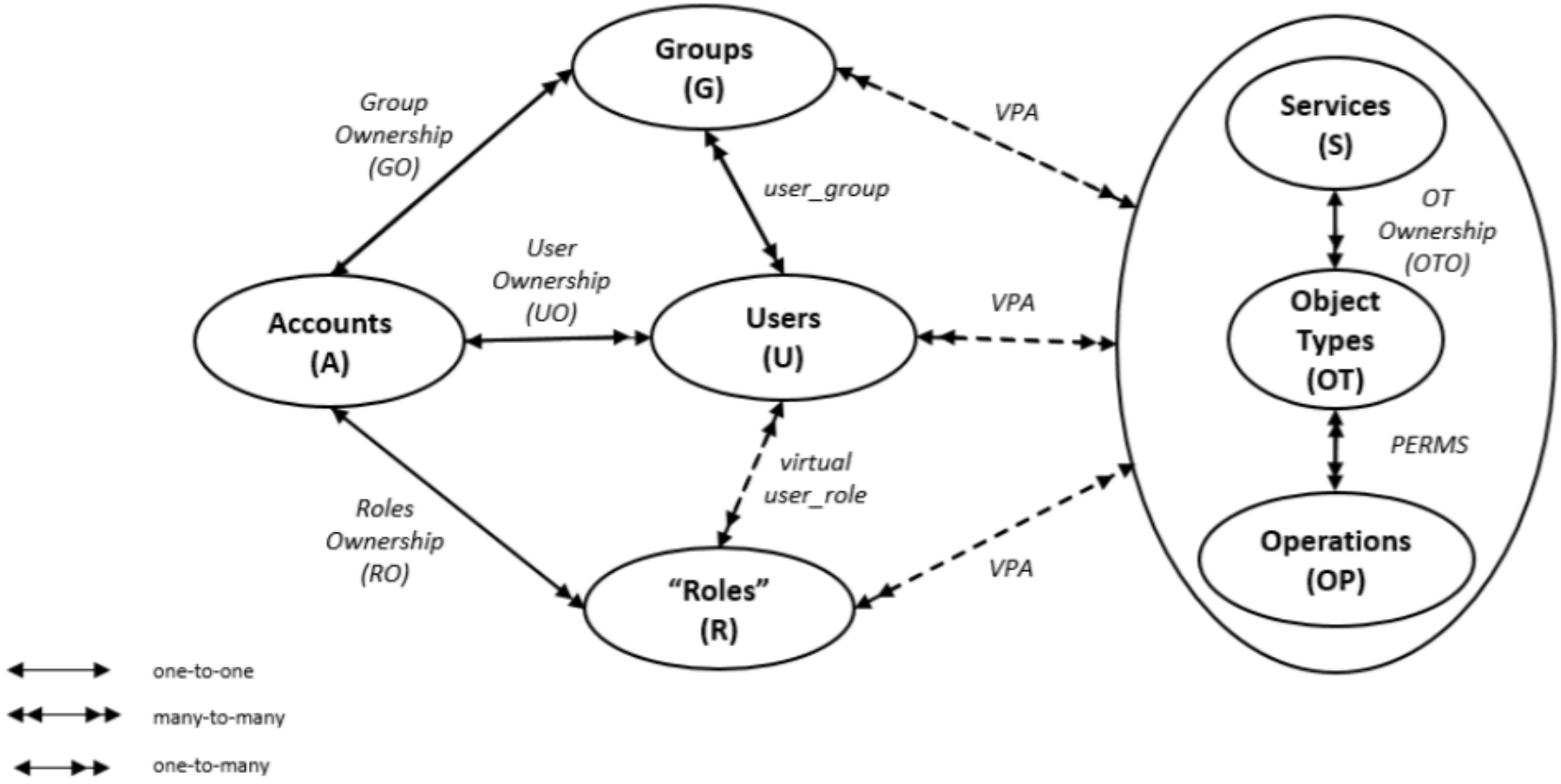


Fig 1: AWS Access Control within a Single Account *

* Zhang, Y., Patwa, F., Sandhu, R.: Community-based secure information and resource sharing in AWS public cloud. In: 1st IEEE Conference on Collaboration and Internet Computing (CIC). pp. 46–53. IEEE (2015)

