I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Access Control Models for Cloud-Enabled Internet of Things

Ph.D. Dissertation Defense

By

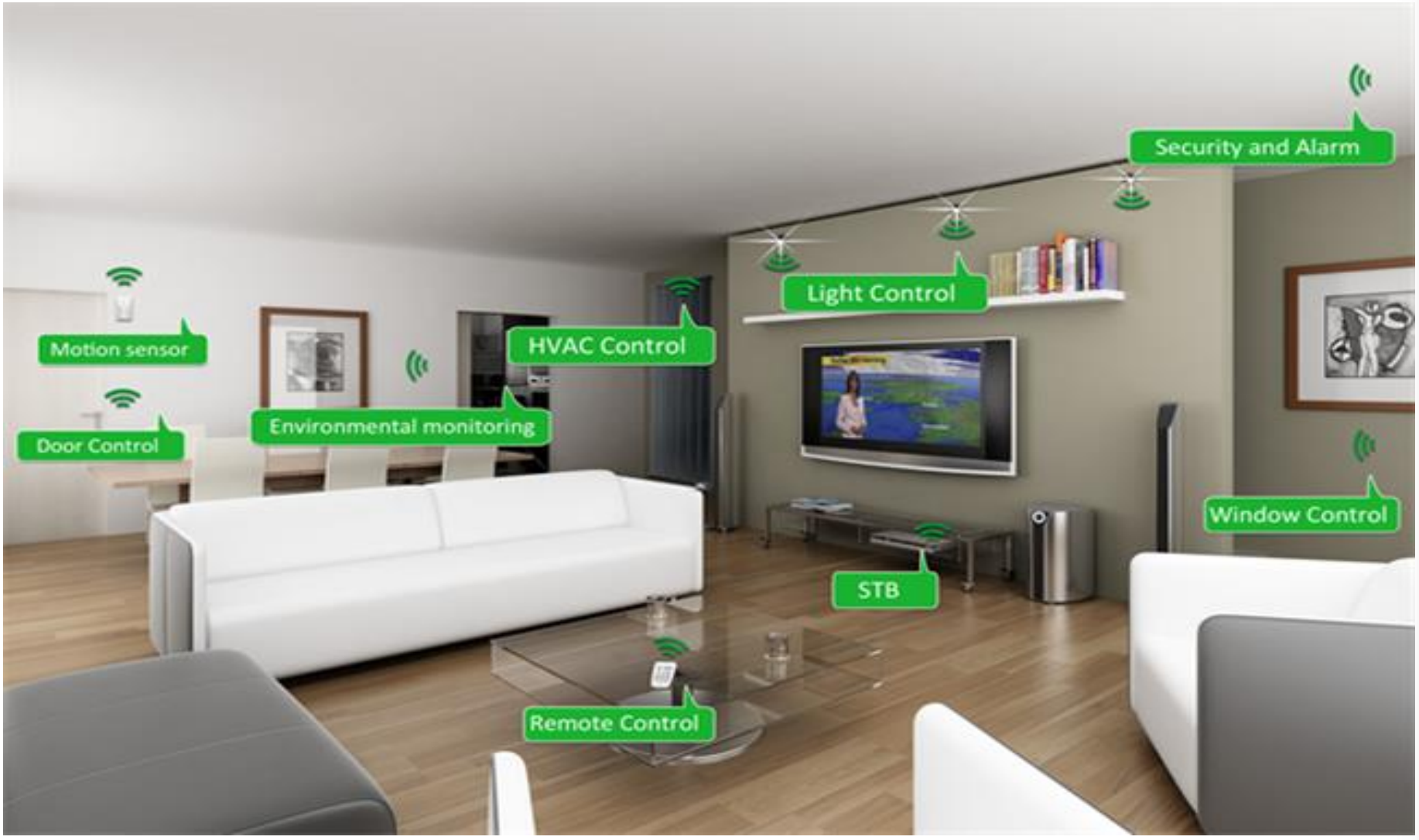
Asma Alshehri

Department of Computer Science
University of Texas San Antonio

Advisor: Dr. Ravi Sandhu
Committee: Dr. Gregory B. White
Dr. Matthew Gibson
Dr. Palden Lama
Dr. Ram Krishnan

