ABAC-CC: Attribute-Based Access Control and Communication Control for Internet of Things

Smriti Bhatt[1], Ravi Sandhu[2]

[1]Department of Computing and Cyber Security, Texas A&M University-San Antonio
[2]Institute for Cyber Security (ICS), CREST-Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)
Department of Computer Science, University of Texas at San Antonio

The 10th ACM Symposium on Access Control Models and Technologies (SACMAT)
June 10-12, 2020

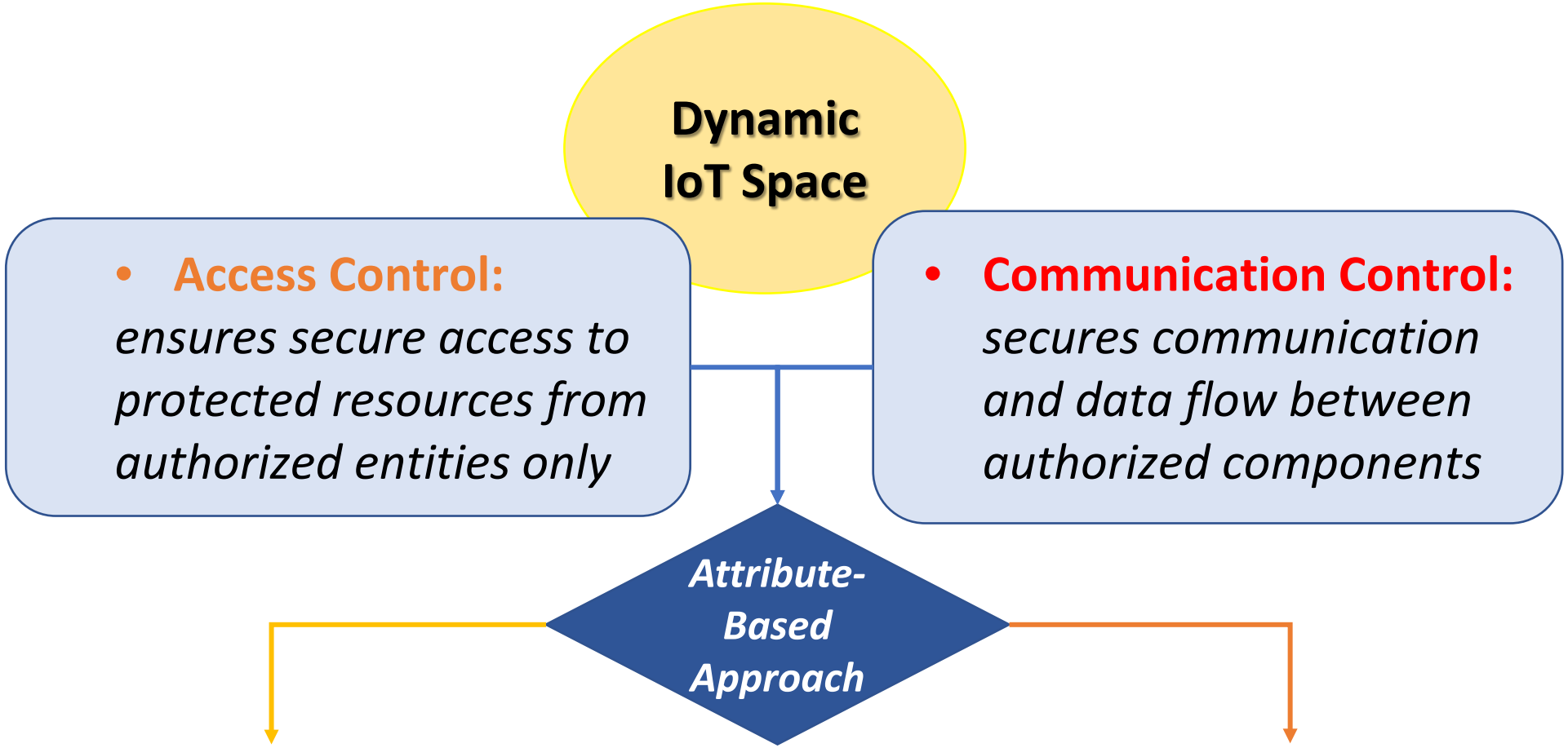
Outline

- Introduction
- Background
- Cloud-Enabled IoT (CE-IoT) Architectures
- Access Control and Communication Control Requirements in CE-IoT
- Use Case Scenarios
- ABAC vs. ABCC
  - Attribute-Based Communication Control (ABCC) – *Conceptual model*
  - Attribute-Based Access Control (ABAC)
- Attribute-Based Access Control and Communication Control (ABAC-CC) Framework
- Future Research Directions
- Conclusion and Future Work

