Access Control Models for a Multi-Cloud IoT Architecture

Smriti Bhatt, Farhan Patwa, and Ravi Sandhu

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

INTRODUCTION

- Internet of Things (IoT), a pervasive and diverse concept, refers to a network of Internet enabled smart devices and their communication with each other, applications and systems.
- With ubiquitous Internet, IoT devices and applications have started to play a vital role in every aspect of our lives with "anything" and "everything" being connected to the Internet.

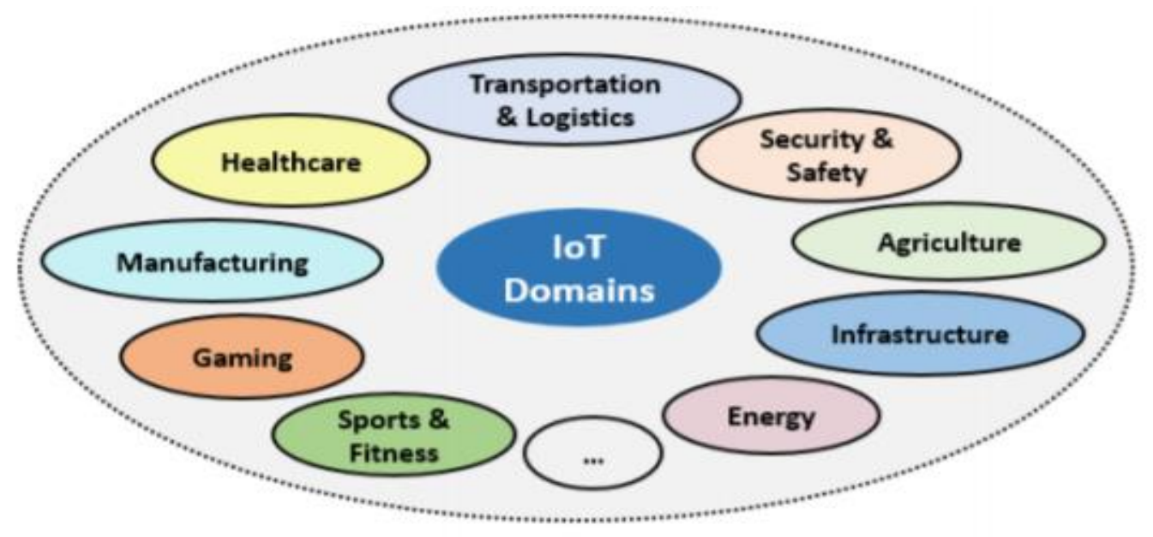


Figure 1: IoT Application Domains [1]

- A recent IoT architecture shaping the industry today is the integration of Cloud and IoT, with major cloud services providers offering IoT services and applications on top of their existing cloud services [1].

MOTIVATION

- Security and Privacy are the primary concerns that need to be addressed in a Cloud-enabled IoT (CEIoT) architecture.
- IoT devices and applications in some domains like healthcare and military are highly privacy and latency sensitive with low bandwidth and power capabilities.