UTSA Computer Science

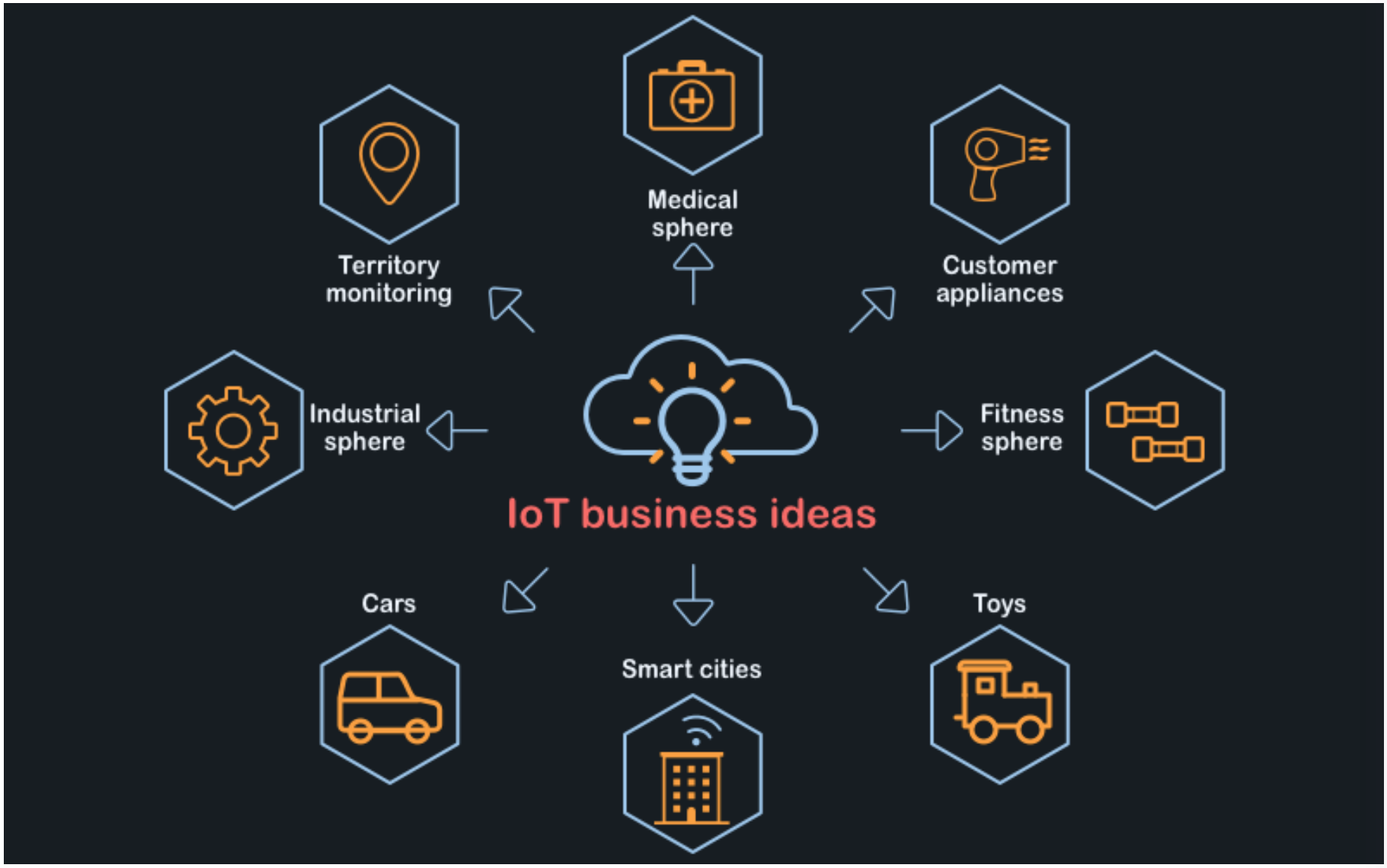
Internet of Things



Outline

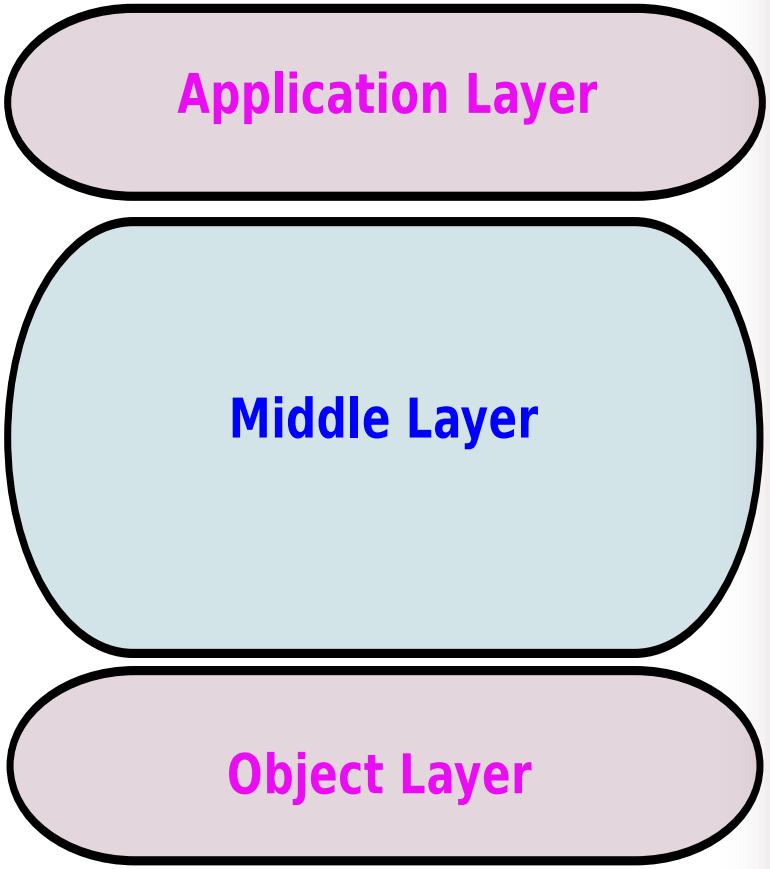
1. Introduction and Background.
2. Access Control Oriented (ACO) Architecture for Cloud-Enabled IoT
3. Access Control Models for VO Communication in ACO Architecture.
4. Access Control Model for VO Communication and Implementation in AWS IoT
5. Conclusion and Future Work

