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

World-Leading Research with Real-World Impact!
Introduction

Cloud-Enabled IoT (CE-IoT)

Security and Privacy

Internet of Things (IoT) [*]

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 ???
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)

Cloud & CE-IoT

World-Leading Research with Real-World Impact!
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

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 Communication
- 2. WIoT Use Case

Enforcement Utilizing Policy Machine and Authorization Engine

Enforcement in AWS IoT
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) ≡ title(u) = Manager ∧ type(o) = Sensitive
Auth_{write} (u, o) ≡ name(u) = created_by(o)
Attribute-Based Access Control

- **Name, Title, ...**
- **Users, Processes, ...**
- **Files, Databases, ...**
- **Type, Created_by, ...**
- **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”**

© Smriti Bhatt
Summary of Contributions

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

© Smriti Bhatt

World-Leading Research with Real-World Impact!
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)

User Attributes (UA)

User Assignment (UA)

Projects (P)

User Assignment (UA)

Roles (R)

Role Assignment (RPA)

Services (S)

Object Types (OT)

Operations (OP)

Tokens (T)

Effective-Token Permission Assignment (ETPA)

Union of attribute-value permissions

User-Attribute Permission Assignment (UAPA)

(Union of role permissions \( \cap \) Union of attribute-value permissions) based on the token of a user

Many-to-Many

One-to-Many

One-to-One
Facilitate attribute assignment through Group and Attribute Hierarchy

Attribute Hierarchy

→ Formalized as Single-Value Enumerated Authorization Policy
  e.g., Policy_{read} = (Manager, Private)

Fig. 2: Restricted Hierarchical Group and Attribute-Based Access Control (rHGABAC) Model
Extended from HGABAC [Servos and Osborn, 2015]
a) An Example of User Group Hierarchy
(Adapted from [Gupta and Sandhu, 2016])

b) User Attribute-value Hierarchy

skills = \{C, C++, Java\}
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

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

**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
Enforcement Architecture

![Diagram of Authorization Architecture Utilizing PM and AE]

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

**e.g., OpenStack**

**Fig. 3: Authorization Architecture Utilizing PM and AE**
Summary of Contributions

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

World-Leading Research with Real-World Impact!

© Smriti Bhatt
• **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, ...

Security and Privacy
Edge Computing (Cloudlets)
• Amazon Web Services (AWS) IoT – *a CE-IoT platform*

• Currently utilize customized policy-based access control

• Lack a formal access control model for controlling access and authorization in cloud-enabled IoT
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

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

AWS Lambda Function

```javascript
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){
      ...
    }
  }
});
```
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

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

- Enforcement Utilizing Policy Machine and Authorization Engine

- 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 in AWS IoT

© Smriti Bhatt

World-Leading Research with Real-World Impact!

25
Enhanced ACO Architecture for CE-IOT

User and Administrator Interaction

- Application Layer
- Cloud Services Layer
- Virtual Object Layer
- Object Layer

User Direct Interaction

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

b) Enhanced ACO (E-ACO) Architecture

User and Administrator Interaction

- Application Layer
- Cloud Services Layer
- Virtual Object Layer
- Object Abstraction Layer
- Object Layer

User Direct Interaction

© Smriti Bhatt

World-Leading Research with Real-World Impact!
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
Fig. 6: Remote Health and Fitness Monitoring (RHFM) Example
Summary of Contributions

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

World-Leading Research with Real-World Impact!

© Smriti Bhatt
Communication Control in CE-IoT

Certificate and Crypto Based Communication Control

Attribute-Based Communication Control

Edge Network of Things

Gateway A

Gateway B

Gateway C

Cloud_1

Cloud_2

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

© Smriti Bhatt

World-Leading Research with Real-World Impact!
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
ABCC for Edge and Cloud Communication

Fig. 8: ABCC for Edge and Cloud Communication Model

Secure Communication through certificates and crypto keys
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 Diagram]

- **Send Allow**
  \[ \text{send (m)} \rightarrow m \]

- **Send Filtered**
  \[ \text{send (m)} \rightarrow m' \]

- **Send Deny**
  \[ \text{send (m)} \rightarrow \emptyset \]
Use Case

ABCC Policies

- **Send Allow** \(\rightarrow gowner(g) = owner(vo) \land \text{heartrate}(m) \geq 150 \land \text{temp}(m) > 104\)
- **Send Filtered** \(\rightarrow gowner(g) = owner(vo) \land \text{heartrate}(m) \leq 75 \) (filter location)
- **Send Deny** \(\rightarrow \text{If policy evaluation failed (e.g., } gowner(g) \neq owner(vo)\))
Enforcement in AWS IoT

- AWS IoT and AWS Greengrass (Edge Computing Service)

**Diagrams:**
- AWS SDKs
- AWS Greengrass Core
- AWS IoT
- AWS Cloud
- Local Shadows
- Arch function
- PAP, PDP, PEP for CCP
- Allow/Deny/Filter
- ABCC-EC Enabled Communication and Privacy Control Point
- AWS Access Control Point

**Abbreviations:**
- PAP – Policy Administration Point
- PDP – Policy Decision Point
- PEP – Policy Enforcement Point
- PIP – Policy Information Point
Sequence Diagram

Heartrate-Temp Sensor

- Send device data to local shadow as an update message

Greengrass Core (Gateway)

- Trigger Lambda function when update message received

AWS Lambda on Greengrass (Gateway)

- Request attributes for virtual objects and gateway
- Get attributes
- Evaluate ABCC-EC policies, if satisfy then allow send message (all/filtered), else deny
  - If allow, then send (all/filtered) message to device shadow (VO)
  - If deny, do not send message to device shadow

AWS IoT Cloud
Evaluation

Device Shadow Update Time

Attribute Caching

© Smriti Bhatt

World-Leading Research with Real-World Impact!
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:


☑ In preparation:

• Smriti Bhatt, Farhan Patwa and Ravi Sandhu, Attribute-Based Communication Control in Cloud-Enabled Internet of Things. Venue TBD.
Thank you!
Questions?