Introduction

- **Internet of Things (IoT)** - *billions of connected smart things enabled by technologies like Cloud Computing, Artificial Intelligence (AI) and Machine Learning (ML)*
- IoT devices have some unique characteristics unlike other Internet-connected user devices –
  - *Distributed and deployed in remote locations*
  - *Diverse in nature (e.g., size, capability, functionality)*
  - *Autonomous operation enabled by AI and Machine learning technologies*
  - *Dynamic behavior based on the context*
- Dynamic *access control* and *communication control* framework to adequately address security and privacy issues in the IoT space

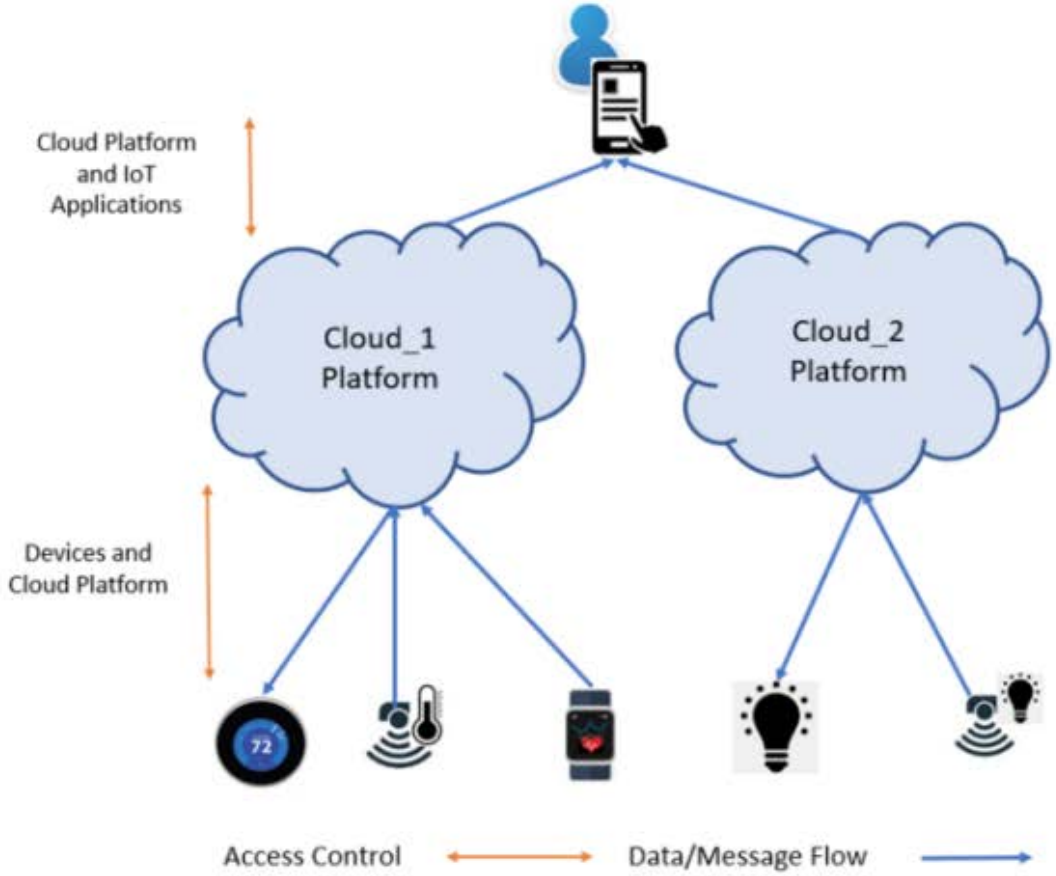
Access Control and Communication Control



