Towards Finer-Grained Access Control for Globally Accessible IoT

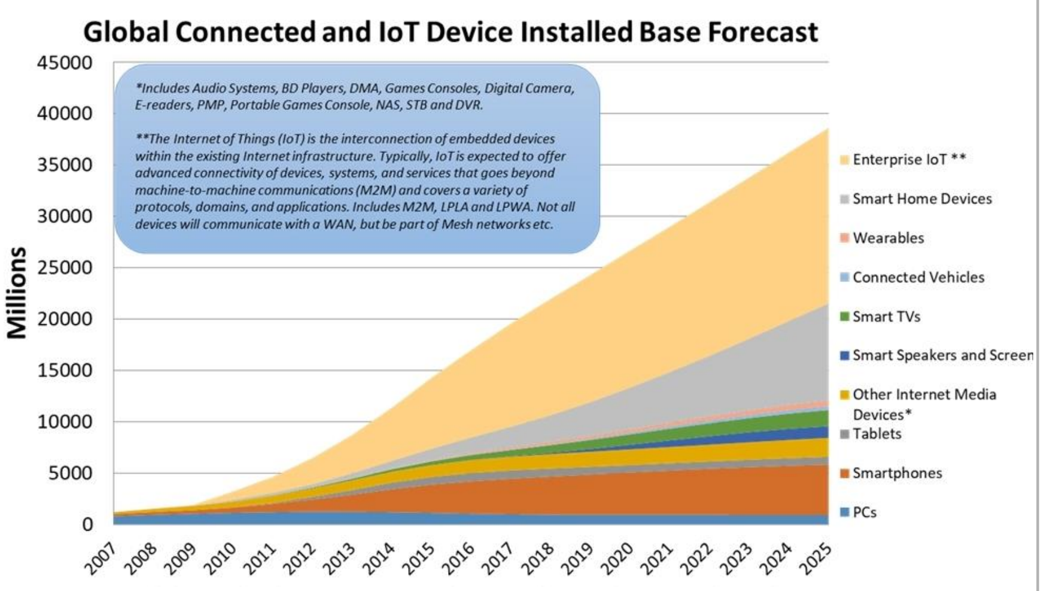
Luoyao Hao, Andrea Huang, Vibhas Naik, Olaedo Okoroafor, and Henning Schulzrinne *
Department of Computer Science, Columbia University
Email: {l.hao, amh2341, vn2302, ooo2139}@columbia.edu, hgs@cs.columbia.edu

Introduction

IoT devices collect and transfer potentially sensitive user data, and a lack of effective access control and authentication protocols leaves them vulnerable as targets and entry points to large-scale attacks that can compromise entire systems.

Fundamental Challenges

- Limited storage, power, and computational capacity of devices
  - Unable to enforce traditional web-based approach
  - Usually rely on a "controller"
- Various scenarios and privileges
  - Need a flexible and powerful mechanism
- Access data in an IoT ecosystem
  - Cross-domain access
- Rapid prototyping & testing
  - Without physical IoT devices
  - Without access to IoT systems


Global Connected and IoT Device Installed Base Forecast
*Includes Audio Systems, BD Players, DMA, Games Consoles, Digital Camera, E-readers, PMP, Portable Games Console, NAS, STB and DVR.
**The Internet of Things (IoT) is the interconnection of embedded devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. Includes M2M, LPLA and LPWA. Not all devices will communicate with a WAN, but be part of Mesh networks etc.
Millions
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Enterprise IoT **
Smart Home Devices
Wearables
Connected Vehicles
Smart TVs
Smart Speakers and Screen
Other Internet Media Devices*
Tablets
Smartphones
PCs