Access Control Model for AWS IoT

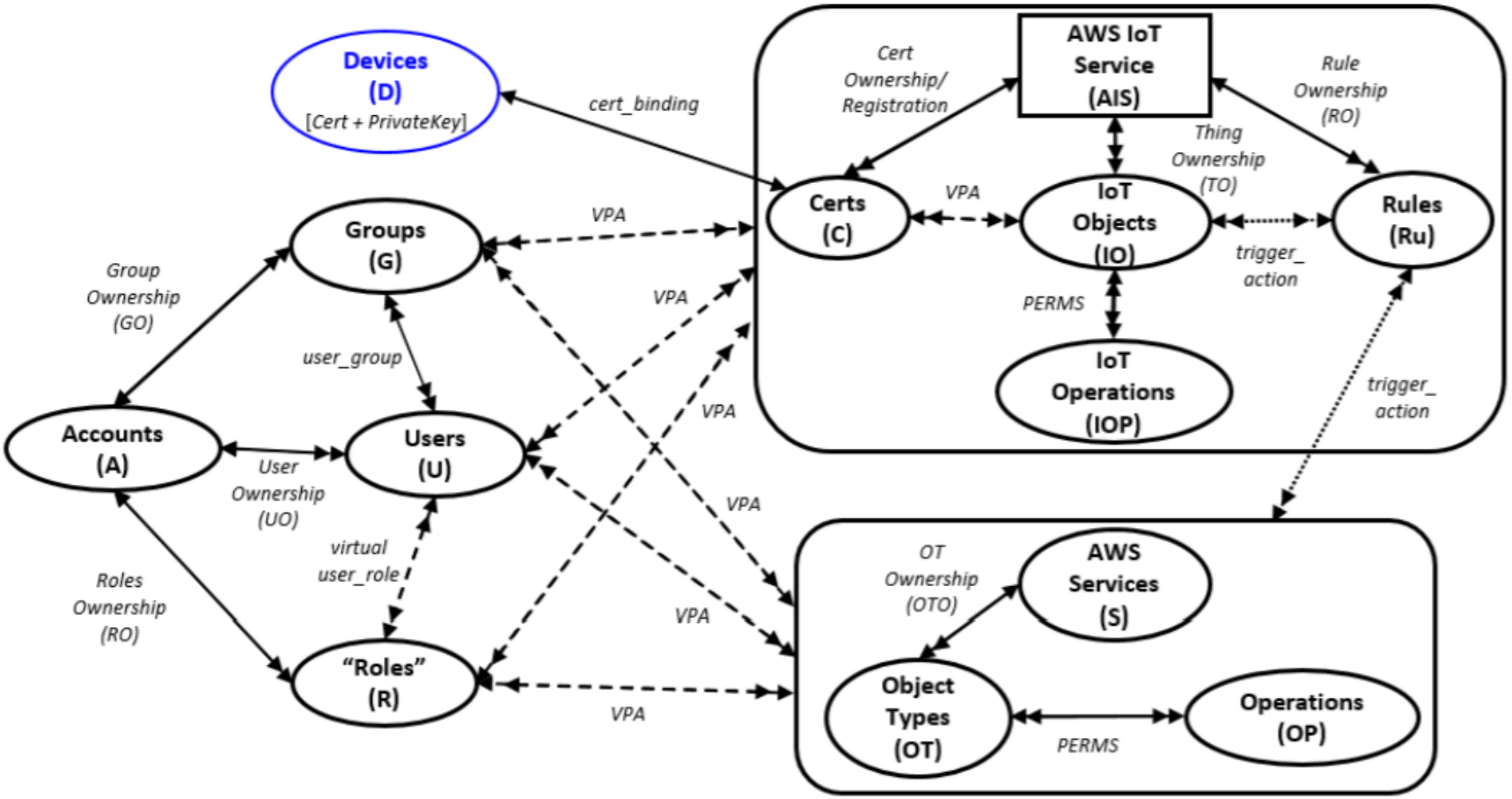


Fig 2: AWS IoT Access Control (AWS-IoTAC) Model within a Single Account

Access Control Model for AWS IoT

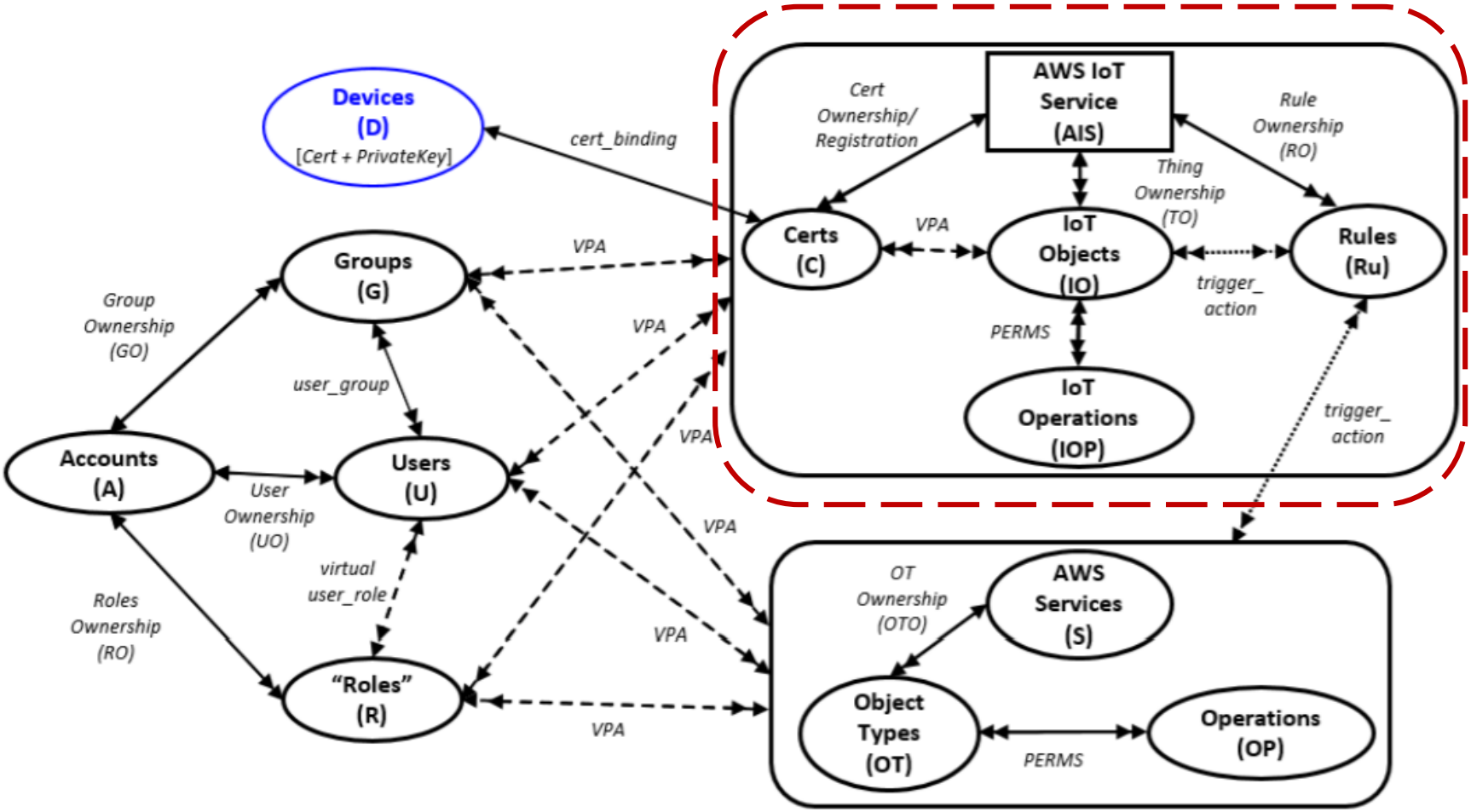