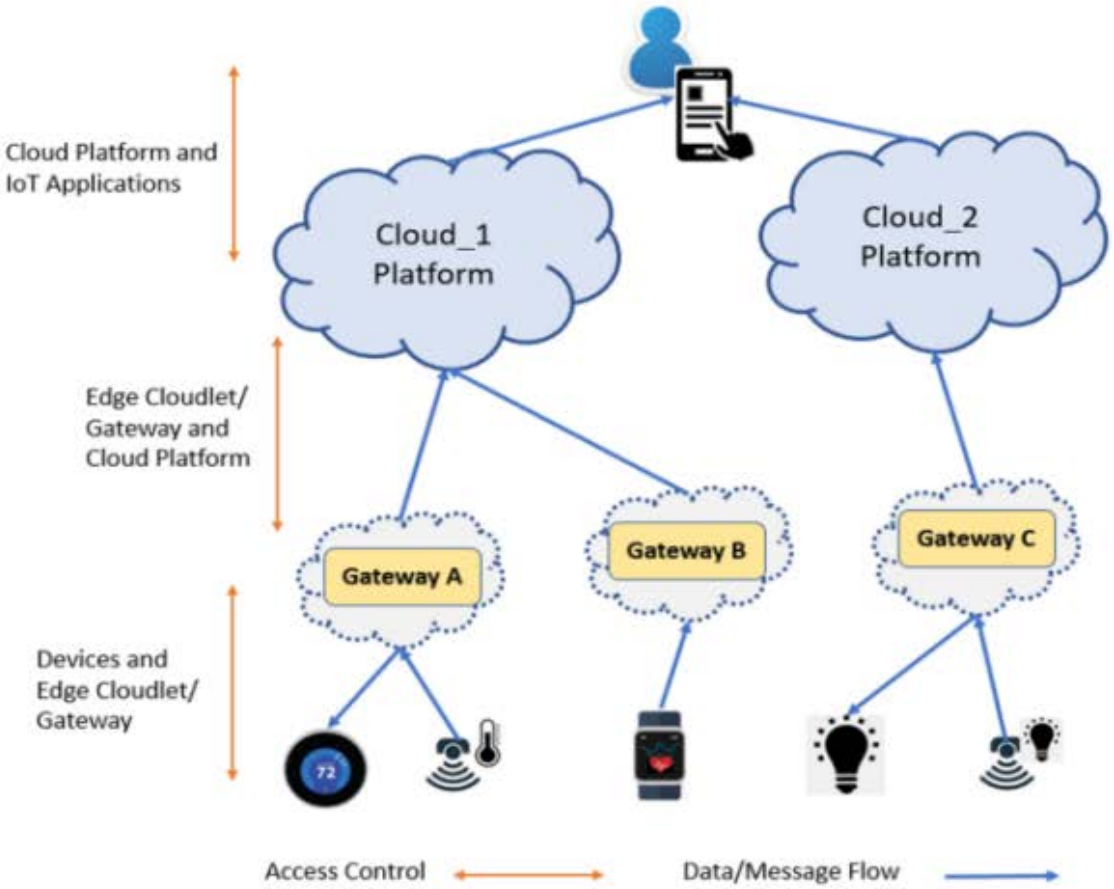
Background

- **Cloud-Enabled Internet of Things (CE-IoT)** –
  - *Cloud computing* has become a key enabling technology with virtually unlimited capabilities (e.g., storage, computation, analytics) for IoT devices
- Major cloud services provides such as Amazon Web Services (AWS) Microsoft Azure, and Google Cloud, including others, have introduced new IoT services
- Emerging security and privacy threats in IoT with new challenges including traditional cloud threats and vulnerabilities