IoT Projects

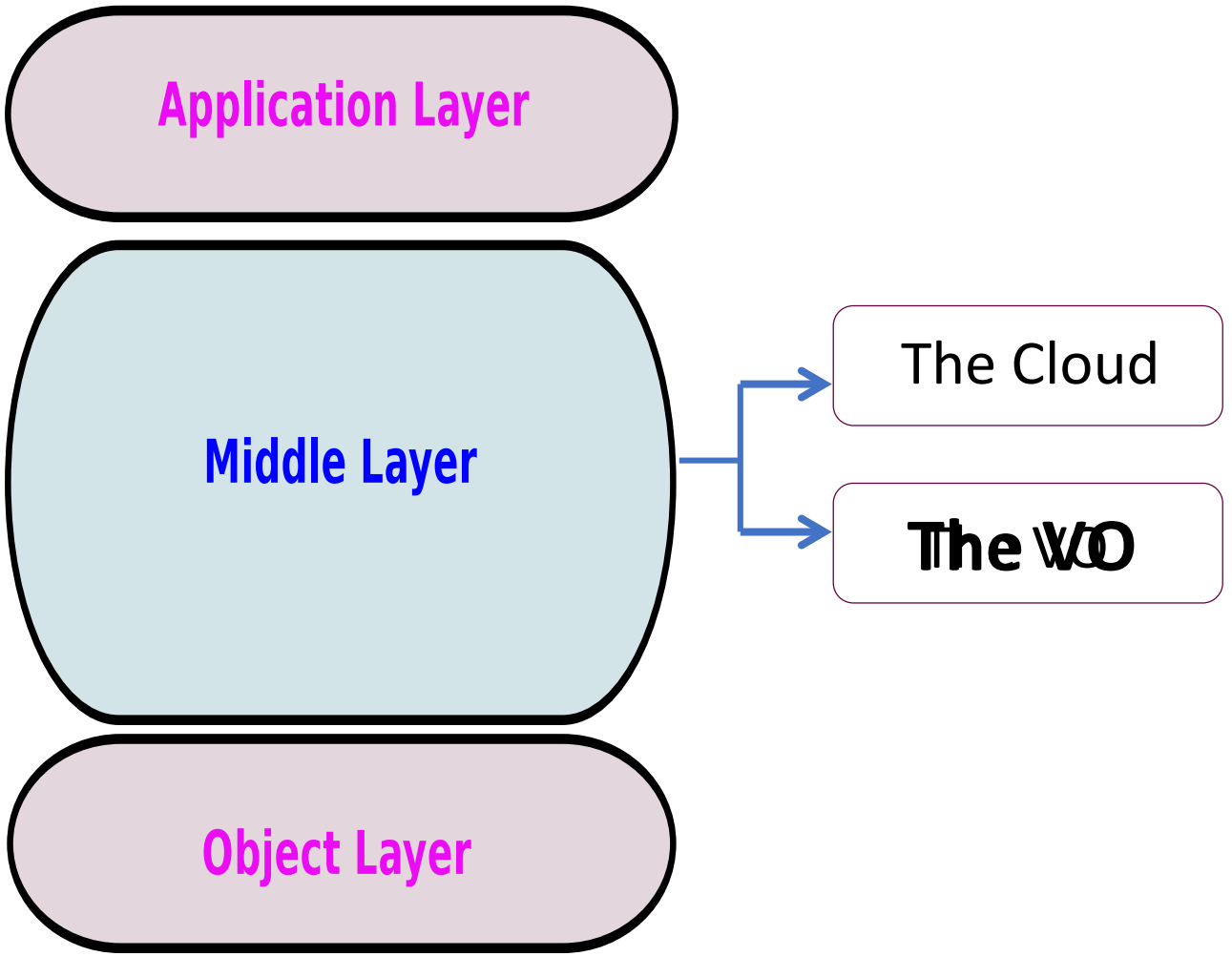


IoT Proposed Architectures

- Architecture:
  - ❖Integrating the Cloud
    - Unlimited computational capabilities
    - Low-cost
    - On-demand storage
    - Resources usable from everywhere
  - ❖Integrating Virtual objects
    - Solution for major IoT Issues
    - Homogeneous communication style
- IoT Security