Source: businesswire.com

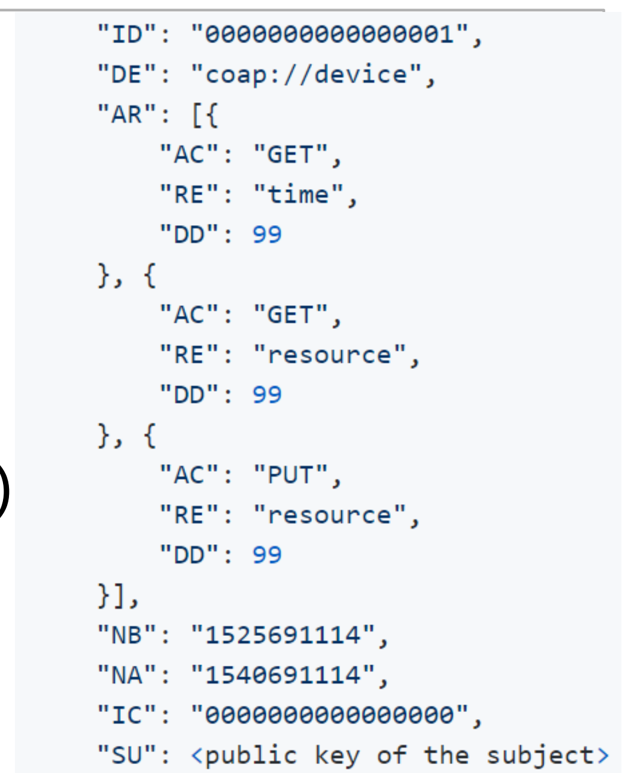
Approach

- Manage metadata of devices as standard description profiles
- Store profiles into federated and distributed IoT directories for retrieval
- Apply finer-grained access control combining roles and attributes
- Federated access using OAuth2 and OpenID
- Two-phase access control trusted by directories

Access Control for IoT

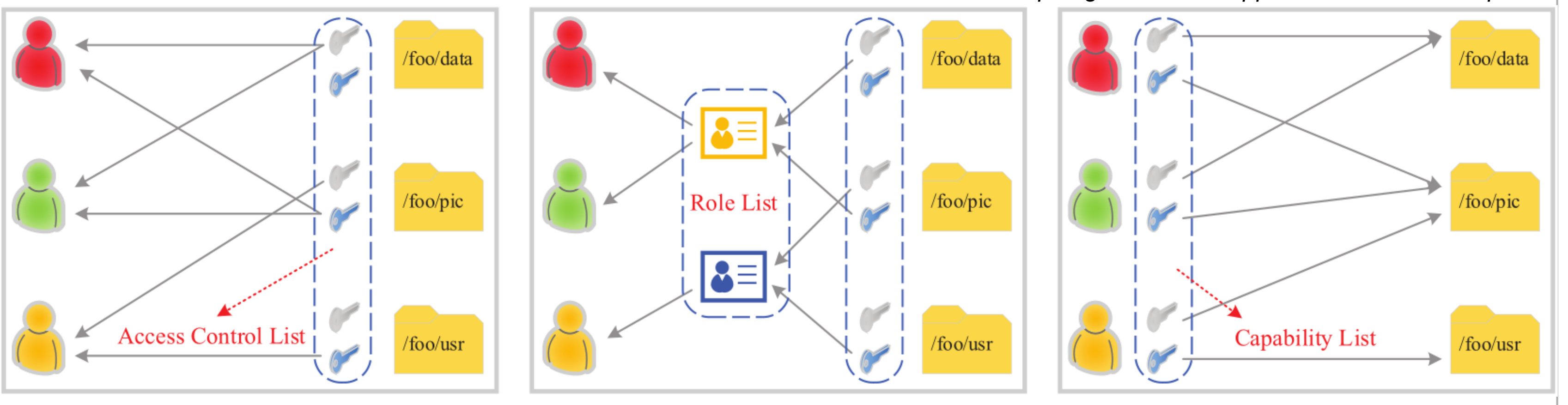
- Classic access control mechanisms
  - Traditional Access Control List (ACL)
  - Role-Based Access Control (RBAC)
  - Attribute-Based Access Control (ABAC)
  - Capability-Based Access Control (CapBAC)