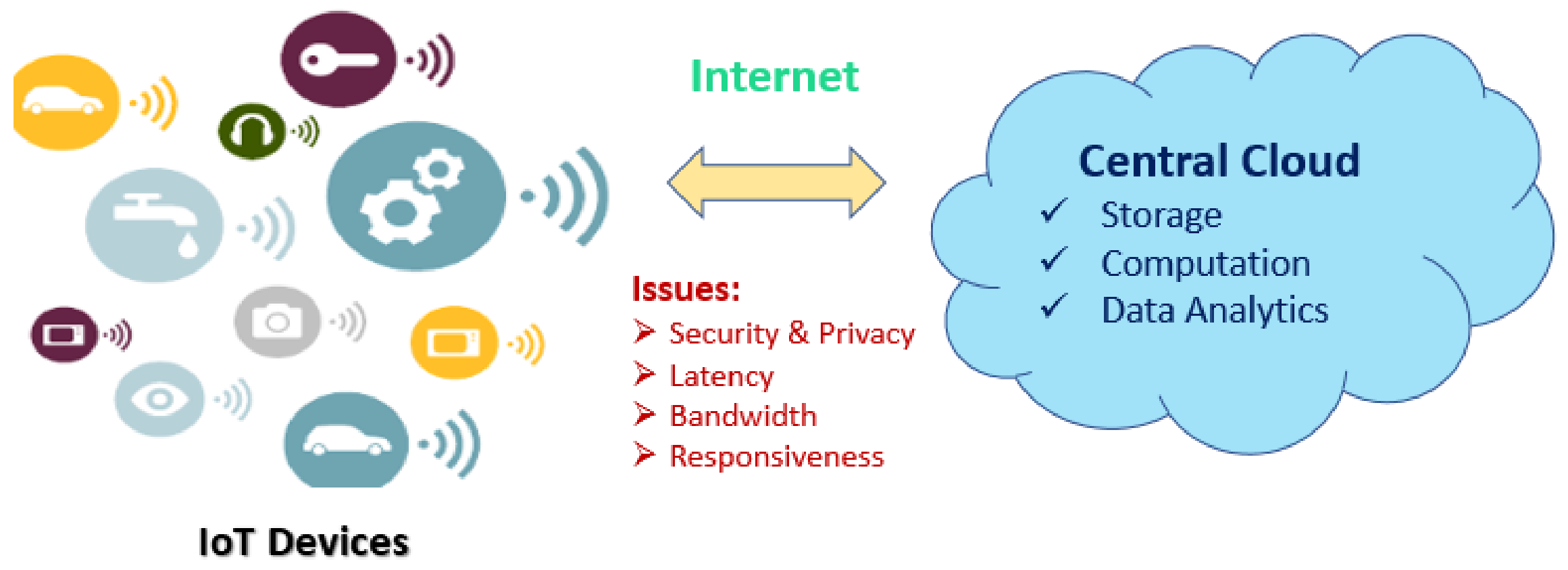


Figure 2: A Cloud-IoT Architecture

- Currently, most cloud-IoT platforms (e.g., AWS IoT [2], Azure IoT Suite [3], etc.) utilize a centralized single-cloud architecture to enable secure connection and communication in IoT.
- According to Gartner, there will be more than 25 billion connected IoT devices by 2020 [4], therefore, we believe that the need for a multi-cloud IoT architecture is inevitable to support IoT in the near future.
- Formal access control models addressing security and privacy issues in such an architecture are still not well-defined.

ACCESS CONTROL MODEL FOR AWS IoT

- Initially, we investigated a commercial cloud-enabled IoT (CEIoT) platform, viz., AWS IoT [2], and developed a formal access control model for it, the AWS-IoTAC model [5].
- AWS [6] uses a policy-based access control mechanism for its cloud and IoT services, where authorization policies can be attached to users, user groups, "roles", and certificates [2].