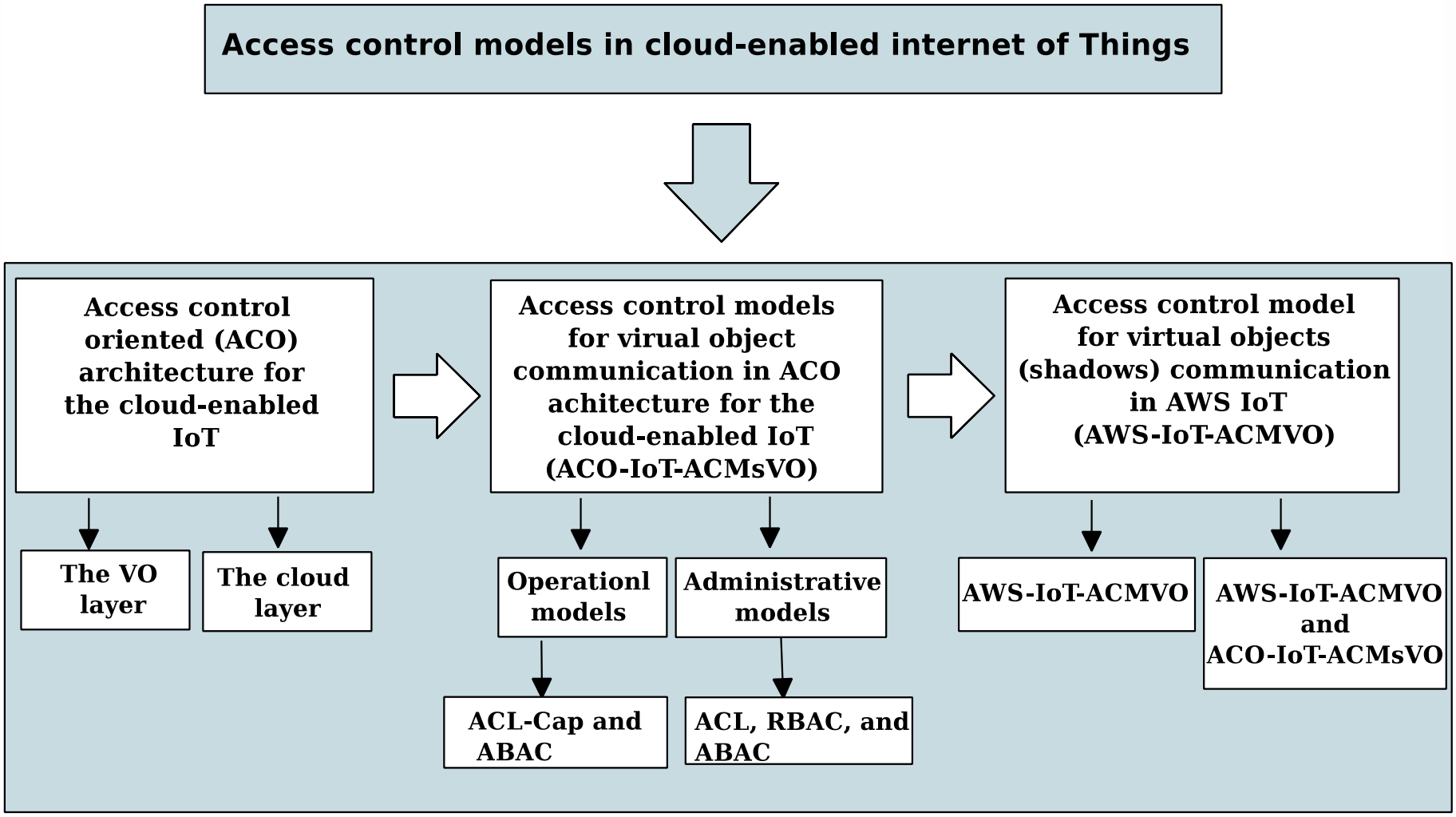
Problem Scope



Thesis Statement

- It is feasible to develop a set of access control models for virtual objects communication in cloud-enabled Internet of Things within the Access control Oriented (ACO) architecture by adapting traditional access control models, specifically, Cap-ACL, RBAC, ABAC and Policy-Based.