(ranked from coarsest to finest granularity)



```
"ID": "0000000000000001",
"DE": "coap://device",
"AR": [{
    "AC": "GET",
    "RE": "time",
    "DD": 99
}, {
    "AC": "GET",
    "RE": "resource",
    "DD": 99
}, {
    "AC": "PUT",
    "RE": "resource",
    "DD": 99
}],
"NB": "1525691114",
"NA": "1540691114",
"IC": "0000000000000000",
"SU": <public key of the subject>
```

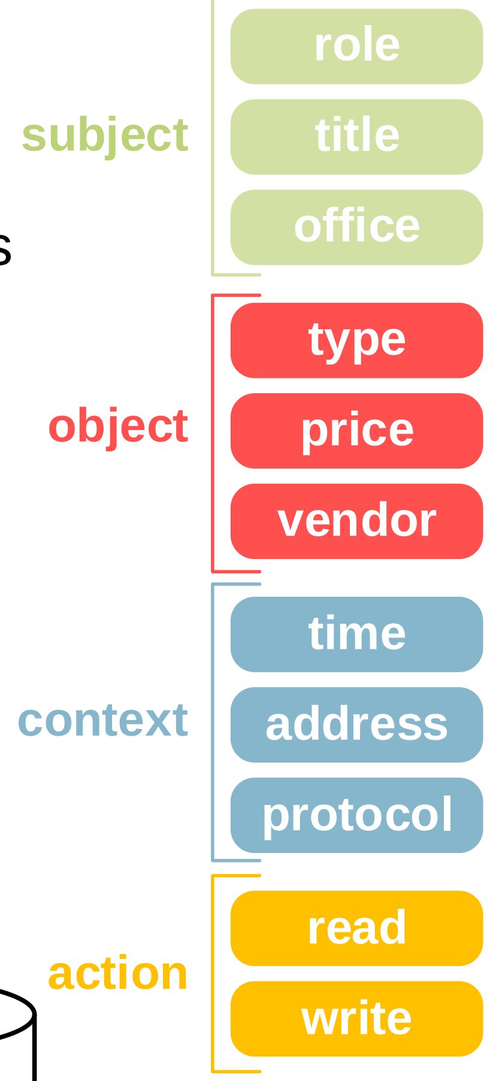
Delegable CapBAC token
https://github.com/Kappanneo/Sawtooth-CapBAC



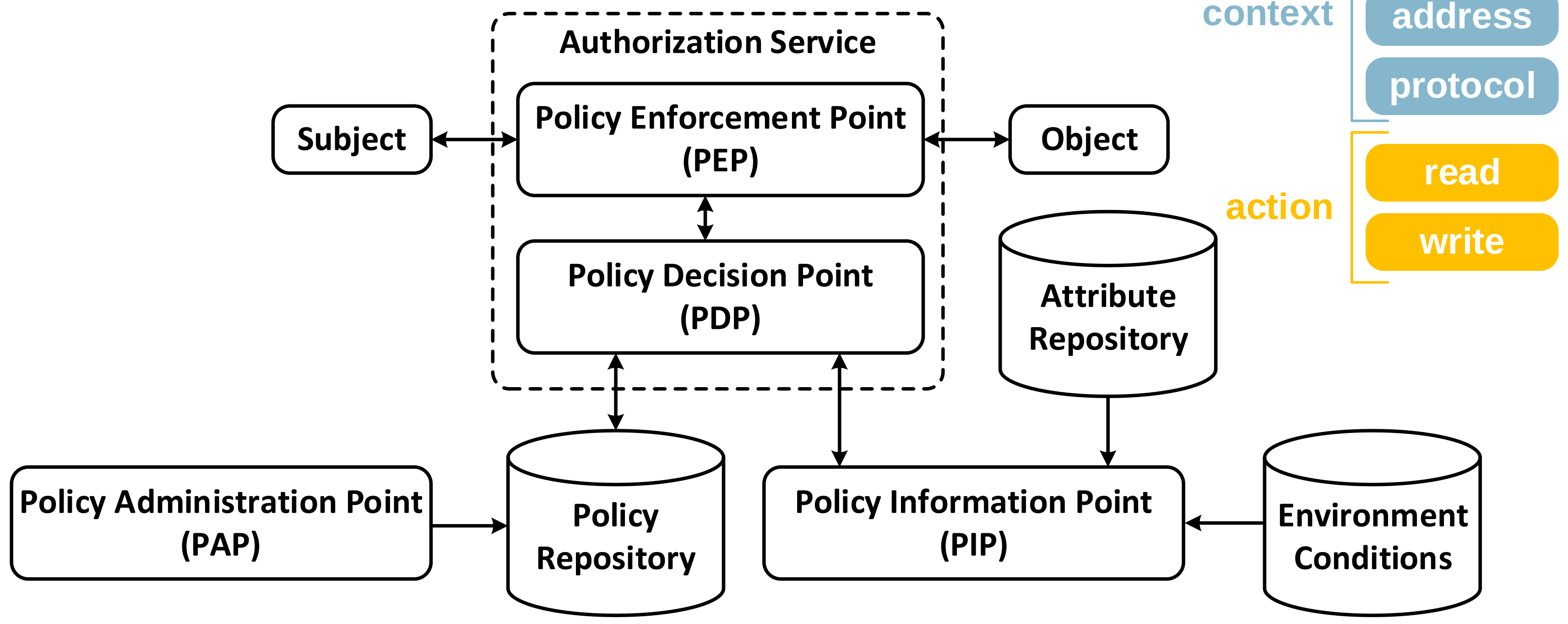
Comparison of access control list, role list, and capability list

