I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

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.

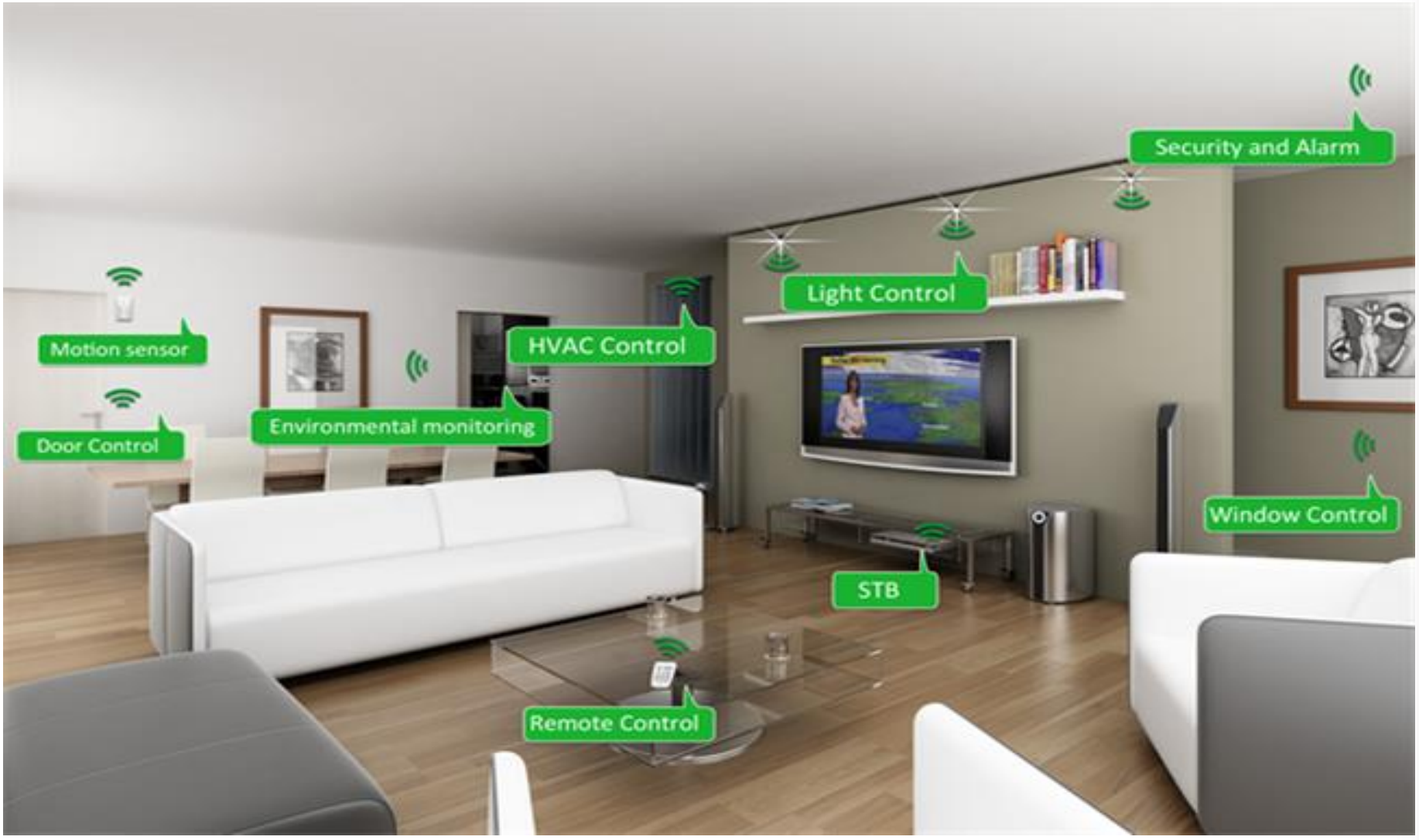
UTSA Computer Science

Outline

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

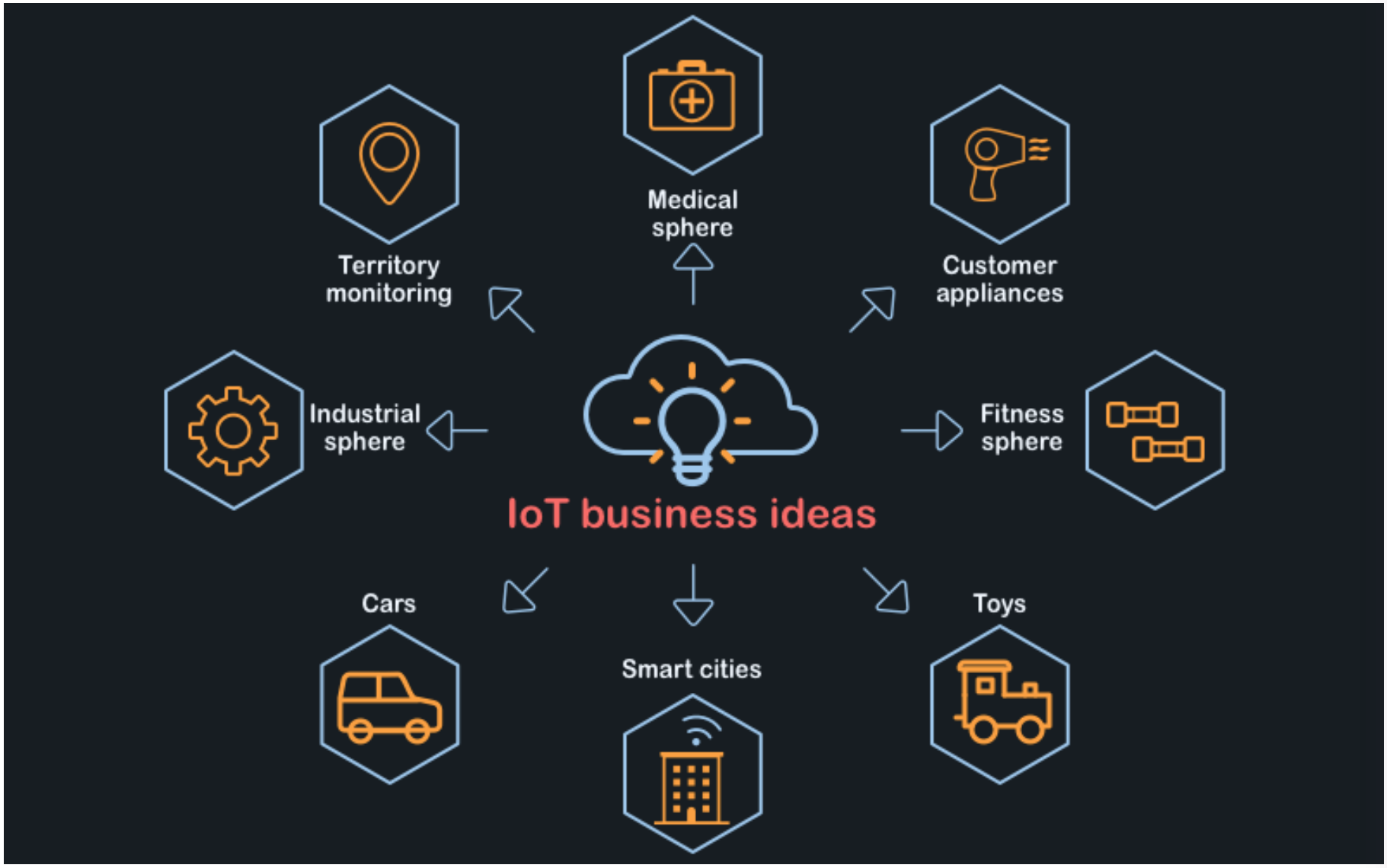
© Asma Alshehri

Internet of Things



© Asma Alshehri

IoT Projects



© Asma Alshehri

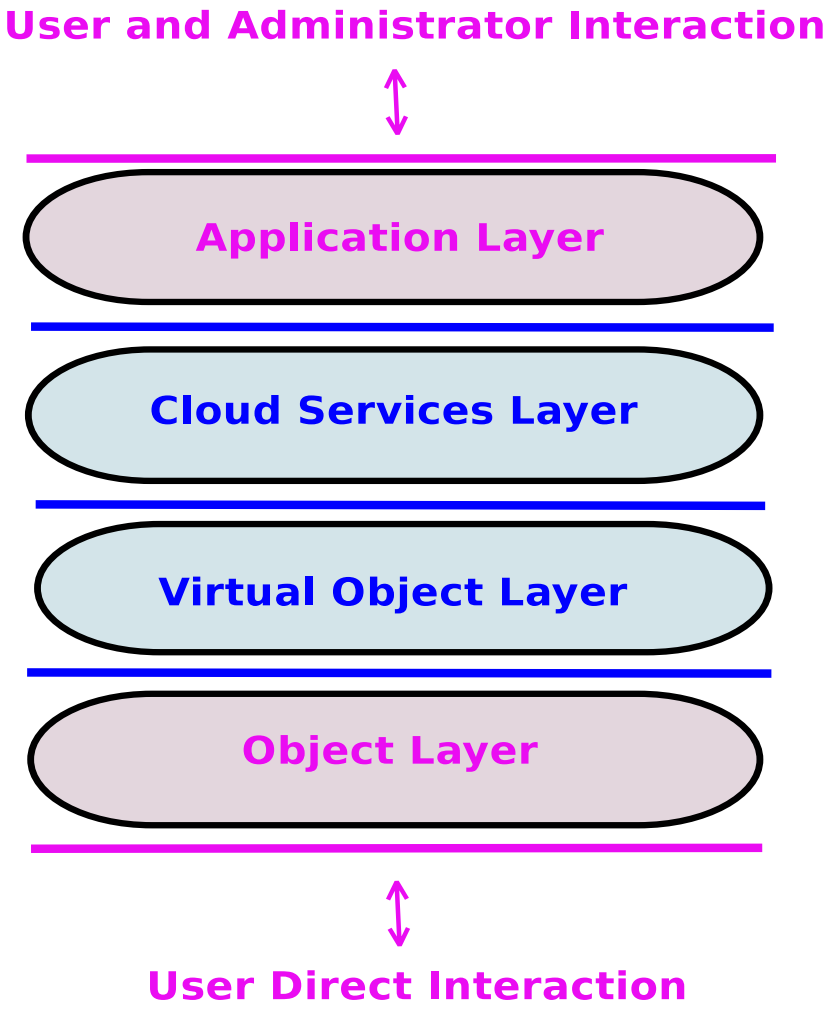
Access Control Oriented (ACO) Architecture for Cloud-Enabled IoT