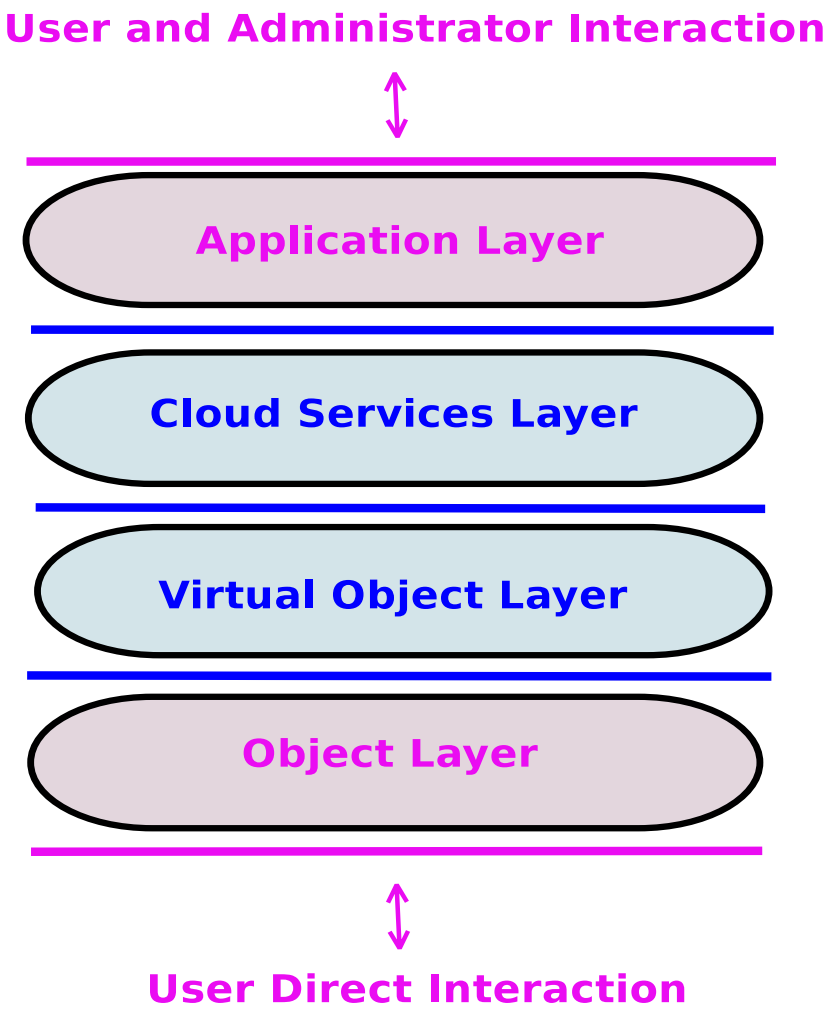
Summary of Contribution



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

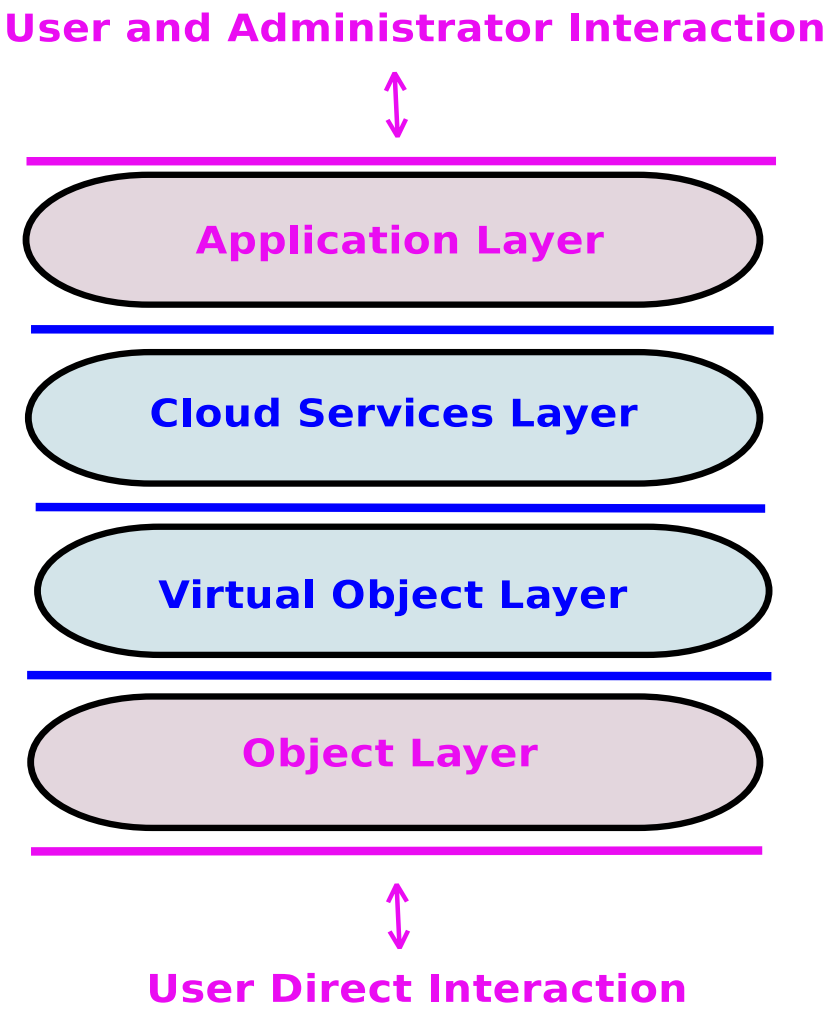
Access Control Oriented (ACO) Architecture for IoT