Attribute-Based Access Control (ABAC)

- Access control rules inspired by the physical world
  - Grants users access to resources based on attributes
  - Flexible to define complex policies
- Not finest-grained, but manageable
  - OASIS XACML standard
  - Directory provides an additional layer of trust



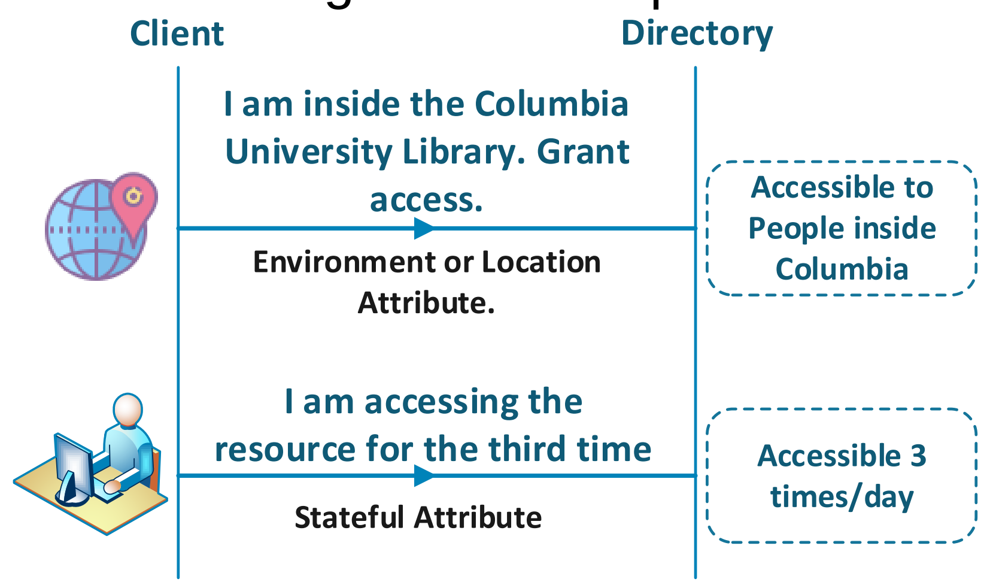
Common ABAC System Architecture


Authorization Service
Subject
Policy Enforcement Point (PEP)
Object
Policy Decision Point (PDP)
Attribute Repository
Policy Administration Point (PAP)
Policy Repository
Policy Information Point (PIP)
Environment Conditions

- PDP: compute access decision
- PEP: response to requests
- PIP: retrieve attributes and data
- PAP: manage and store policies