Fig 2: AWS IoT Access Control (AWS-IoTAC) Model within a Single Account

ACO Architecture for Cloud-Enabled IoT

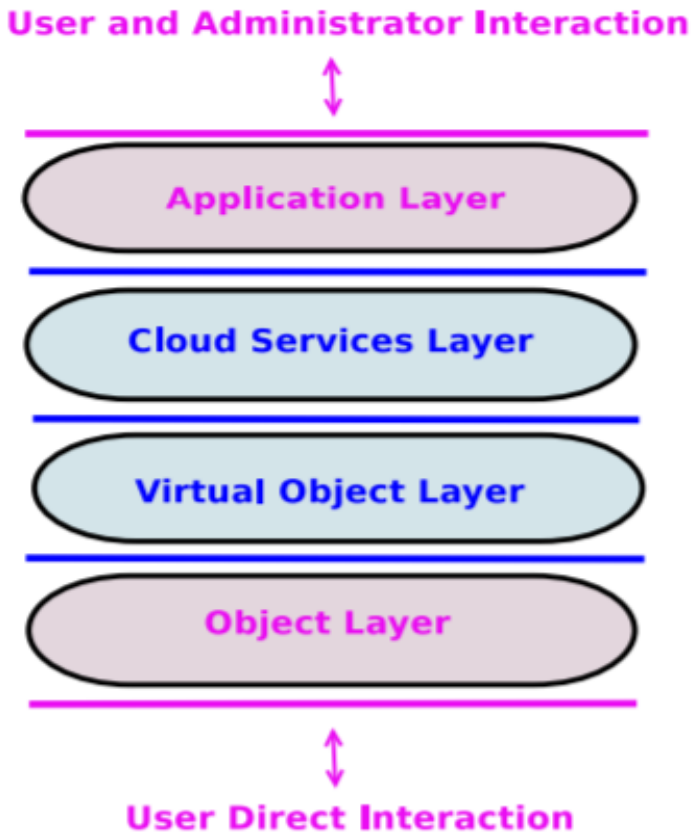


Fig 3: ACO Architecture for the Cloud-Enabled IoT *

* Alshehri, A., Sandhu, R.: Access control models for cloud-enabled internet of things: a proposed architecture and research agenda. In: 2nd IEEE International Conference on Collaboration and Internet Computing (CIC), pp. 530–538. IEEE (2016)

