Access Control Model for Virtual Objects (Shadows)
Communication for AWS Internet of Things

Asma Alshehri, James Benson, Farhan Patwa, and Ravi Sandhu

Institute for Cyber Security (ICS)
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)
Department of Computer Science
University of Texas at San Antonio

The 8th ACM Conference on Data and Application Security and Privacy (CODASPY)
March 19 - 21, 2018. Tempe, AZ, USA.
1. Introduction and Background.
2. Access Control Model for VO Communication for AWS IoT.
3. A Use Case Implementation
4. Performance
5. Conclusion and Future Work
Internet of Things

World-Leading Research with Real-World Impact!
IoT Projects

IoT business ideas

- Territory monitoring
- Medical sphere
- Customer appliances
- Industrial sphere
- Fitness sphere
- Cars
- Smart cities
- Toys
Access Control Oriented (ACO) Architecture for Cloud-Enabled IoT

The Object layer:
- Physical objects
- Collect data
- Communication

The Virtual Object Layer:
- Presents status of objects
- Communication
- O-VO Association
• The Cloud Layer:
  • Big data
  • Functionality
  • Communication

• The Application Layer:
  • Interface
  • Users and Admin
  • Generate AC policies
Access Control Issues in ACO Architecture for IoT
Access Control Models for VO Communications in ACO Architecture

Access control models for VO communication in two layers:

A. Operational models
   A. ACL-Cap operational model
   B. ABAC operational model

B. Administrative models
   A. ACL administrative model
   B. RBAC administrative model
   C. ABAC administrative model
A Use Case within ACO Architecture

Cloud Service layer

Virtual Object layer

Object layer

VS1  T1  VS2  T2  Tn-1  VSn  Tn  VC1

DynamoDB

S1  S2  Sn  C1

© Asma Alshehri

World-Leading Research with Real-World Impact!
Access Control Model for VO Communication for AWS IoT
The AWS-IoT-ACMVO Model for AWS IoT

Cloud Service Layer

- AWS IoT Policy
- Virtual Objects
- MQTT Topics
- Rules Engine
- Devices

Virtual Object Layer

- Certificates

Object Layer

- AWS Services
  - IAM Role
  - Policy
  - Rules
  - Actions
• Certificates: An identity for devices authentication
• AWS IoT policy: A policy for authorization purpose
• Virtual objects: A JSON document that stores information about the current and future status of a device.
• MQTT topics: AWS IoT service generates reserved MQTT topics for each created virtual object
The AWS-IoT-ACMVO Model for AWS IoT

• Rules: Recognize and analyze messages that are sent to MQTT topics and trigger actions.

• Actions: There are fixed AWS actions that can be selected, such as inserting a message into a DynamoDB table, invoking a Lambda function, and republishing messages to AWS IoT topics.

• AWS identity and access management (IAM) role: Actions authorization
The Publish/Subscribe Topic-Based Scheme

- The communication channel between two VOs is a shared topic
• The communication channel between two VO Topics is the Rules Engine
The Sensing Speeding Cars Use Case

Cloud Service layer

Virtual Object layer

Object layer

DynamoDB

© Asma Alshehri

World-Leading Research with Real-World Impact!
Sensing the Speed of One Car with two Sensors

World-Leading Research with Real-World Impact!
```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iot:GetThingShadow",
        },
        {
            "Effect": "Allow",
            "Action": "iot:Publish",
        }
    ]
}
```
Sensing the Speed of Multiple Cars with Multiple sensors

© Asma Alshehri

World-Leading Research with Real-World Impact!
Conclusion and Future Work
Conclusion

1. Develop access control models for VO communications for AWS IoT
2. Reconcile the academic access control models within the AWS IoT
3. Implement the sensing speeding cars use case
Future Work

Access Control

Communication

Data

Sub-Data

Individual Collected Data

Accumulated Data

Users

Administrators

Applications

Clouds

Virtual Objects

Objects
Questions