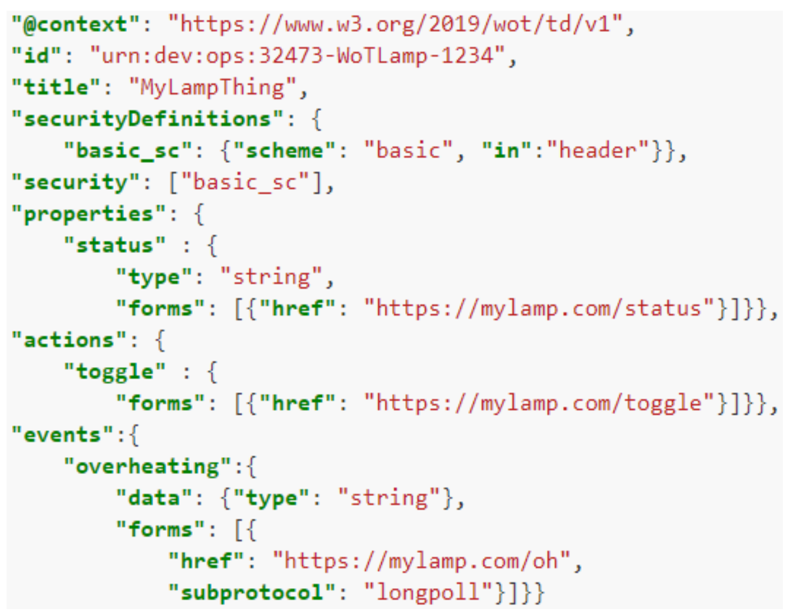
IoT poses new challenges

- Decentralized management
- Various attributes
- Customized policies
- Multiple administrative domains


Client
Directory
I am inside the Columbia University Library. Grant access.
Environment or Location Attribute.
Accessible to People inside Columbia
I am accessing the resource for the third time
Stateful Attribute
Accessible 3 times/day