Asma Alshehri and Ravi Sandhu. Access control models for cloud-enabled internet of things: A proposed architecture and research agenda. In the 2nd IEEE International Conference on Collaboration and Internet Computing (CIC), pages 530-538. IEEE, 2016.

© Asma Alshehri

Access Control Oriented (ACO) Architecture for IoT

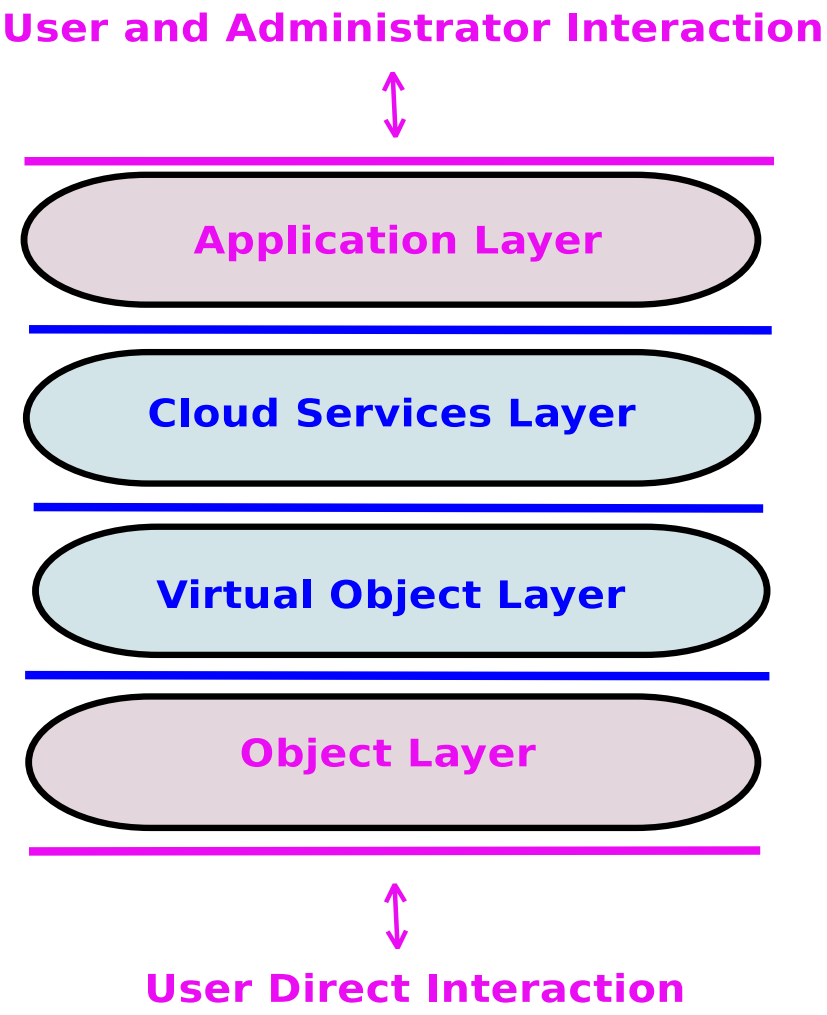
- **The Object layer:**
  - Physical objects
  - Collect data
  - Communication
- **The Virtual Object Layer:**
  - Presents status of objects
  - Communication
  - O-VO Association