ACO Architecture & AWS-IoTAC

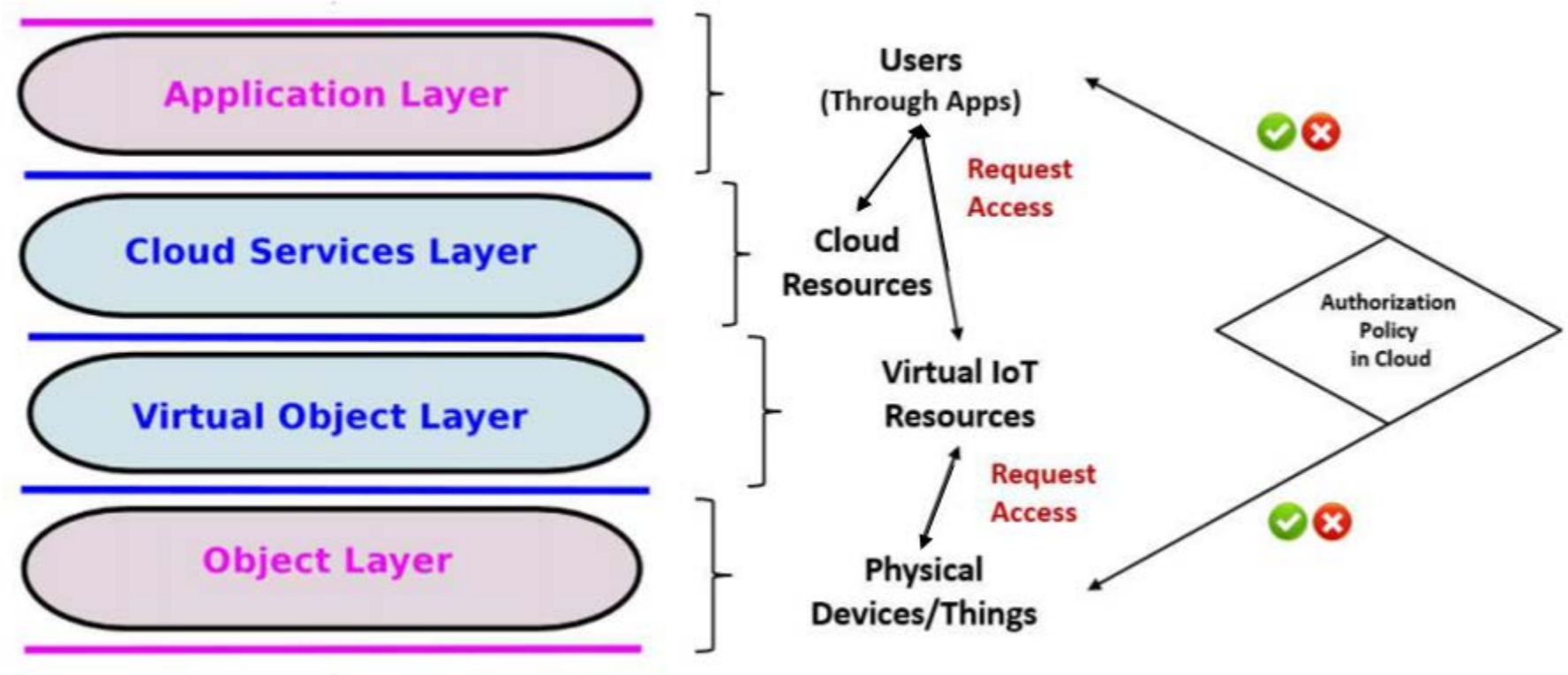


Fig 4: AWS-IoTAC Entities Mapping to ACO Architecture for Cloud-Enabled IoT