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

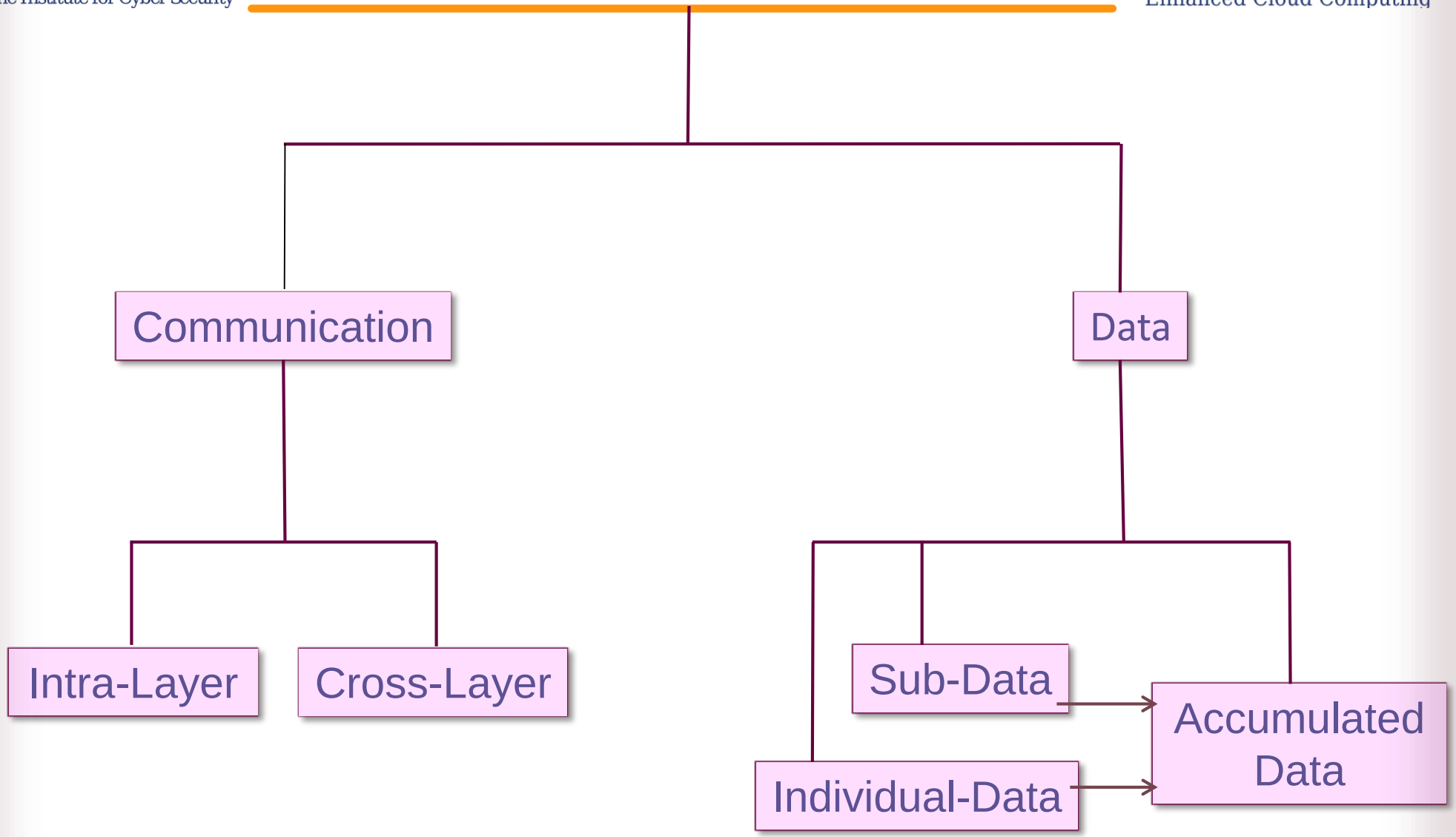


Access Control Oriented (ACO) Architecture for IoT

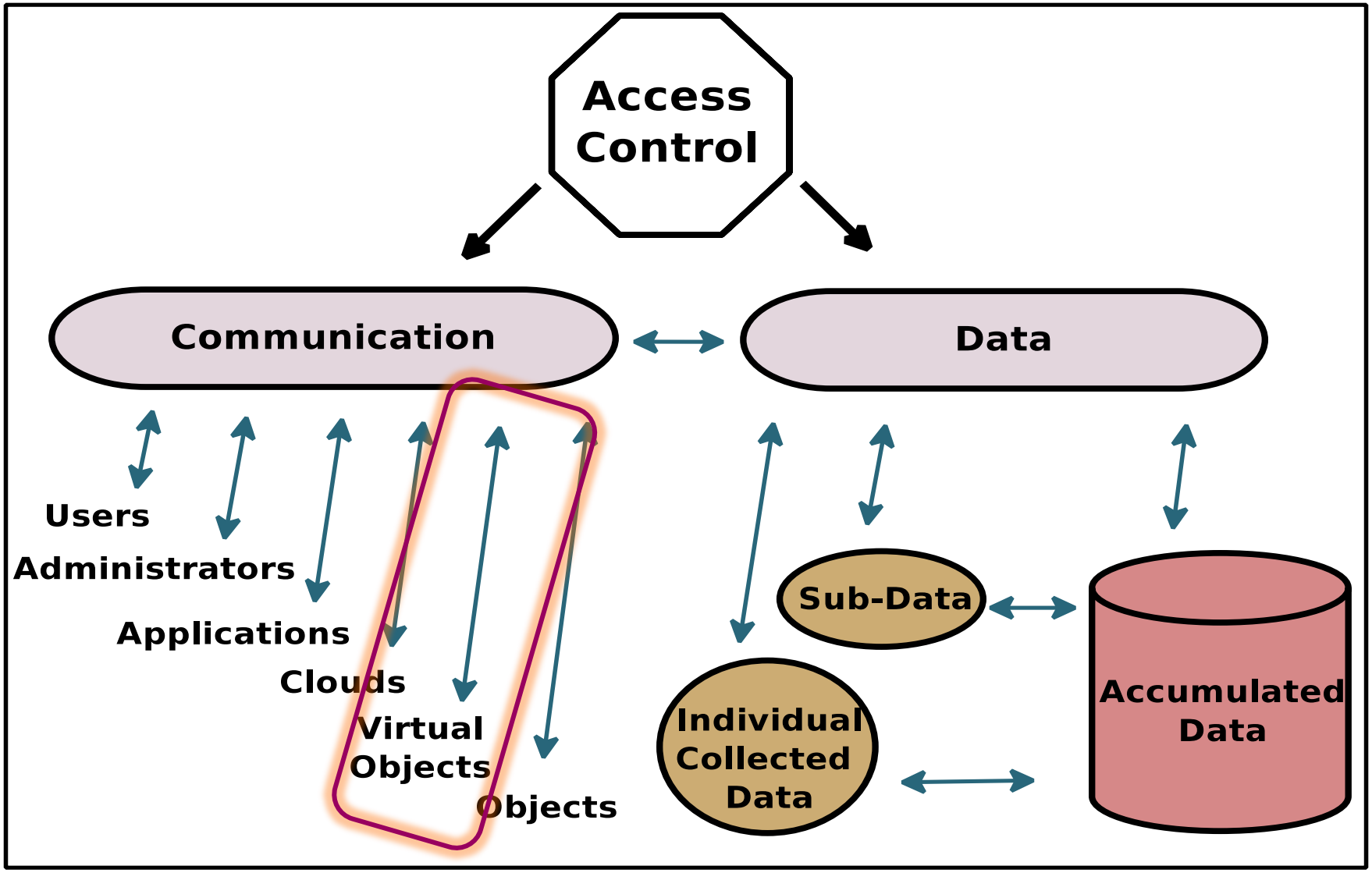
- **The Cloud Layer:**
  - Big data
  - Functionality
  - Communication
- **The Application Layer:**
  - Interface
  - Users and Admin
  - Generate AC policies