© Asma Alshehri

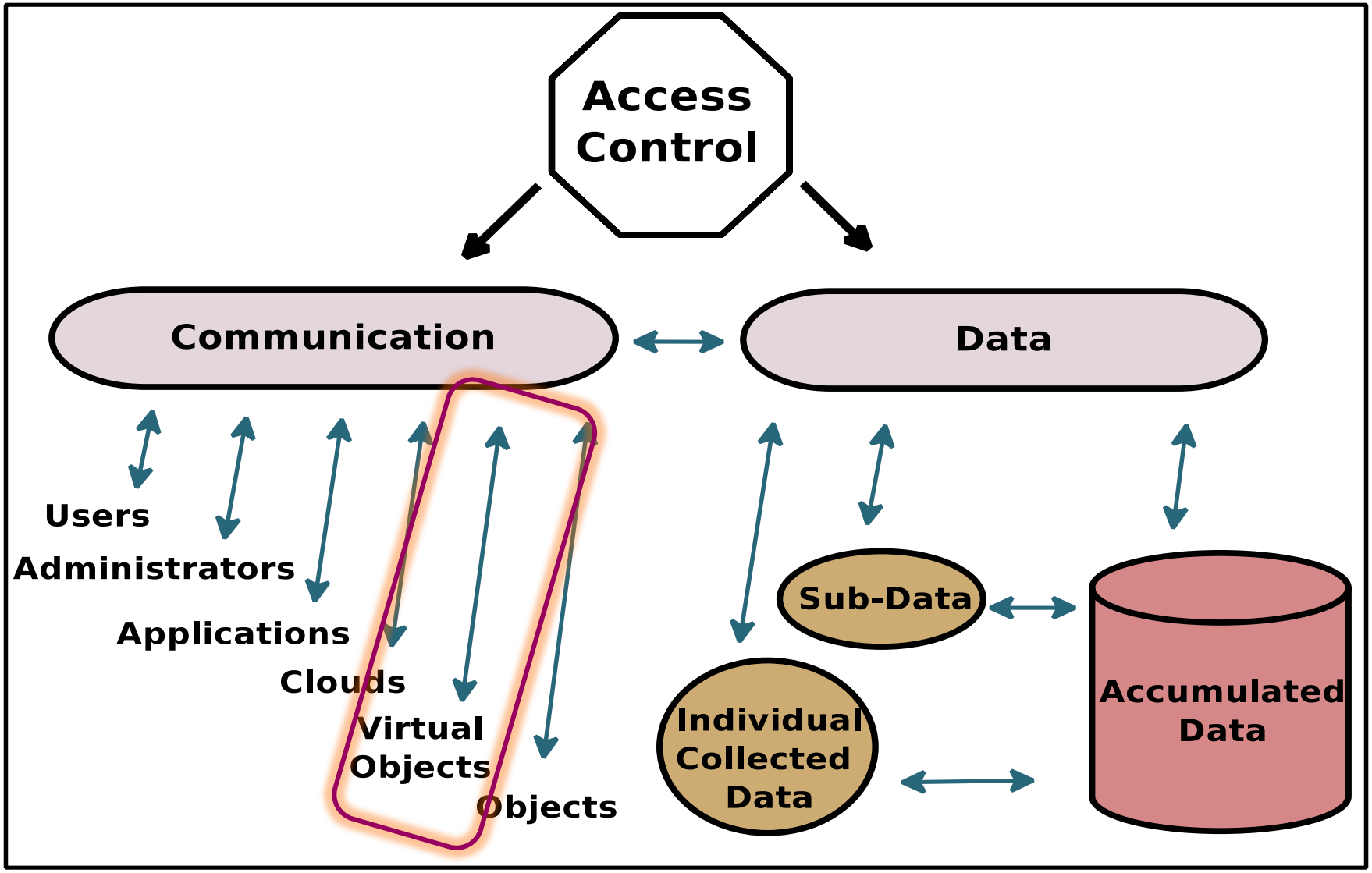
Access Control Oriented (ACO) Architecture for IoT

- **The Cloud Layer:**
  - Big data
  - Functionality
  - Communication
- **The Application Layer:**
  - Interface
  - Users and Admin
  - Generate AC policies



© Asma Alshehri

Access Control Issues in ACO Architecture for IoT



© Asma Alshehri

Access Control Models for VO Communications in ACO Architecture

Asma Alshehri and Ravi Sandhu. Access control models for virtual object communication in cloud-enabled iot. In The 18th International Conference on Information Reuse and Integration (IRI). IEEE, 2017.

© Asma Alshehri

Access Control Models for VO Communication

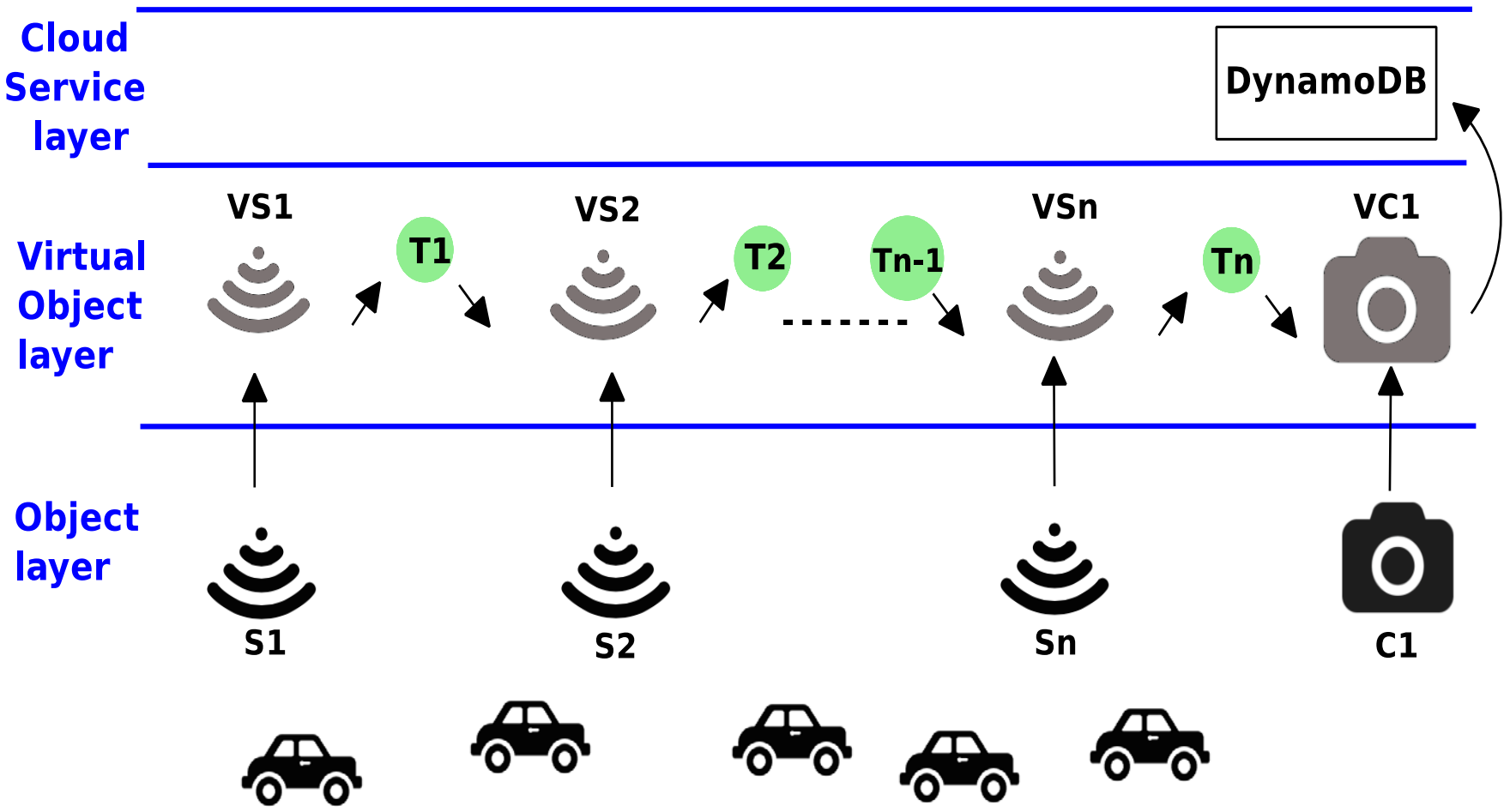
Access control models for VO communication in two layers:

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

© Asma Alshehri

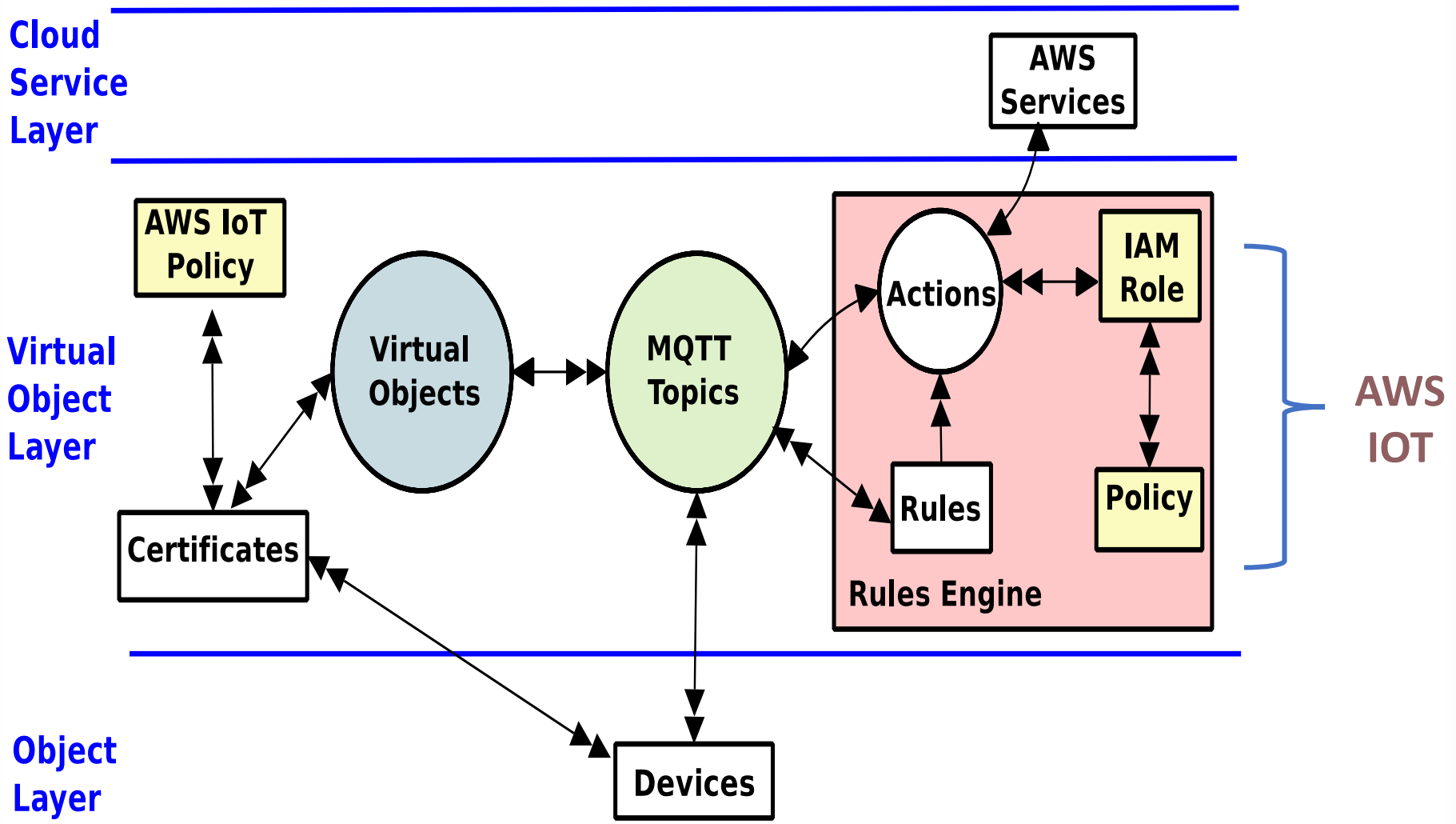
A Use Case within ACO Architecture



Access Control Model for VO Communication for AWS IoT

© Asma Alshehri

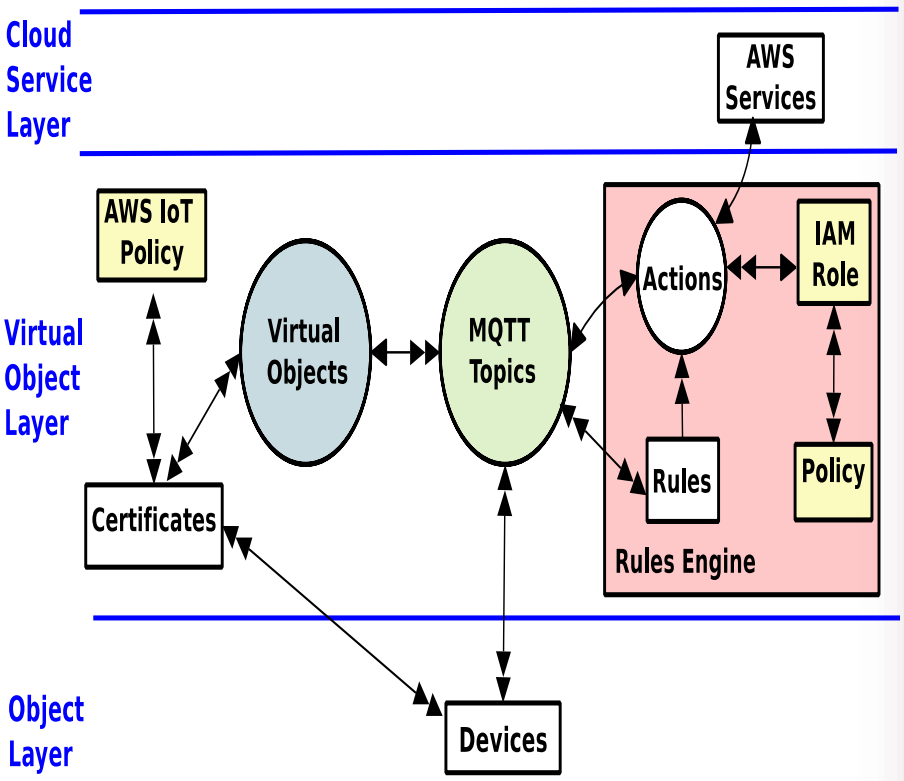
The AWS-IoT-ACMVO Model for AWS IoT



© Asma Alshehri

The AWS-IoT-ACMVO Model for AWS IoT

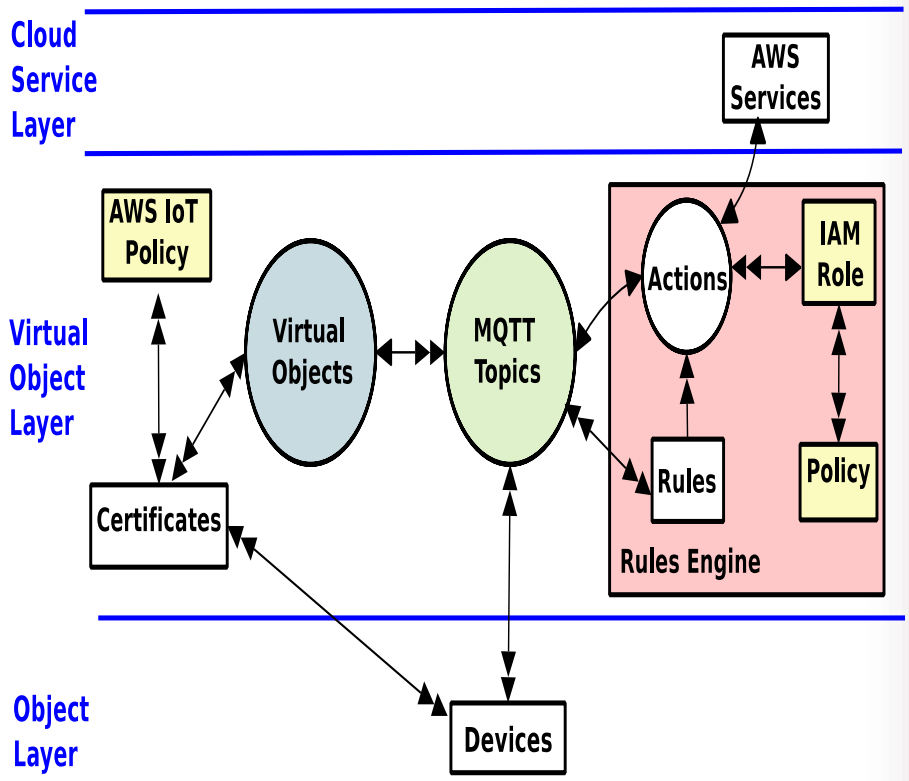
- Certificates: An identity for devices authentication
- AWS IoT policy: A policy for authorization purpose
- Virtual objects: A JSON document that stores information about the current and future status of a device.
- MQTT topics: AWS IoT service generates reserved MQTT topics for each created virtual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