Smart Home Use Case in AWS IoT

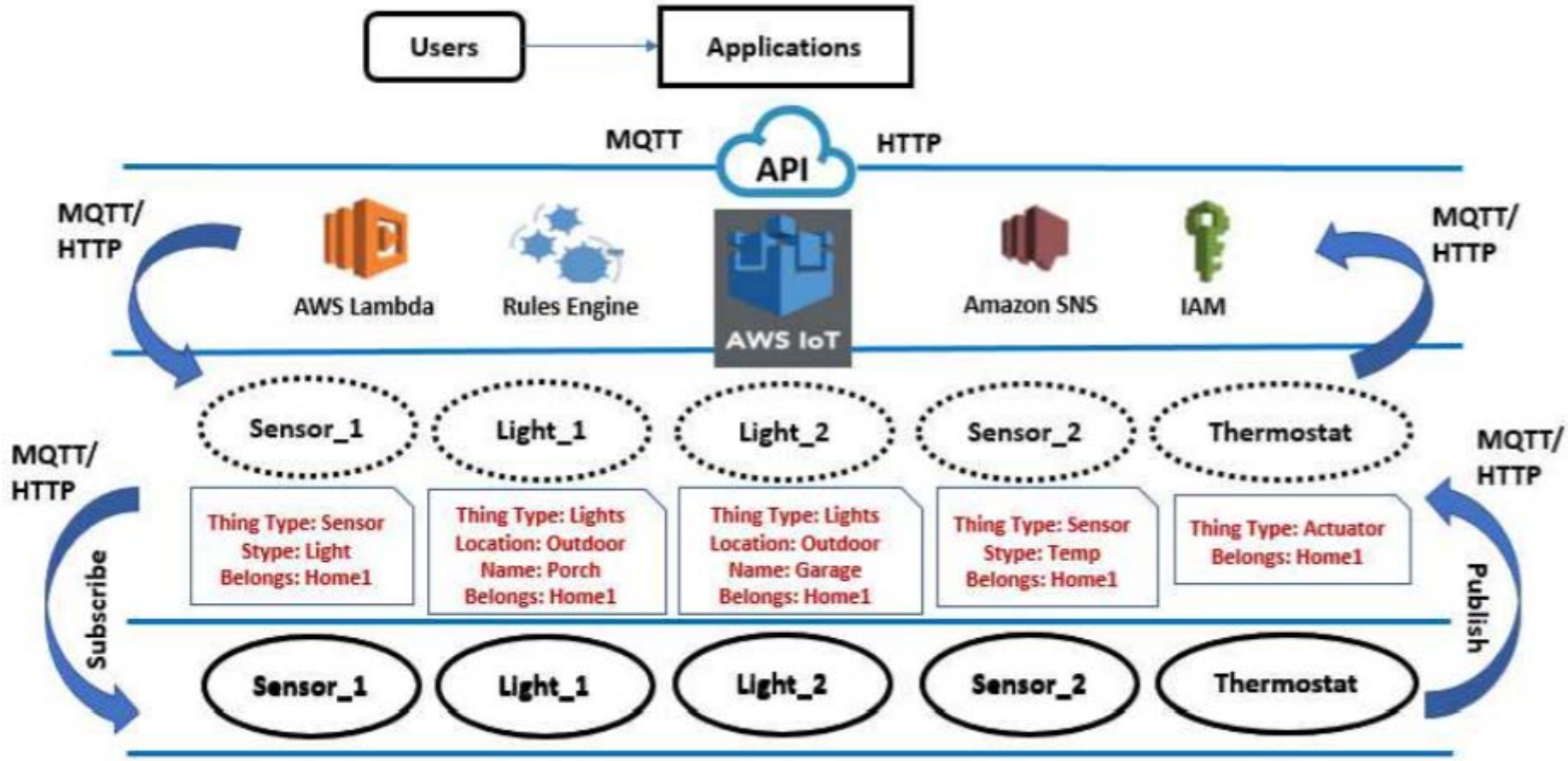
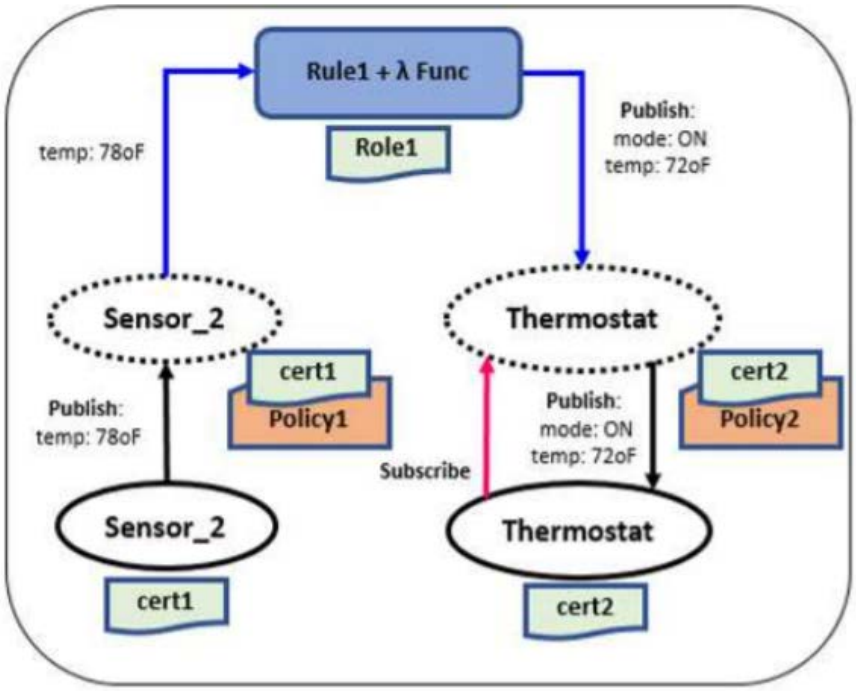