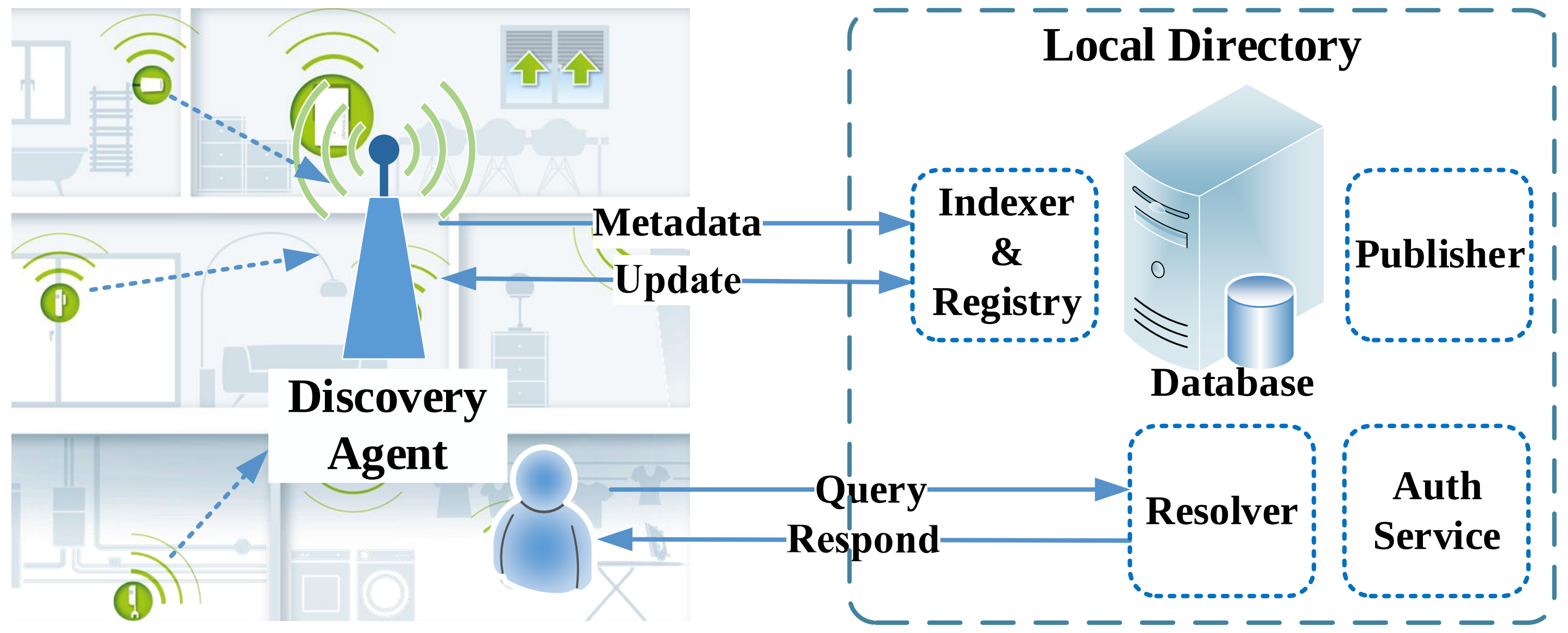
A Trusted Metadata Store

- Metadata directory as an intermediate Between IoT devices and the Internet
  - Gather metadata locally
  - Resolve queries globally
  - Storage and computing resources reasonably assumed to be enough



```
"@context": "https://www.w3.org/2019/wot/td/v1",
"id": "urn:dev:ops:32473-WoTLamp-1234",
"title": "MyLampThing",
"securityDefinitions": {
    "basic_sc": {"scheme": "basic", "in":"header"}},
"security": ["basic_sc"],
"properties": {
    "status" : {
        "type": "string",
        "forms": [{"href": "https://mylamp.com/status"}]}},
"actions": {
    "toggle" : {
        "forms": [{"href": "https://mylamp.com/toggle"}]}},
"events":{
    "overheating":{
        "data": {"type": "string"},
        "forms": [{
            "href": "https://mylamp.com/oh",
            "subprotocol": "longpoll"}]}}
```