© Asma Alshehri

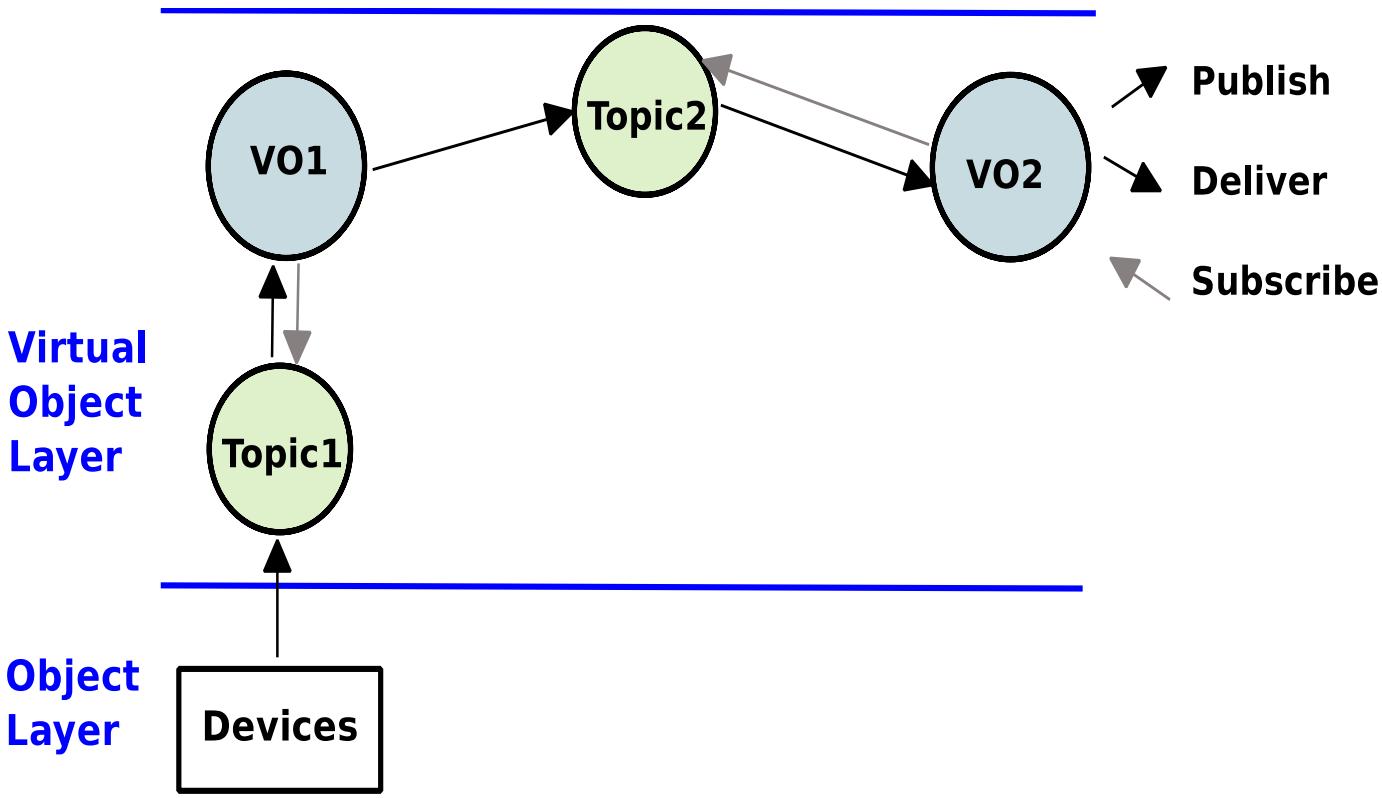
The AWS-IoT-ACMVO Model for AWS IoT

- 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



© Asma Alshehri

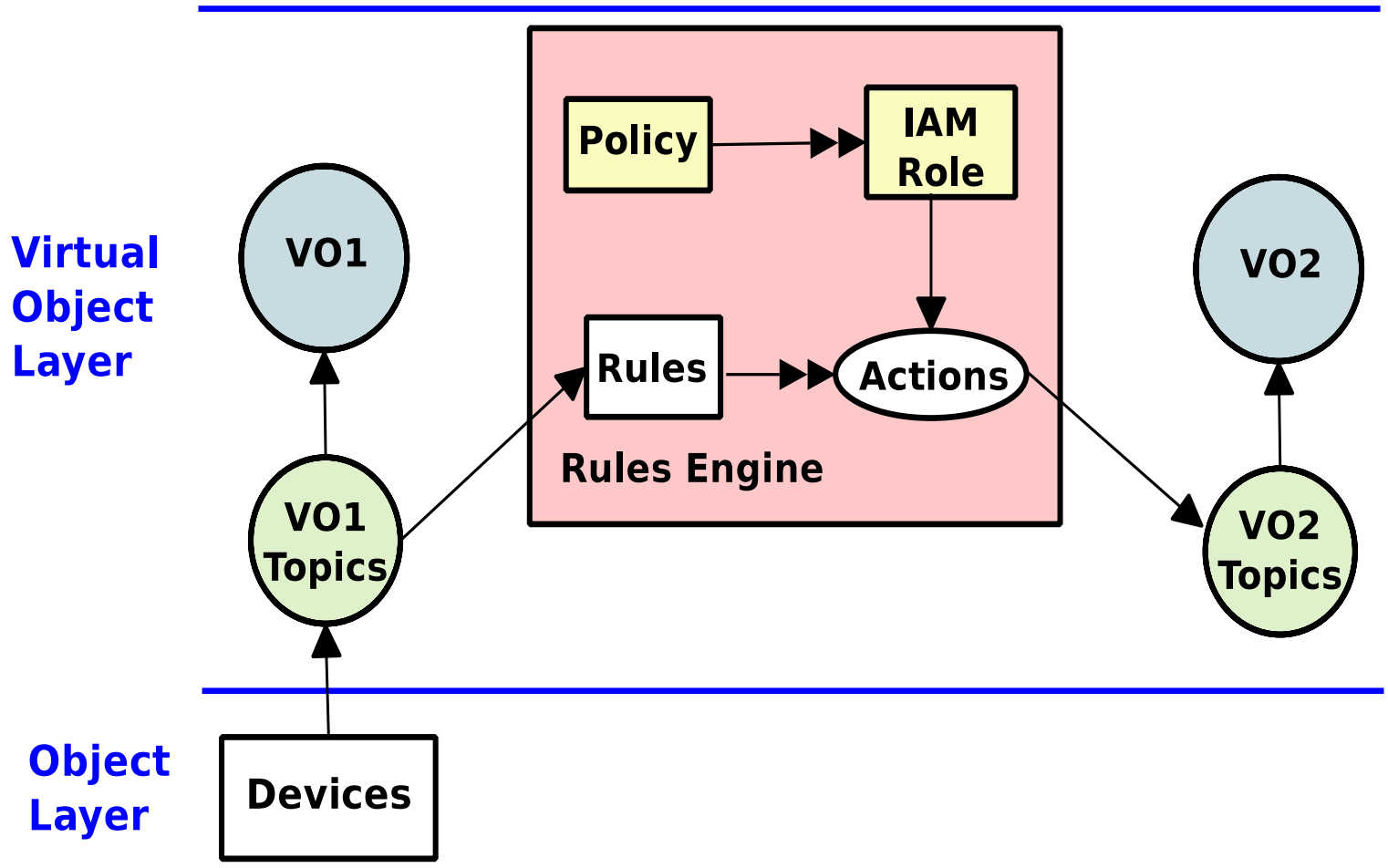
The Publish/Subscribe Topic-Based Scheme