Fig 5: Smart-Home Use Case Utilizing AWS IoT and Cloud Services

Use Case – Scenario 1



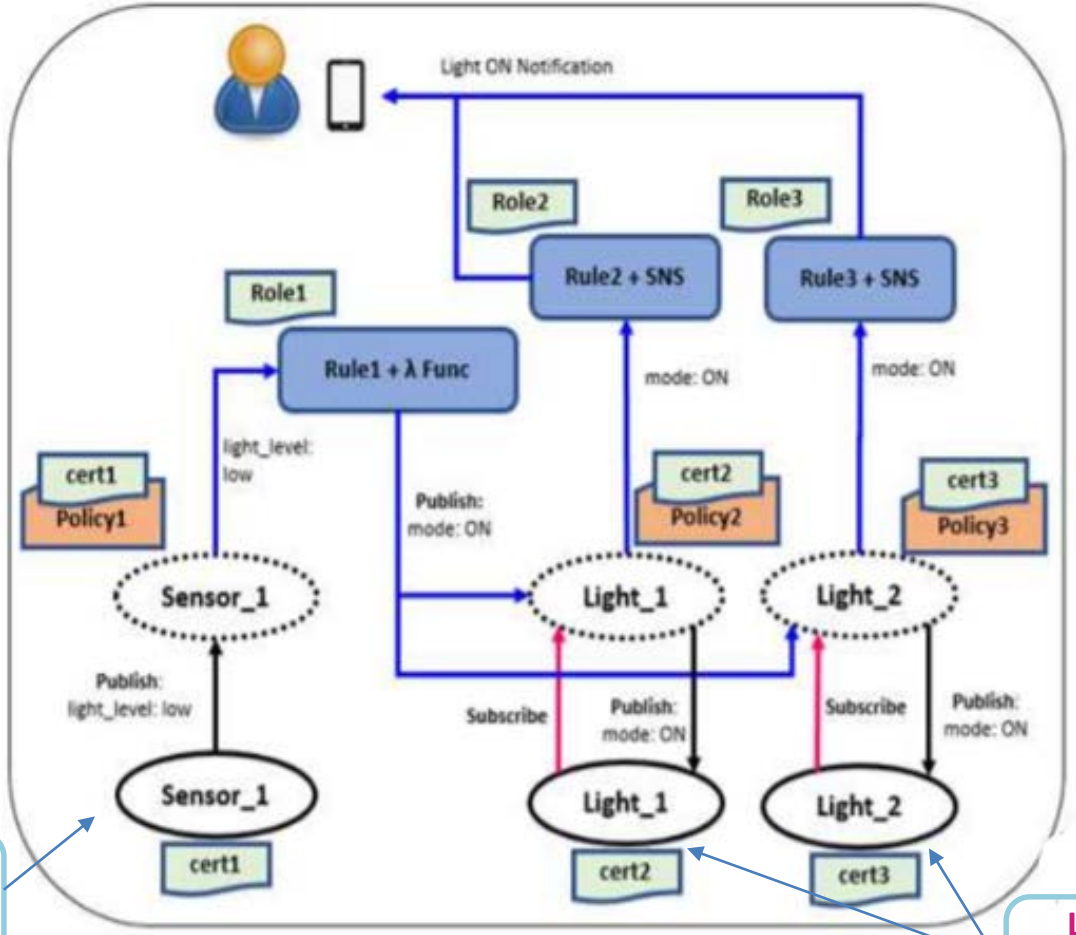
A temperature sensor and thermostat use case

```
{
"Version": "2012-10-17",
"Statement": [    {
      "Effect": "Allow",
      "Action": "iot:*",
      "Resource": "*"
     } ]
}
```

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

Fig 6: Smart-Home Use Case Scenario 1

Use Case – Scenario 2



a. Use Case – Scenario 2

Sensor Attribute:
Belongs = Home1

Light Attributes:
Location = Outdoor
Belongs = Home1

Use Case – Scenario 2

```
{
"Version": "2012-10-17",
"Statement": [  {
  "Effect": "Allow",
  "Action": "iot:Connect",
  "Resource": "arn:aws:iot:us-east-1:154003771683:client/Sensor_1"
 },
 {
  "Effect": "Allow",
  "Action": [ "iot:Publish", "iot:Subscribe", "iot:Receive"],
  "Resource": "*",
  "Condition": { "StringEquals": {
    "iot:Connection.Thing.Attributes[Belongs]": "Home1"
  } }
 }
]
}
```

b. A Fine-grained IoT Policy

Allows the sensor (client) to connect to AWS IoT only if it is connecting with a client ID as *"Sensor_1"*

Allows the sensor to Publish, Subscribe, and Receive messages to any iot resource in AWS IoT only if the sensor has attribute *"Belongs=Home1"*