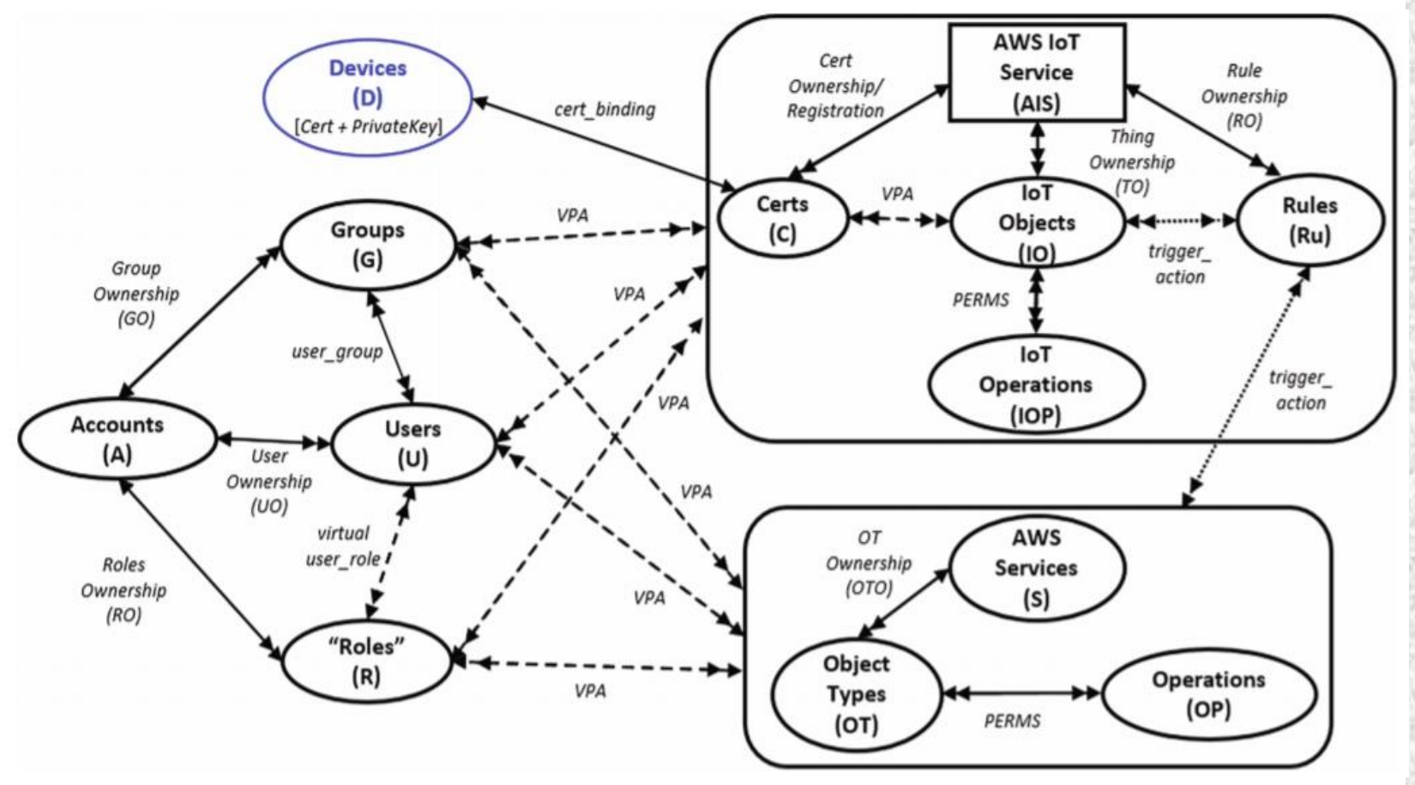
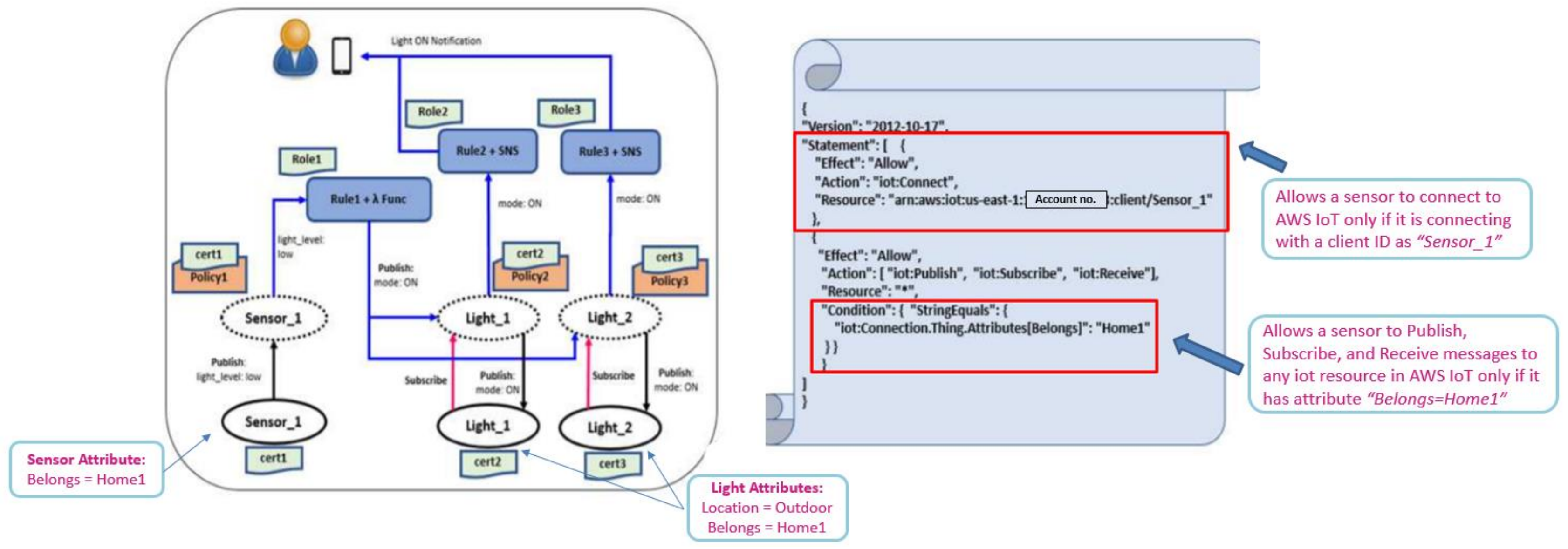