CE-IoT Architectures

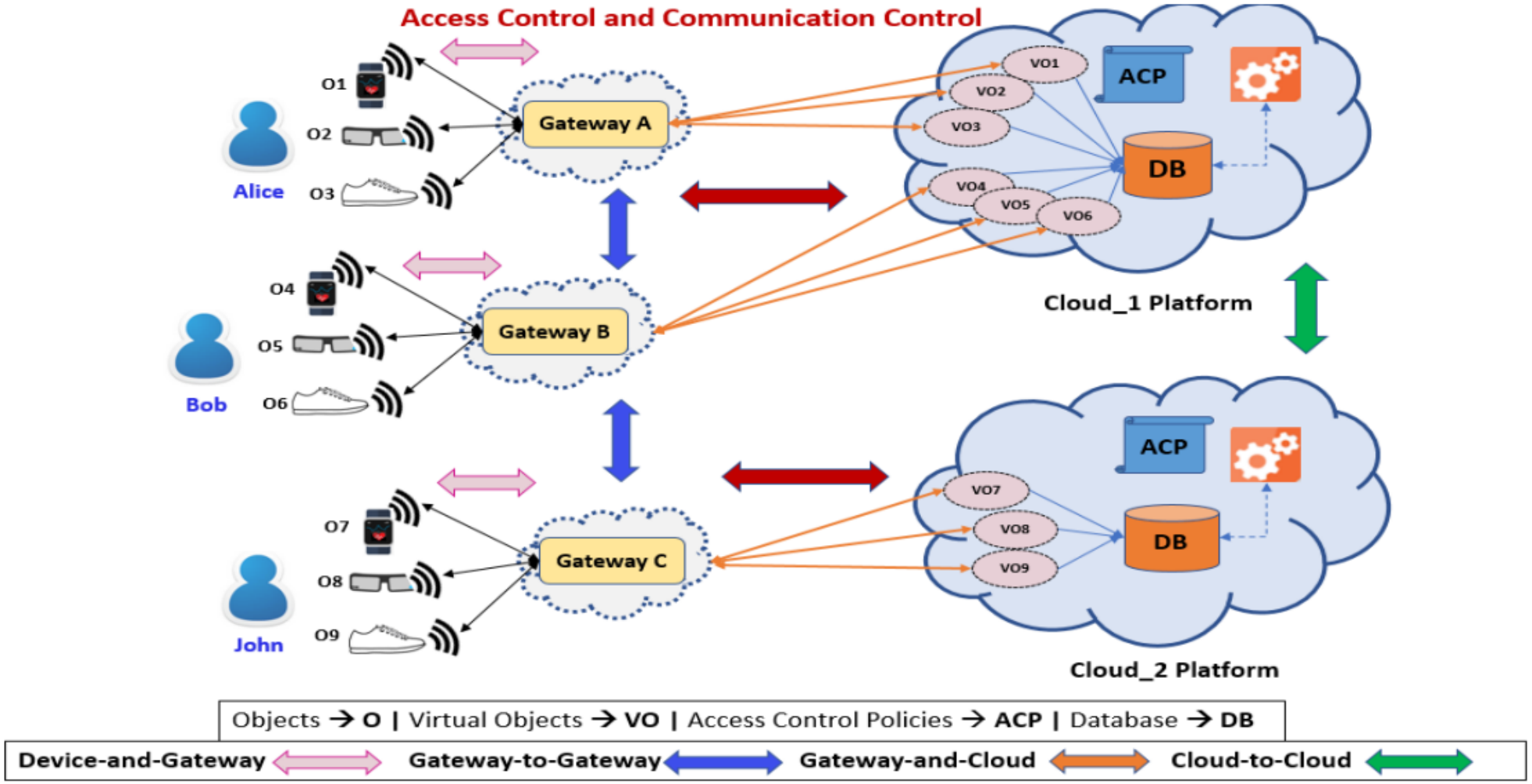


(a) Cloud-Enabled IoT Platform with no edge Cloudlet/Gateway: All the data from devices go to the Cloud Platform



(b) Cloud-Enabled IoT Platform with edge Cloudlet/Gateway: All the data from devices go to the Cloud Platform

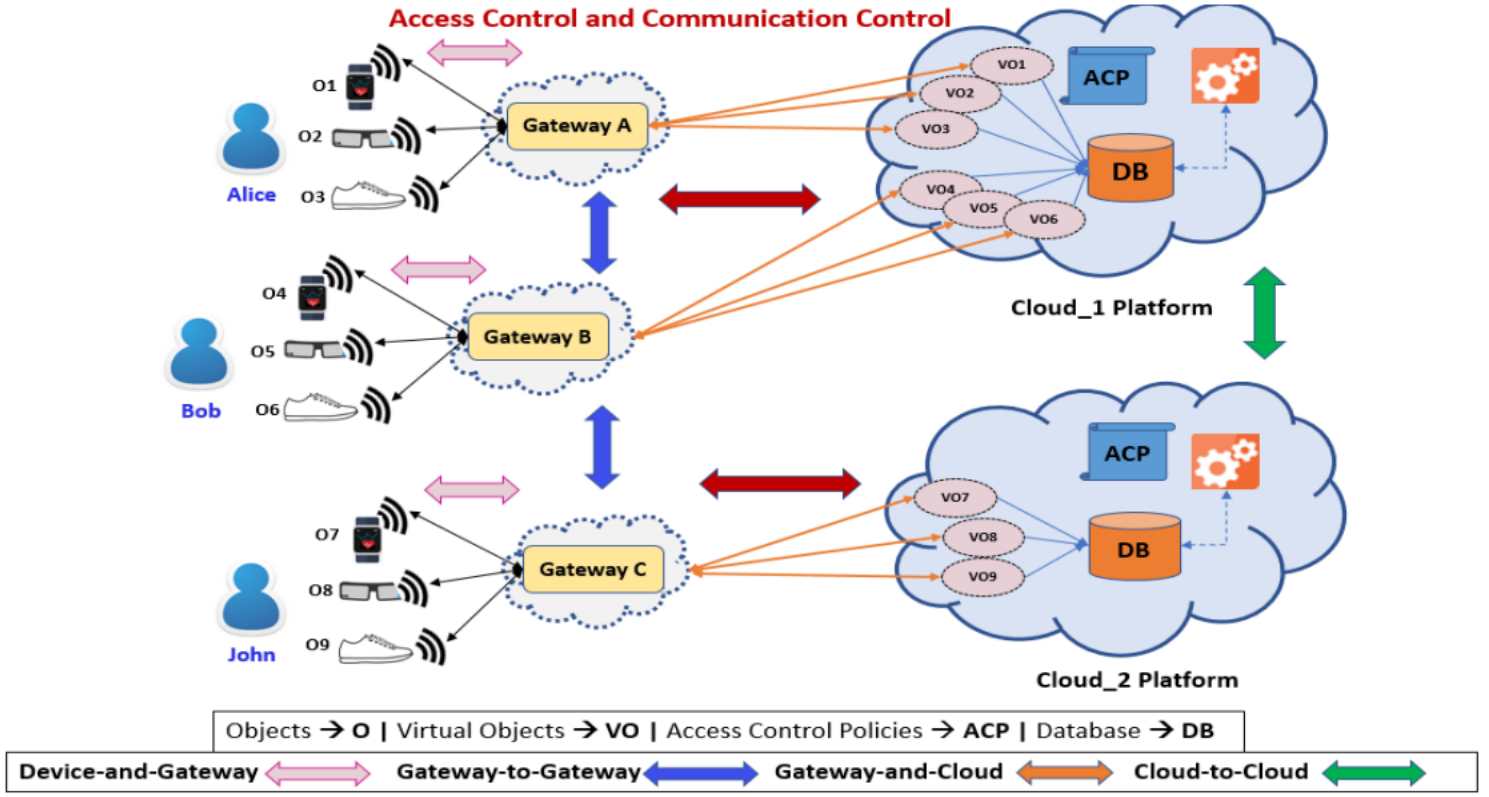
Access Control and Communication Control Requirements