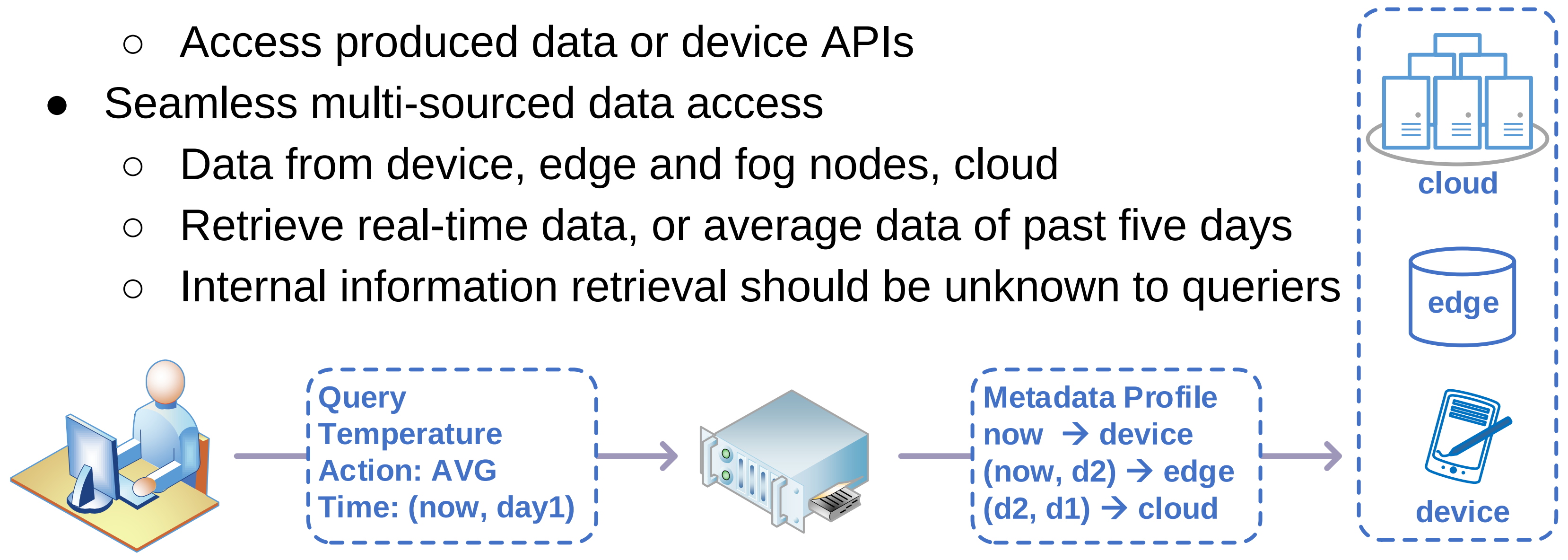
Source: W3C Thing Description



Functional modules of a local metadata directory

Directory-Assisted ABAC

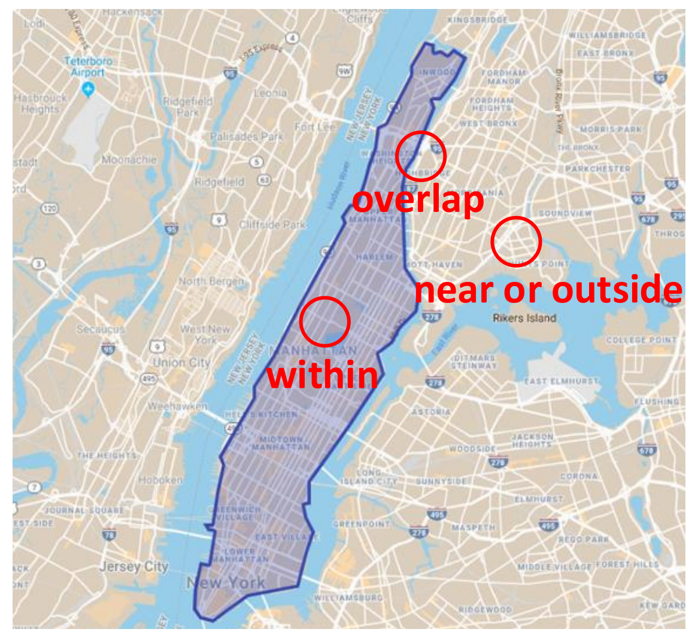
- Two-phase access approach
  - Discover metadata in distributed directories
  - Access produced data or device APIs
- Seamless multi-sourced data access
  - Data from device, edge and fog nodes, cloud
  - Retrieve real-time data, or average data of past five days
  - Internal information retrieval should be unknown to queriers