Figure 3: AWS IoT access control (AWS-IoTAC) model within a single account [4]

- Attributes of different entities, such as IoT things, could also be used in an authorization policy consistent with Attribute-based access control (ABAC) [7] but in limited scope.
- To demonstrate access control and authorization aspects of a CEIoT, we present a smart-home use case configured based on the AWS-IoTAC model utilizing AWS IoT and cloud services, with defined access control policies.



```
{
"Version": "2012-10-17",
"Statement": [   {
  "Effect": "Allow",
  "Action": "iot:Connect",
  "Resource": "arn:aws:iot:us-east-1: Account no. :client/Sensor_1"
  },
  {
   "Effect": "Allow",
   "Action": [ "iot:Publish",  "iot:Subscribe",  "iot:Receive"],
   "Resource": "*",
   "Condition": {  "StringEquals": {
     "iot:Connection.Thing.Attributes[Belongs]": "Home1"
    }}
   }
]
}
```

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

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

a. Use case setup in AWS IoT

b. Authorization policy for *Sensor 1*

Fig 5: A smart light use case scenario [5]

MULTI-CLOUD IoT ARCHITECTURE

- In a multi-cloud architecture, there are numerous IoT components, such as multiple-clouds, associated users, devices and applications, and interaction between these components need to be controlled with appropriate access control models.
- One of the IoT domains where multiple clouds interactions can be realized is health care.
- **A Remote Health and Fitness Monitoring (RHFM) Example [1]:**