Use Case Scenarios

- **Scenario 1 (Devices/Gateway to Cloud) --** Users want restrict privacy sensitive data to be shared with the Cloud at all times and rather confine the data at the edge network and only send important updates to cloud based on some predefined conditions.

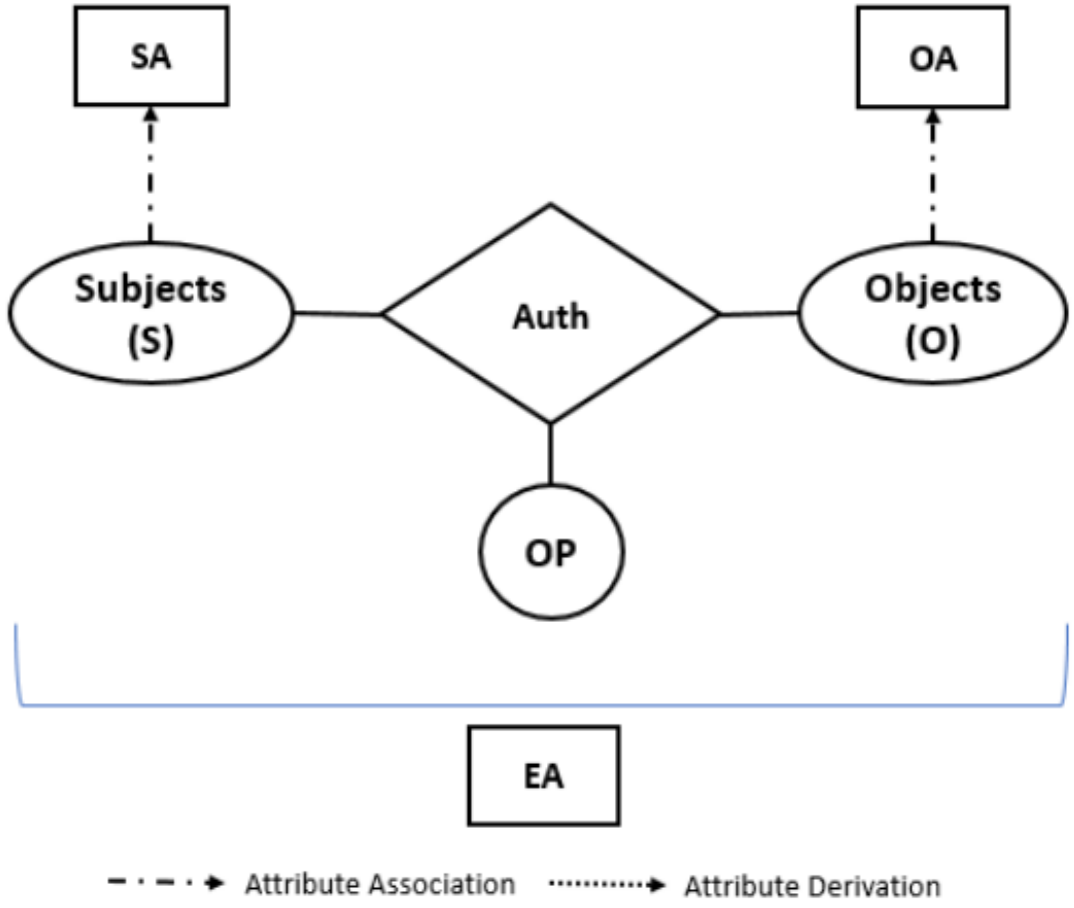
- **Scenario 2 (Cloud to Gateway/Devices) --** Users want to restrict messages coming from Cloud to users through IoT applications.