- The communication channel between two VOs is a shared topic

© Asma Alshehri

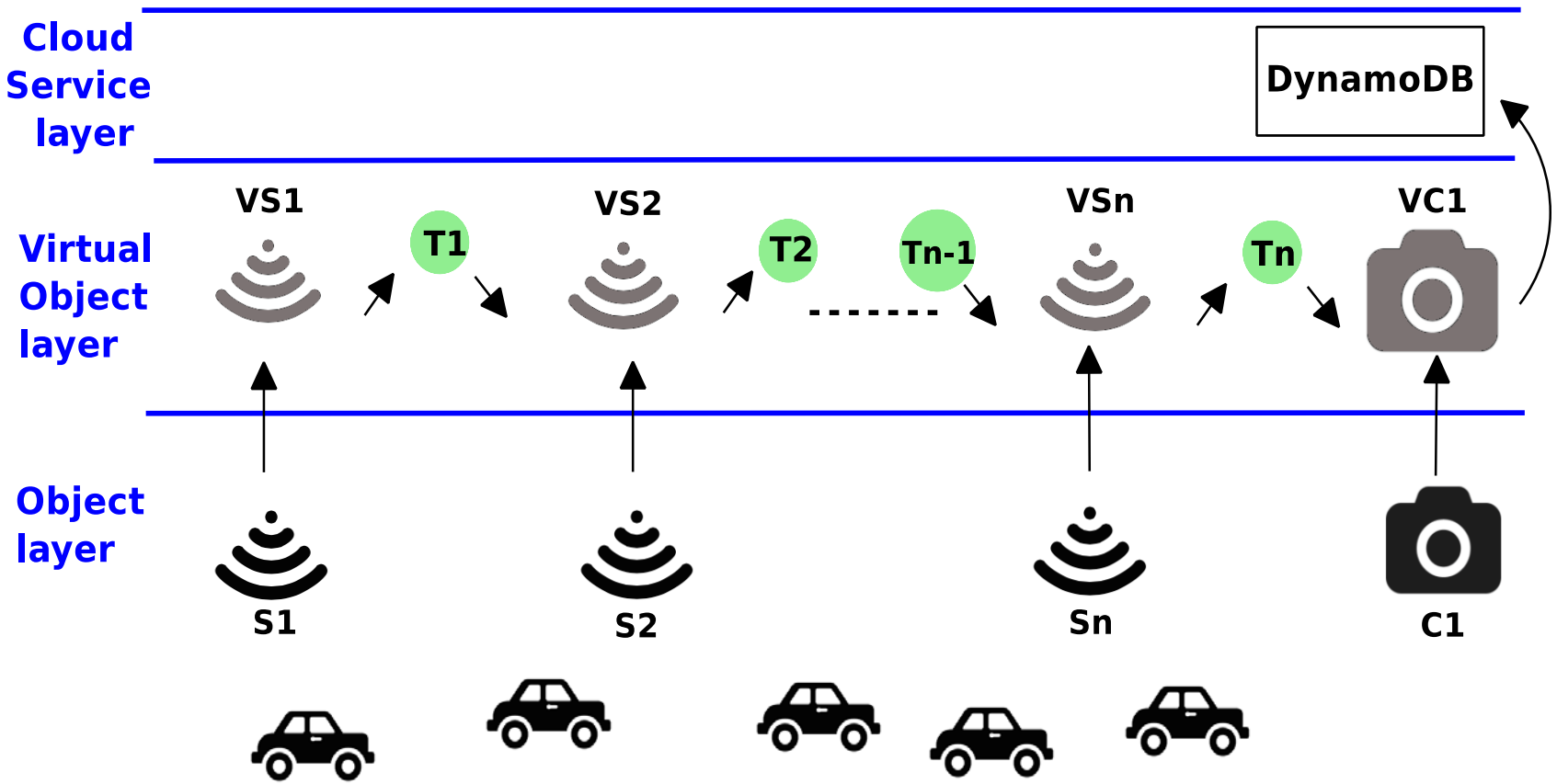
Communication Channel in AWS IoT



- The communication channel between two VO Topics is the Rules Engine

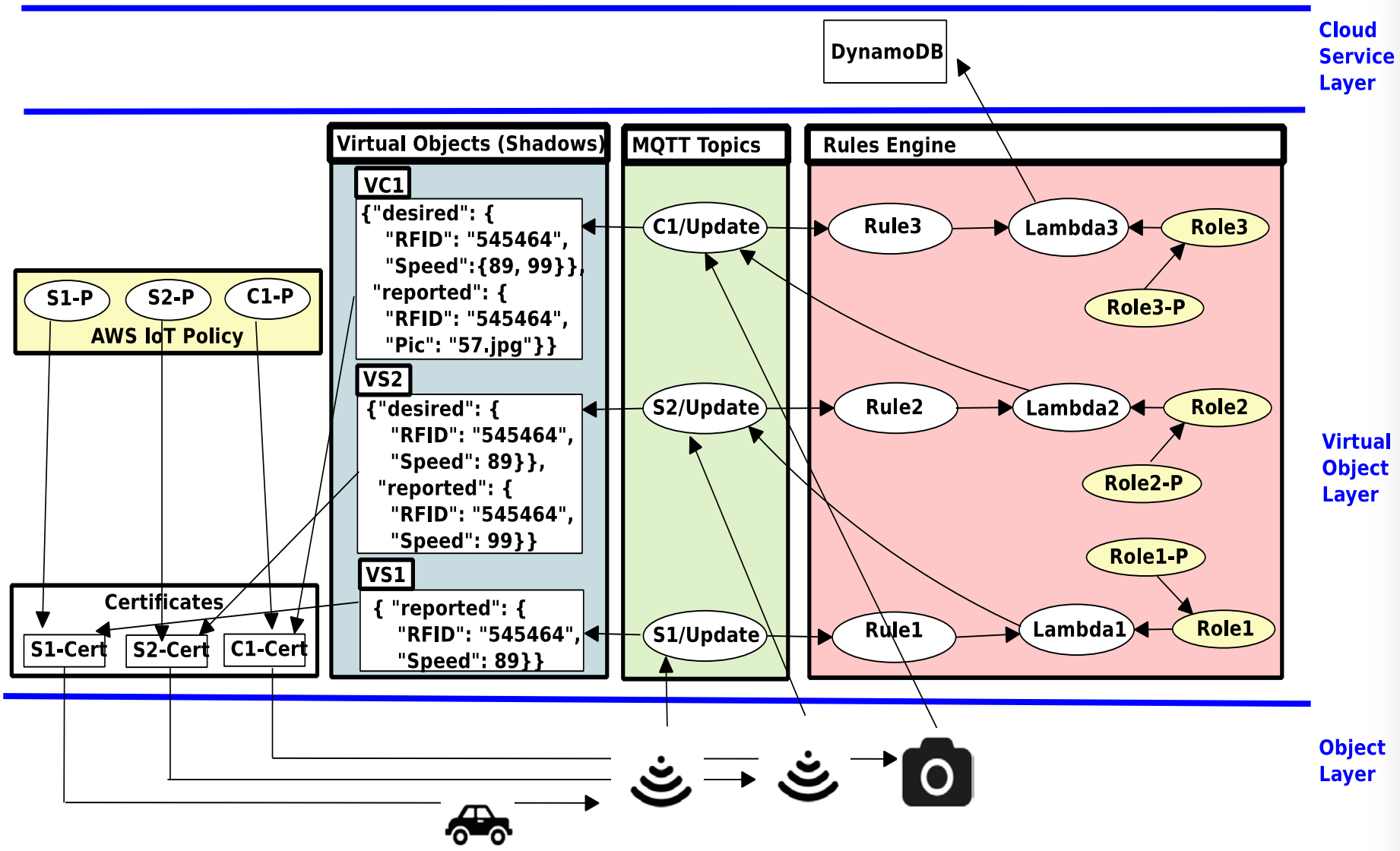
© Asma Alshehri

The Sensing Speeding Cars Use Case



© Asma Alshehri

Sensing the Speed of One Car with two Sensors



© Asma Alshehri

Role2 Policy that is Attached to Role2