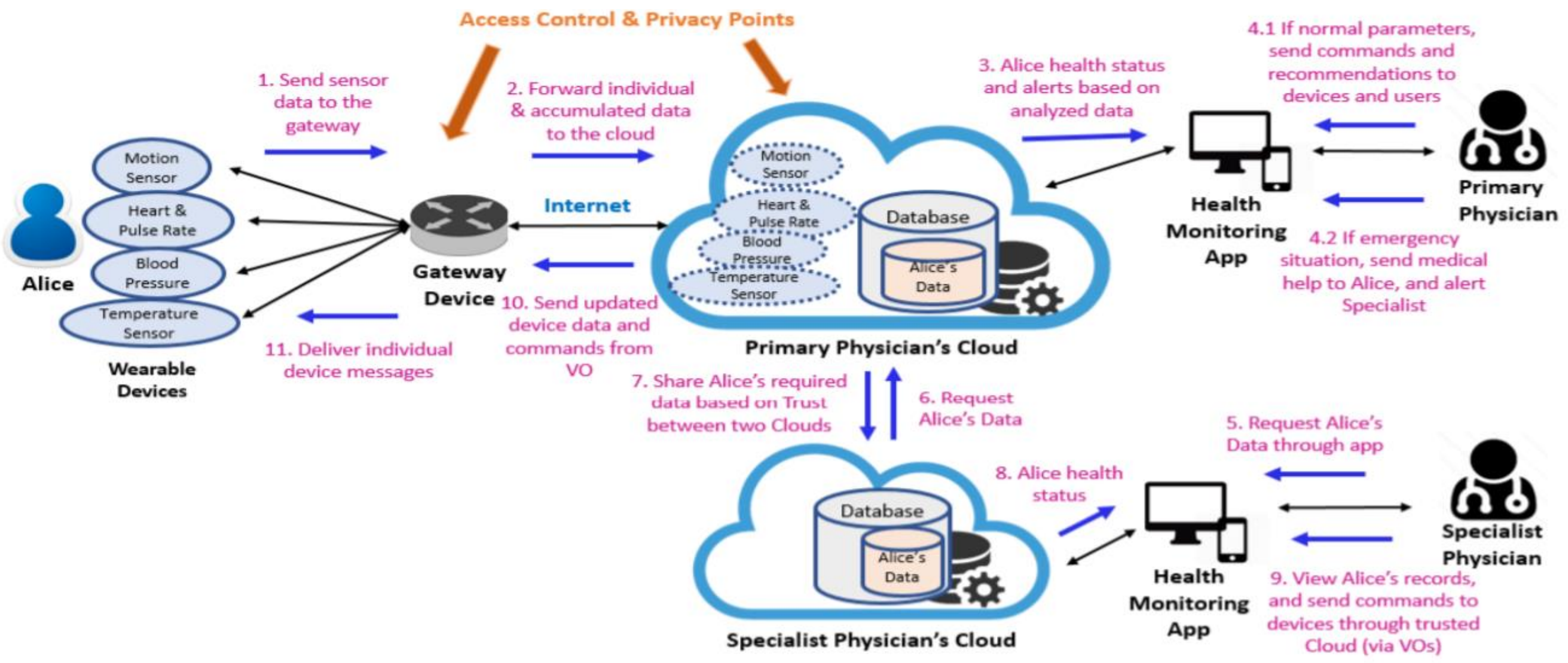

Access Control & Privacy Points
1. Send sensor data to the gateway
2. Forward individual & accumulated data to the cloud
3. Alice health status and alerts based on analyzed data
4.1 If normal parameters, send commands and recommendations to devices and users
Alice
Motion Sensor
Heart & Pulse Rate
Blood Pressure
Temperature Sensor
Wearable Devices
Gateway Device
Internet
Database
Alice's Data
Primary Physician's Cloud
Health Monitoring App
Primary Physician
4.2 If emergency situation, send medical help to Alice, and alert Specialist
10. Send updated device data and commands from VO
11. Deliver individual device messages
7. Share Alice's required data based on Trust between two Clouds
6. Request Alice's Data
5. Request Alice's Data through app
8. Alice health status
Specialist Physician's Cloud
Health Monitoring App
Specialist Physician
9. View Alice's records, and send commands to devices through trusted Cloud (via VOs)

Fig 6: A sequential view of RHFM Example [1]

ACCESS CONTROL IN MULTI-CLOUD IoT

- **Access Control Requirements:**
  - ➢ User-centric data security and privacy
  - ➢ Privacy-preserving policies at gateway level
  - ➢ Secure collaborative data sharing
  - ➢ Secure trust mechanisms between two or more clouds