ABAC

Attribute-Based Access Control (ABAC)

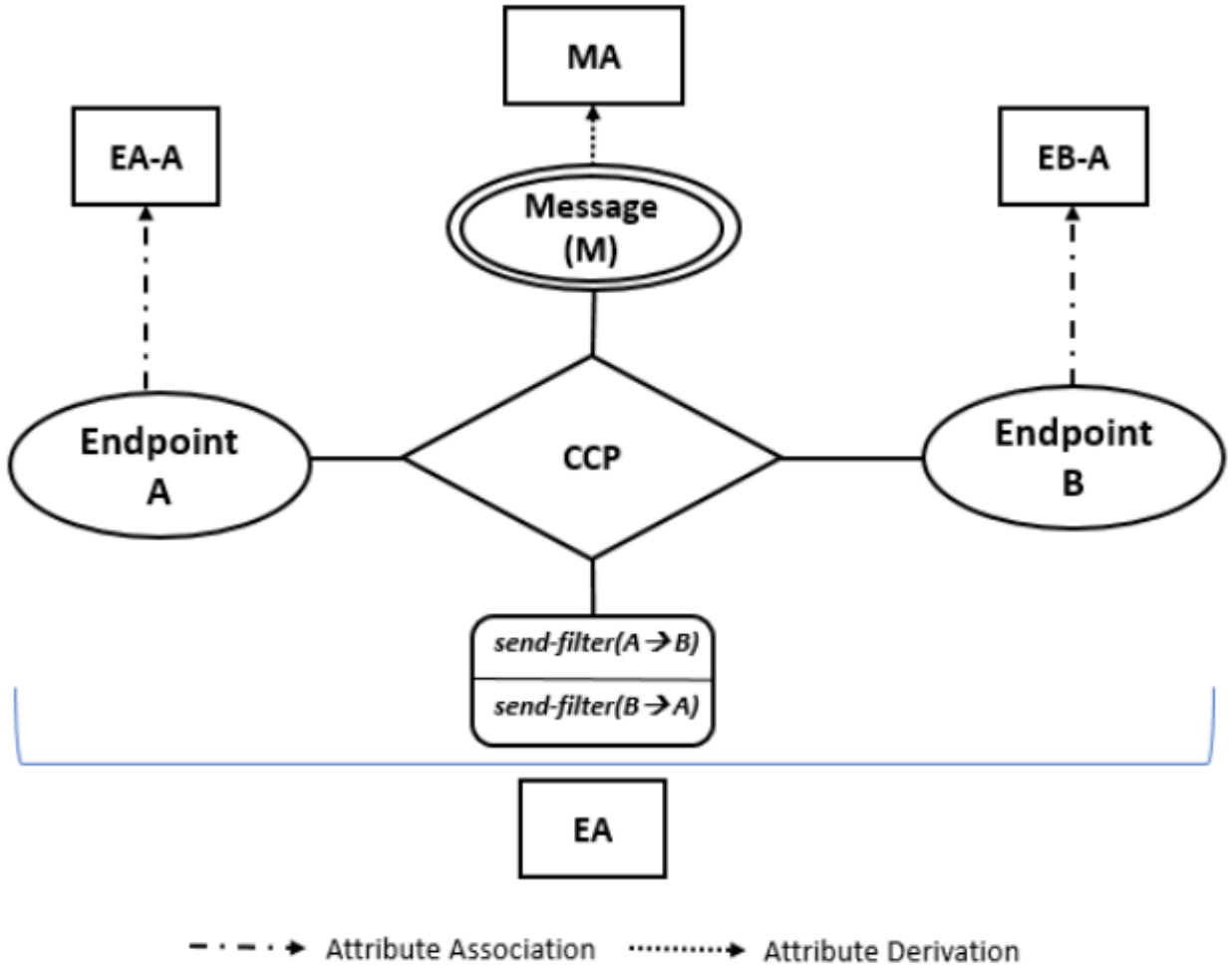
- **Subjects:** who request access (e.g., users, processes, devices, etc.)
- **Objects:** protected resources and entities (e.g., devices, files or folders, data)
- **Subject Attributes (SA):** title, age, etc.
- **Object Attributes (OA):** sensitivity, type, etc.
- **Environmental Attributes (EA):** location, time
- **Operations (or actions):** read(r), write(w)
- **Authorization Function:** *Auth_func = (s, o, r)*