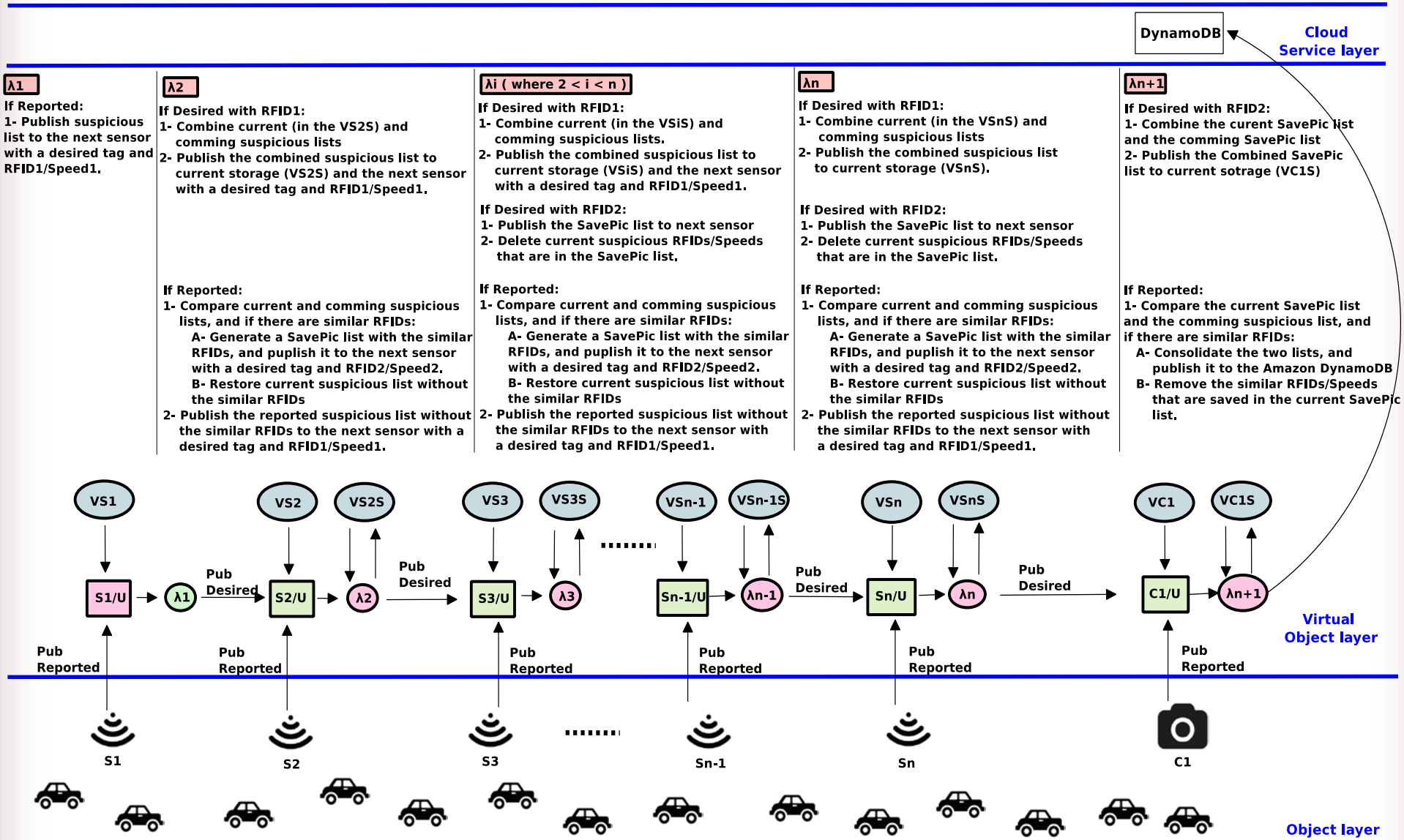

```
{
   "Version": "2012-10-17",
   "Statement": [
      {  "Effect": "Allow",
         "Action": "iot:GetThingShadow",
         "Resource": "arn:aws:iot:us-west-2:760000000000:
          thing/Sensor2"
      },
      {  "Effect": "Allow",
         "Action": "iot:Publish",
         "Resource": "arn:aws:iot:us-west-2:760000000000:
          topic/$aws/things/Camera/shadow/update"
      }
   ]
}
```