Use Case – Scenario 2

- Utilizing target resource (things) attributes through AWS Lambda function

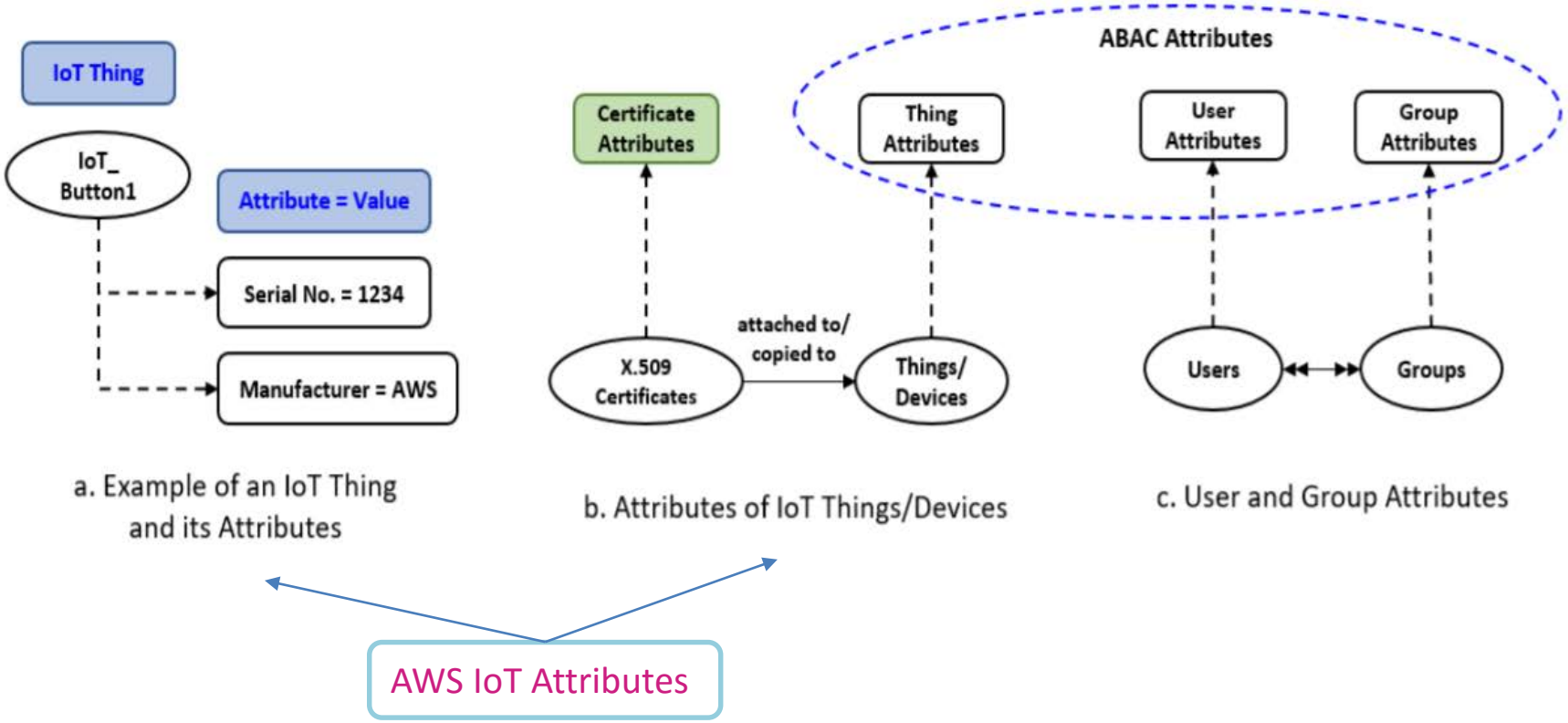
```
...
var params2 = {attributeName: 'Location',
               attributeValue: 'Outdoor'
};
iot.listThings(params2, function(err, data) {
  ...
    for (i in data.things) {
        x = data.things[i].thingName;

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

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

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

Fig. 7: Lambda Function

ABAC Enhancements for AWS-IoTAC



ABAC Enhancements for AWS-IoTAC (Contd.)

- ABAC Including Attributes of Target Resources
  - Attributes of things performing IoT operations
  - Attributes of things on which the operations are being performed
- ABAC Including User and Group Attributes
  - Attributes besides things attributes in access control policies
- Policy Management Utilizing the Policy Machine
  - Policy-Explosion
  - Customized policy management for enterprises

Conclusion and Future Work

- Presented a formal access control model for AWS IoT, a cloud-enabled IoT platform by the largest cloud services provider – Amazon Web Services (AWS)
- AWS-IoTAC, an initial step towards a general access control model for cloud-enabled IoT
- Demonstrated a practical use case along various access control configurations
- Proposed ABAC enhancements to the AWS-IoTAC model
- **Future Work:**
  - Include ABAC enhancements in the AWS-IoTAC model
  - Access control and authorization in other real-world cloud-enabled IoT platforms

Thank you!!!

Questions???