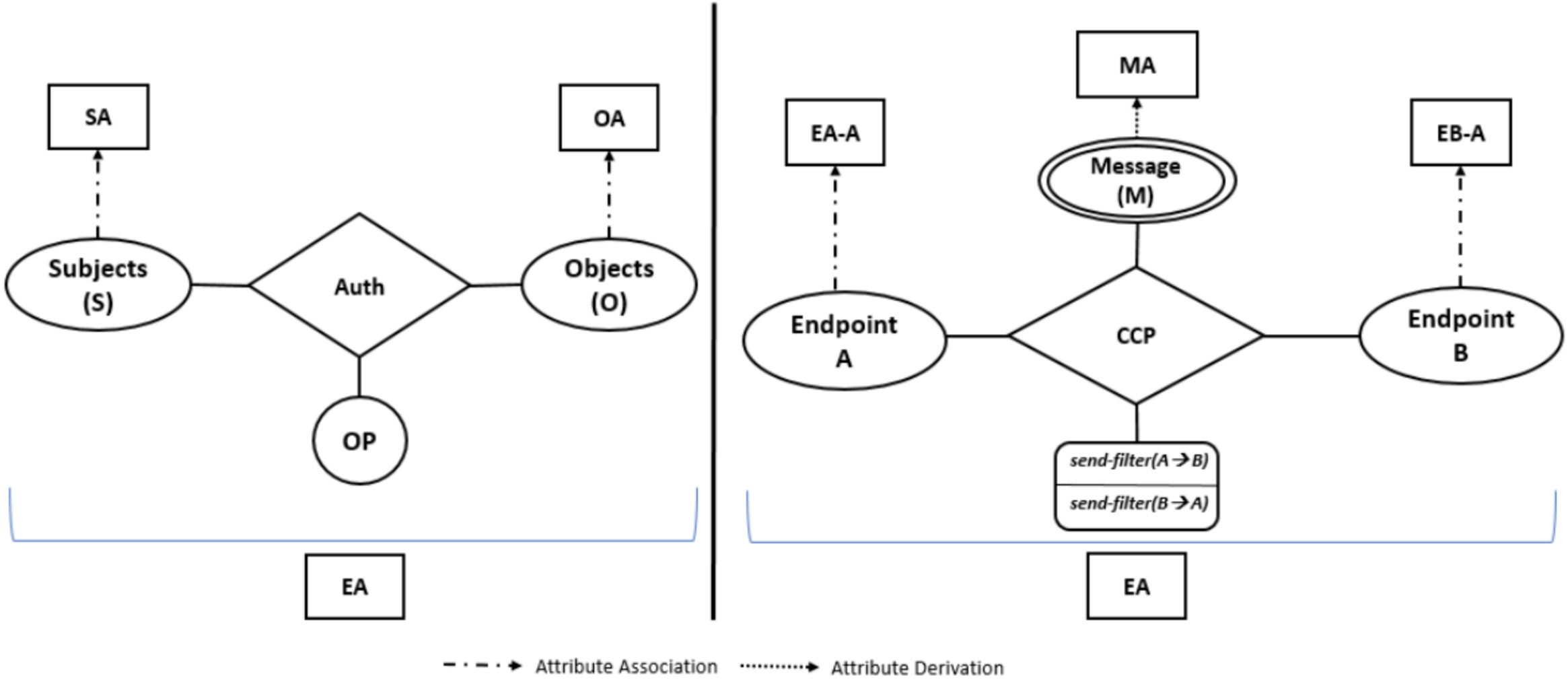
Attribute-Based Communication Control (ABCC)

- **EndpointA and EndpointB**
- **Endpoint Attributes (EA-A and EB-A)**
- **Message (M):** unit of communication
- **Message Attribute (MA)**
- **Environmental Attributes (EA):** location, time
- **Operations:** *send-filter*
  - *send-filter(A → B)*
  - *send-filter(B → A)*
- **Communication Control Policy (CCP) function:**

  Decisions → message can be sent unfiltered (original message), filtered (removing/sanitizing sensitive information), or not sent from a sender to a receiver