© Asma Alshehri

Sensing the Speed of Multiple Cars with Multiple sensors

I·C·S The Institute for Cyber Security

C·SPECC Center for Security and Privacy Enhanced Cloud Computing

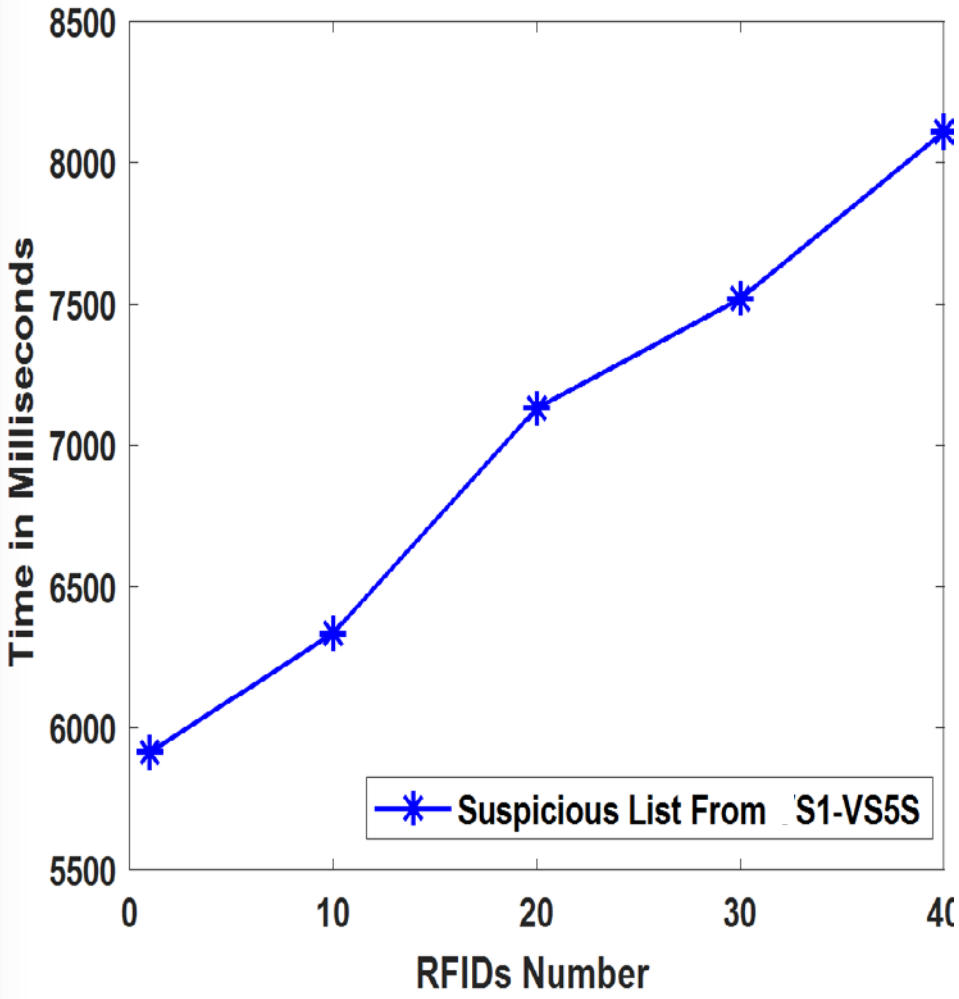


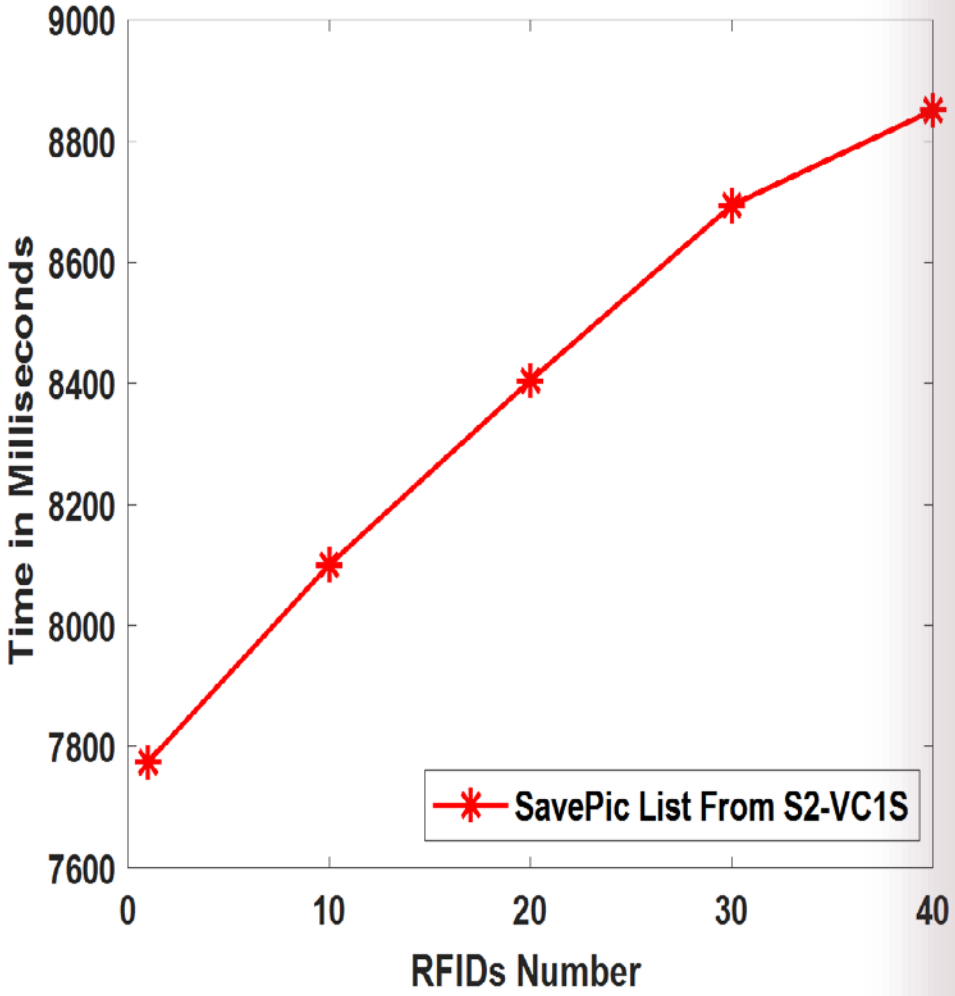
© Asma Alshehri

World-Leading Research with Real-World Impact!

UTSA Computer Science

Performance





© Asma Alshehri

Conclusion and Future Work

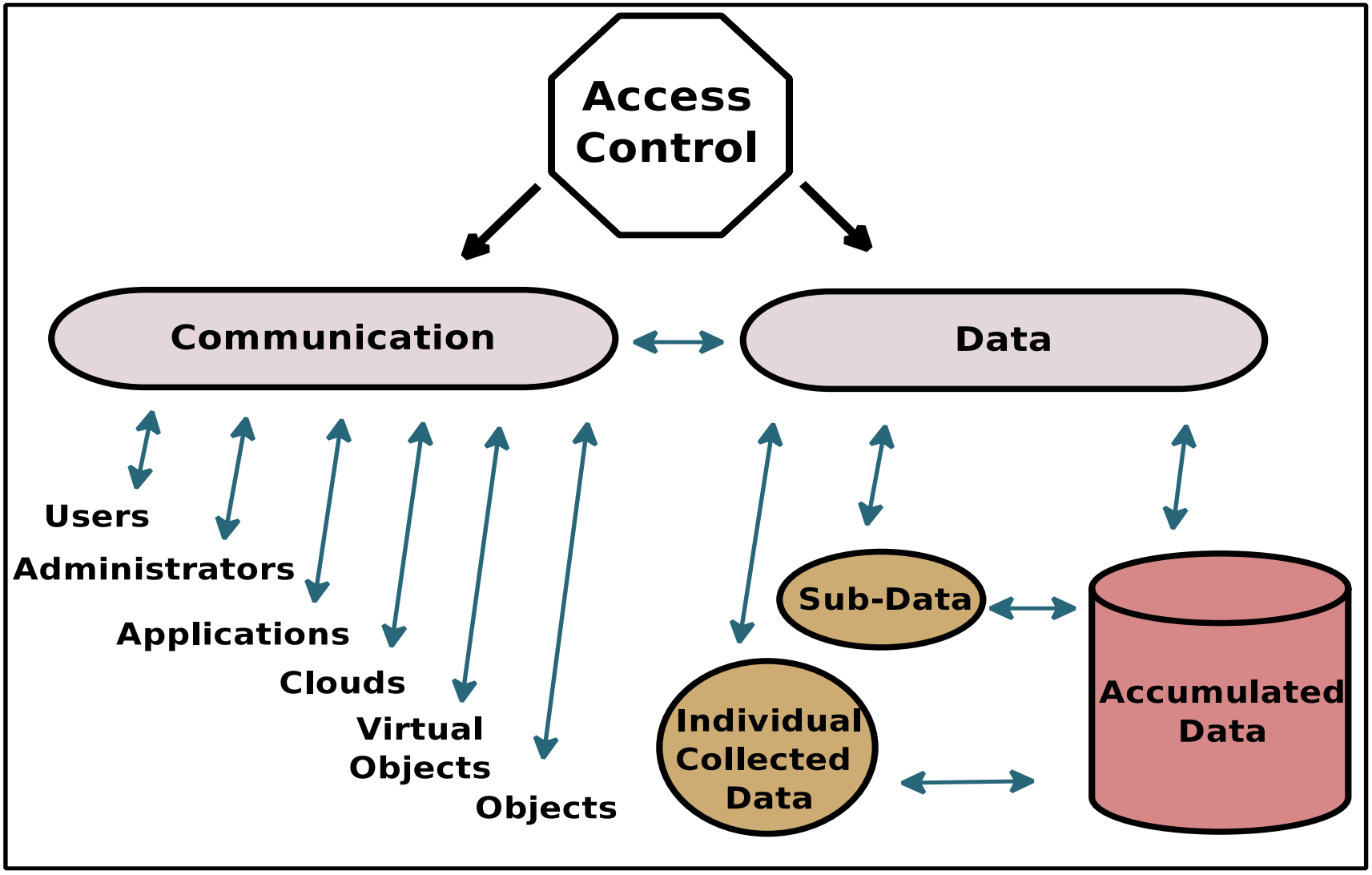
© Asma Alshehri

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

© Asma Alshehri

Future Work



© Asma Alshehri

Questions

© Asma Alshehri