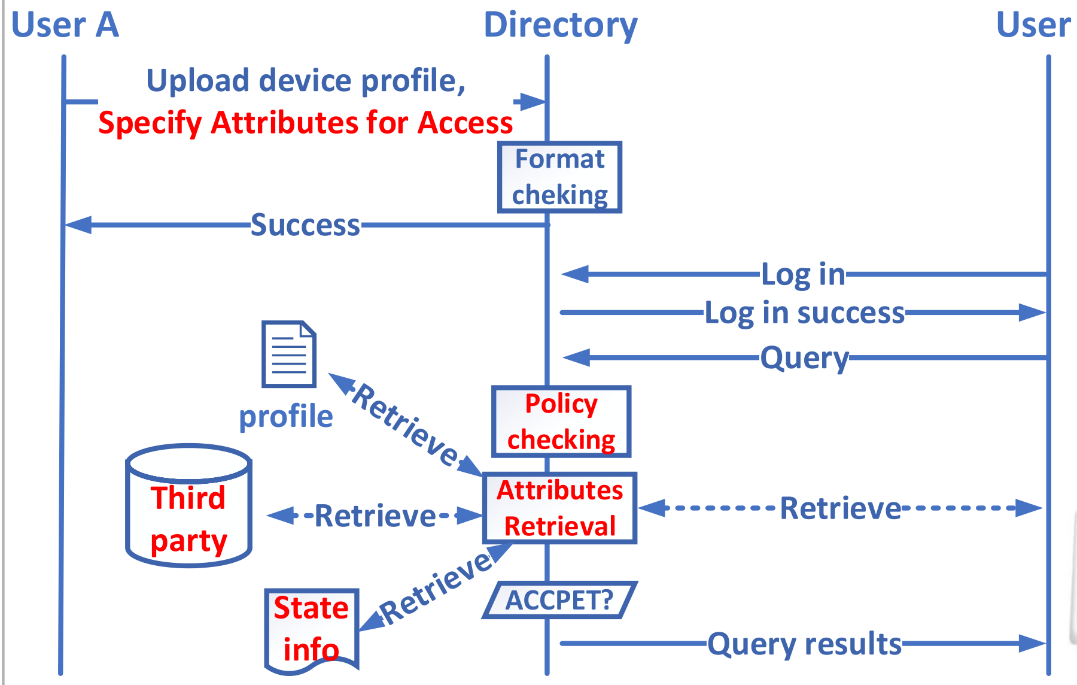


Data retrieved from different sources automatedly, and unknown to users

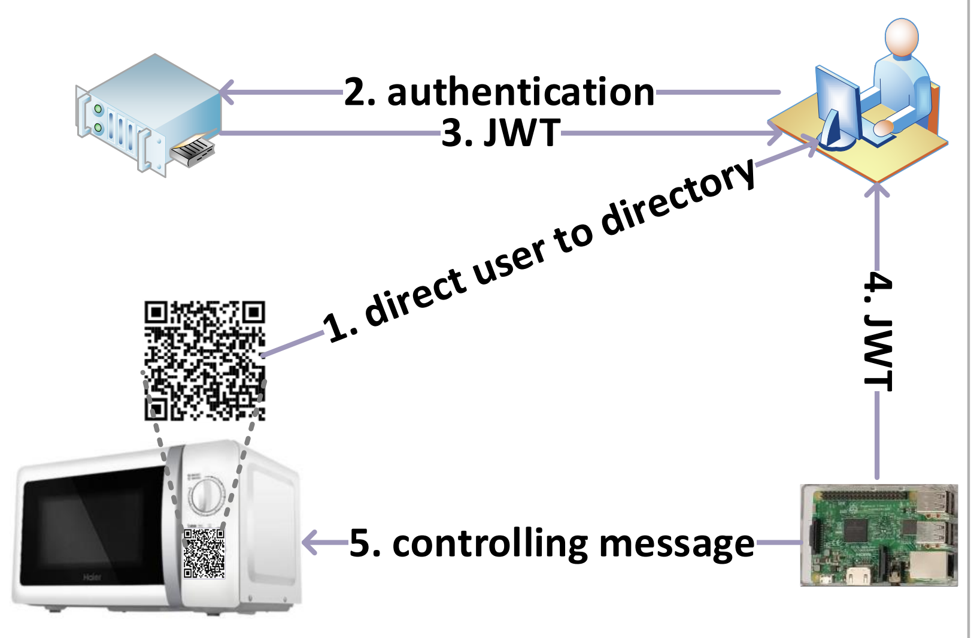
Attribute retrieval taxonomy

- Subject attributes through Single Sign On
- Object attributes through metadata profiles
- Attributes through third-party providers
- Geospatial attributes
  - Retrieve geospatial objects
- Stateful attributes through logs





Workflow of Directory-assisted ABAC



Directory-assisted access to device APIs

Challenges and Future Work

Attributes

- Automated, dynamic, and real-time device attributes update
- Represent and convert geospatial properties

Access Control

- Address multi-owner issues
- Grant least privileges in the directory-assisted access control system

References

1. W3C Thing Description. https://www.w3.org/TR/wot-thing-description/
2. Vincent Hu, et al. "Guide to attribute based access control (ABAC) definition and considerations." NIST special publication 800.162, 2014.
3. Luoyao Hao and Henning Schulzrinne. "When Directory Design Meets Data Explosion: Rethinking Query Performance for IoT." IEEE International Symposium on Networks, Computers and Communications, 2020.
4. Valenitna Beltran and Antonio Skarmeta. "Overview of Device Access Control in the IoT and its Challenges." IEEE Communications Magazine, pp. 1-7, 2019.

* Authors ordered alphabetically by last name