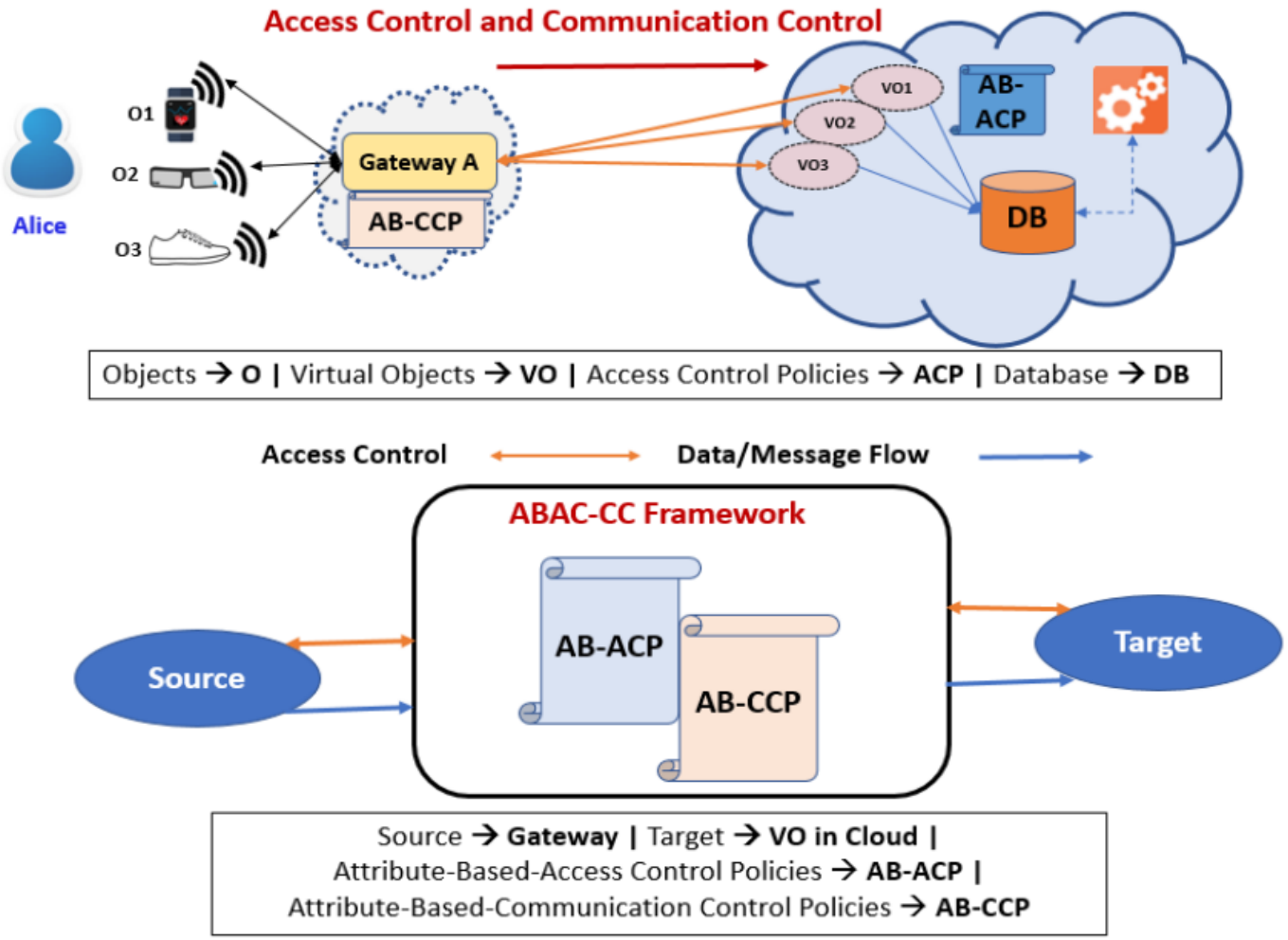
ABAC vs. ABCC



ABAC-CC in a Smart Health Monitoring Use Case Scenario

Access and Communication from Gateway to Cloud (VO)

- Gateway (EndpointA)
- VOs (EndpointB)
- Gateway and Device attribute: owner
- Message (m)
- Message Attribute: *location, temp, heartrate*
- *send-filter(A->B) => m, or m', or null*



Future Research Directions

- Artificial Intelligence and Machine Learning
- Distributed Computing
- Collaborative IoT Models
- Insider Threats and Rogue Devices
- Dynamic Edge and Fog Computing

Conclusion and Future Work

- Introduced the **Attribute-based Communication Control (ABCC)** model and compared its structure with the basic ABAC
- Proposed an ***Attribute-Based*** approach for developing the ABAC-CC framework to secure access and communication in CE-IoT architecture
- Discussed a smart health monitoring use case and presented future research directions
- **Goal:**
  - To reevaluate and rethink current access control mechanisms and design new models on top of the attribute-based approach to secure IoT access, communication, and data at rest and in motion
  - Stimulate research on ABCC models for real-world IoT application domains, such as Smart Home, Smart Health
- **Future Work:** Develop formal ABCC models for securing communication between various components in the context of CE-IoT.

Thank You!

Questions???