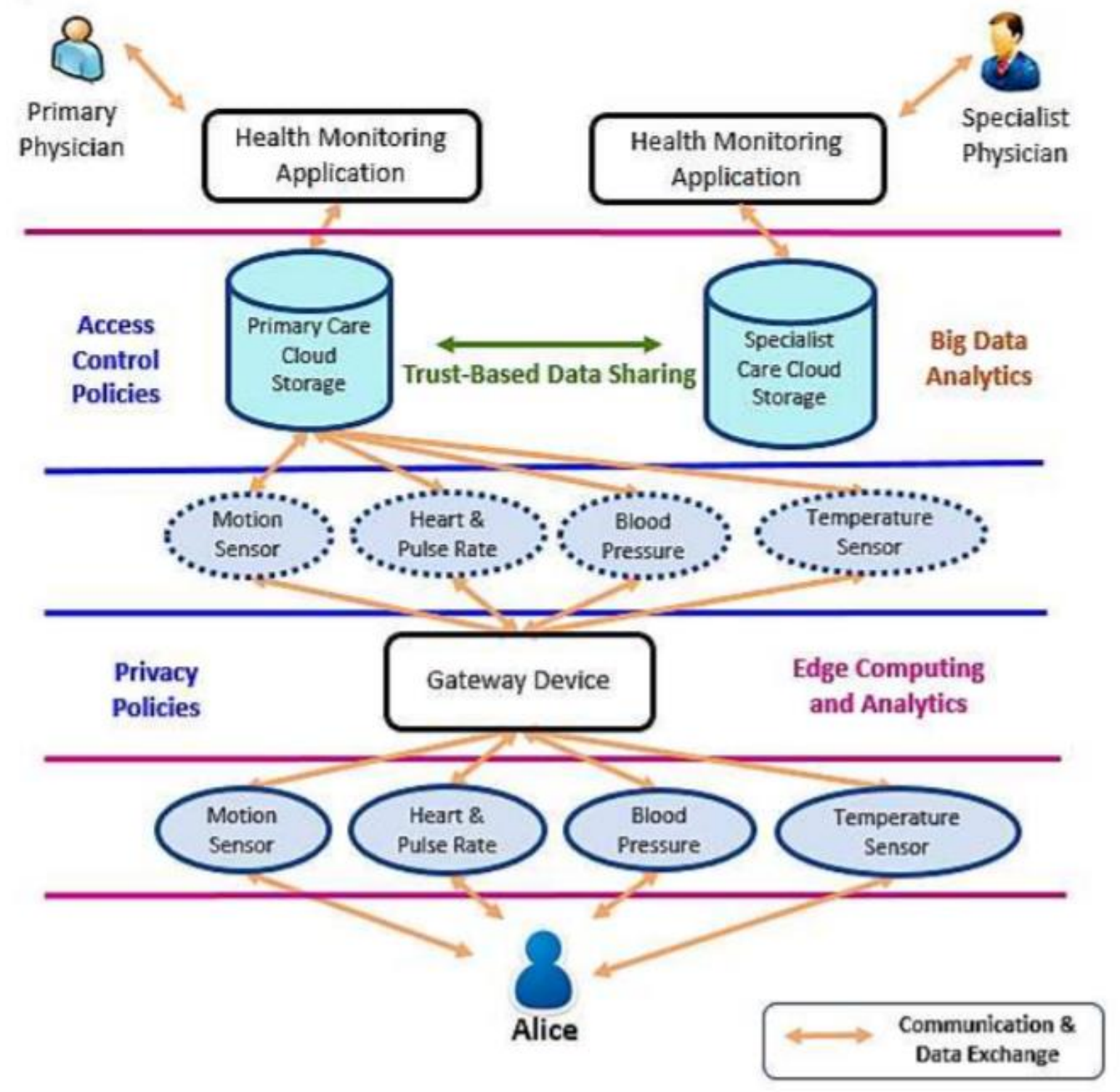


Figure 7: A layered view of RHFM example [1]

CONCLUSION & FUTURE WORK

- Access control model for AWS IoT will act as a base model and allow us to develop multi-cloud IoT models to control access to IoT entities and data in multiple cloud scenario (can be realized as cross-account in homogenous clouds).
- Besides role-based access control (RBAC) [8], ABAC is a promising approach for securing dynamic IoT space, moreover relationship-based access control (ReBAC) [9] is another model we plan to investigate to capture user-devices and other relationships.

REFERENCES

[1] Smriti Bhatt, Farhan Patwa and Ravi Sandhu, "An Access Control Framework for Cloud-Enabled Wearable Internet of Things". [To be Published] In Proceedings of the 3rd IEEE International Conference on Collaboration and Internet Computing (CIC), San Jose, CA, October 15-17, 2017, 11 pages.

[2] AWS IoT Platform, http://docs.aws.amazon.com/iot/latest/developerguide/ what-is-aws-iot.html.

[3] Azure IoT Suite, https://azure.microsoft.com/en-us/suites/iot-suite/.

[4] "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," http://www.gartner.com/newsroom/id/2636073.

[5] Bhatt, Smriti, Farhan Patwa, and Ravi Sandhu. "Access Control Model for AWS Internet of Things." In *International Conference on Network and System Security*, pp. 721-736. Springer, Cham, 2017.

[6] Amazon Web Services (AWS), https://aws.amazon.com/.

[7] Jin, Xin, Ram Krishnan, and Ravi S. Sandhu. "A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC." *DBSec* 12 (2012): 41-55.

[8] Sandhu, Ravi S., Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-based access control models." *Computer* 29, no. 2 (1996): 38-47.

[9] Cheng, Yuan, Jaehong Park, and Ravi Sandhu. "Relationship-based access control for online social networks: Beyond user-to-user relationships." In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, pp. 646-655. IEEE, 2012.