ACO Architecture for IoT

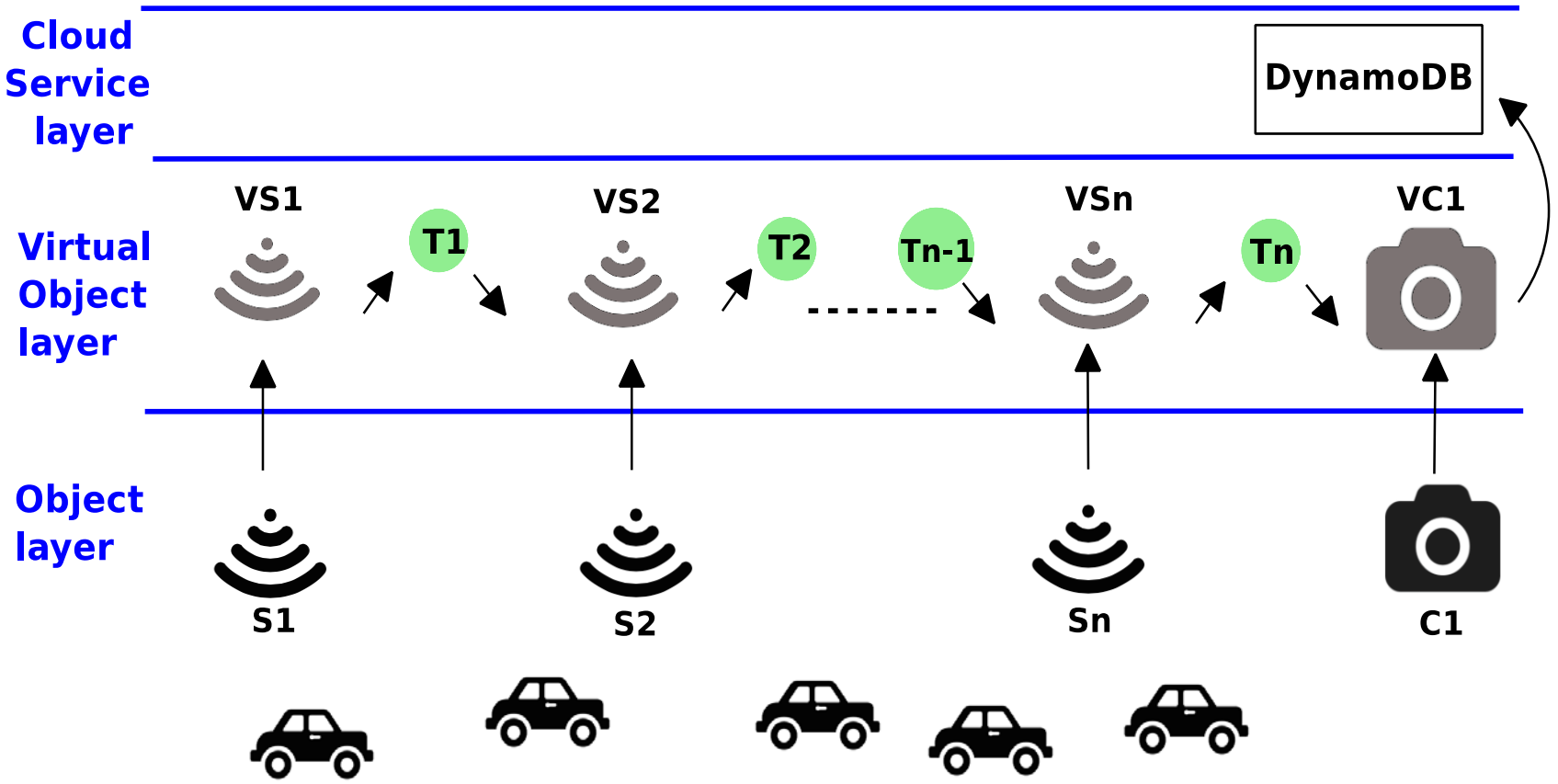


Access Control Issues in ACO Architecture for IoT



Access Control Models for VO Communications in ACO Architecture

Use Case within ACO



Access Control Models for VO Communication

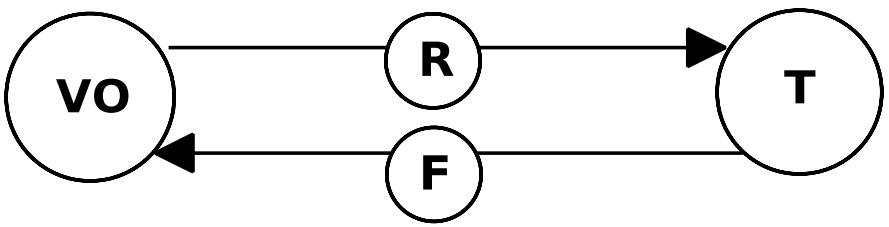
Develop access control models for VO communication in two layers:

- A - Operational models
- B - Administrative models

Operational Access Control for VO Communication

A. ACL and Capability Based (ACL-Cap) Operational Model

B. ABAC Operational Model



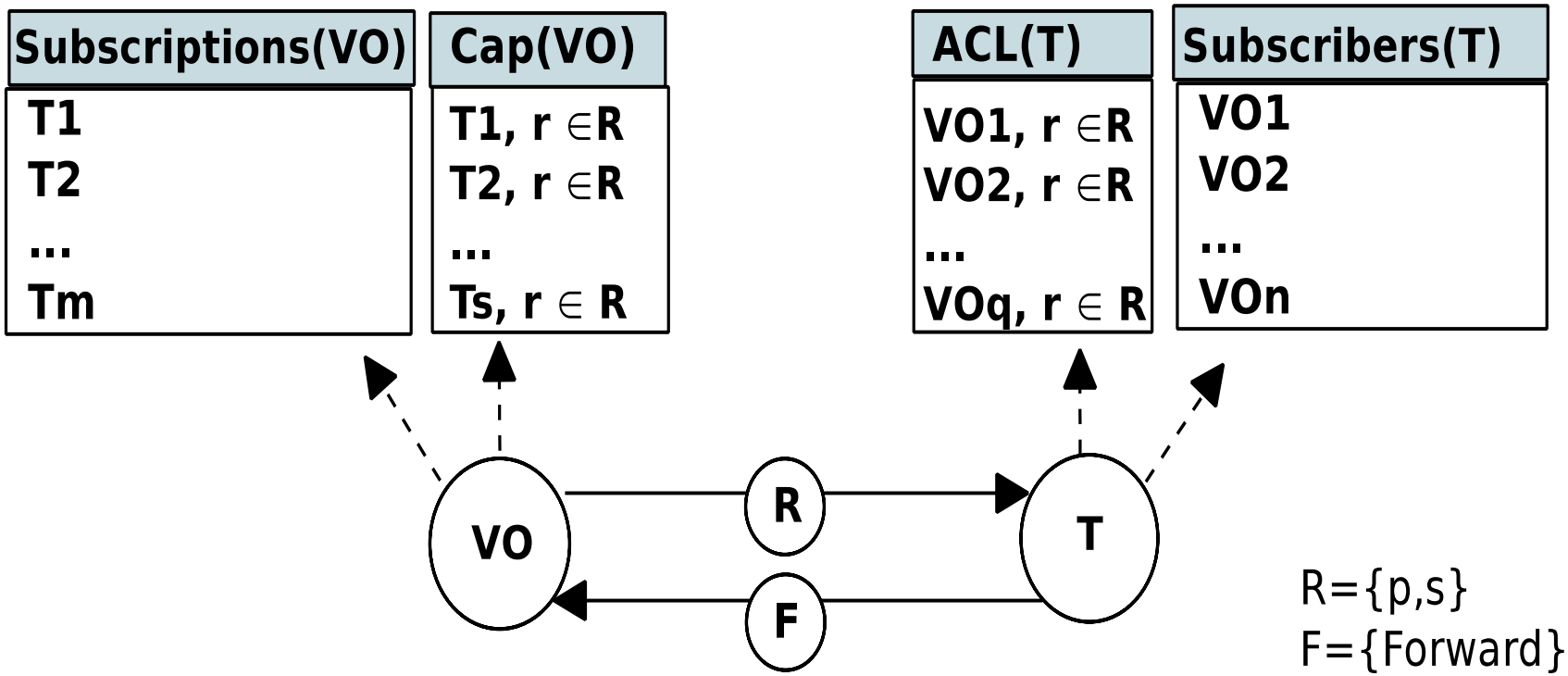
R={p,s}
F={Forward}

Four Questions:

- Which VOs are allowed to publish or send a subscription request to a topic?
- Which topics should VOs publish or send a subscription request to?
- Which VOs should a topics forward data to?
- Which topics should VOs receive data from?

A. ACL and Capability Based (ACL-Cap) Operational Model

- The operational models recognize sets of entities:
  - Virtual objects (VO) and topics (T)
  - A set of rights R={Publish, Subscribe}.
  - F={Forward}



A. ACL and Capability Based (ACL-Cap) Operational Model

- The authorization rule for publish is expressed as follows.

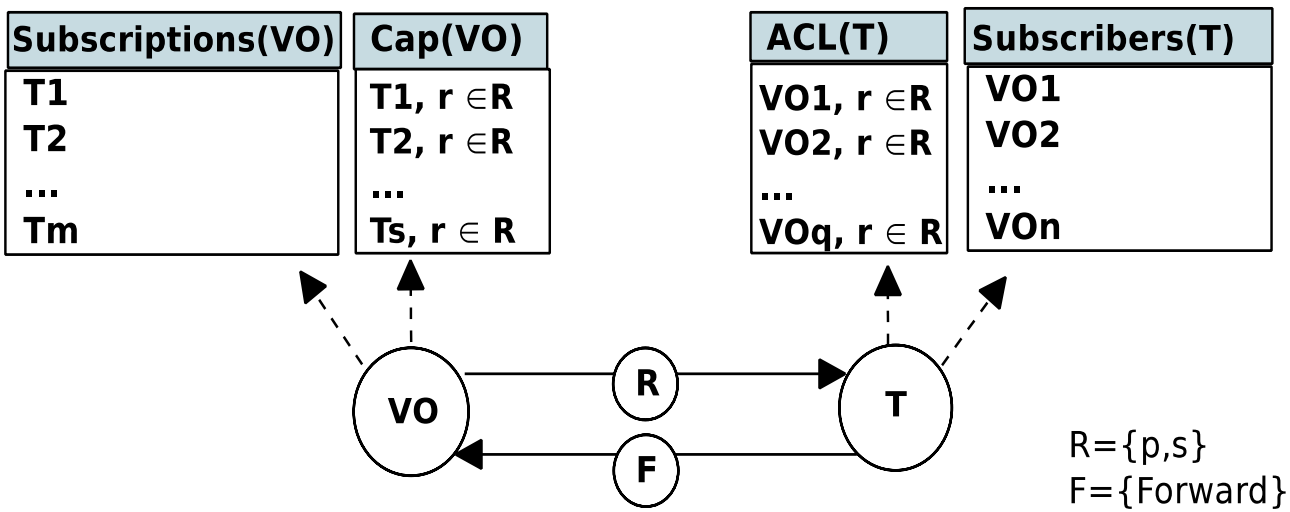
$$\text{Auth-Publish}(VO,T) \equiv (T,p) \in \text{Cap}(VO) \wedge (VO, p) \in \text{ACL}(T)$$

- The authorization rule for subscribe is expressed as follows.

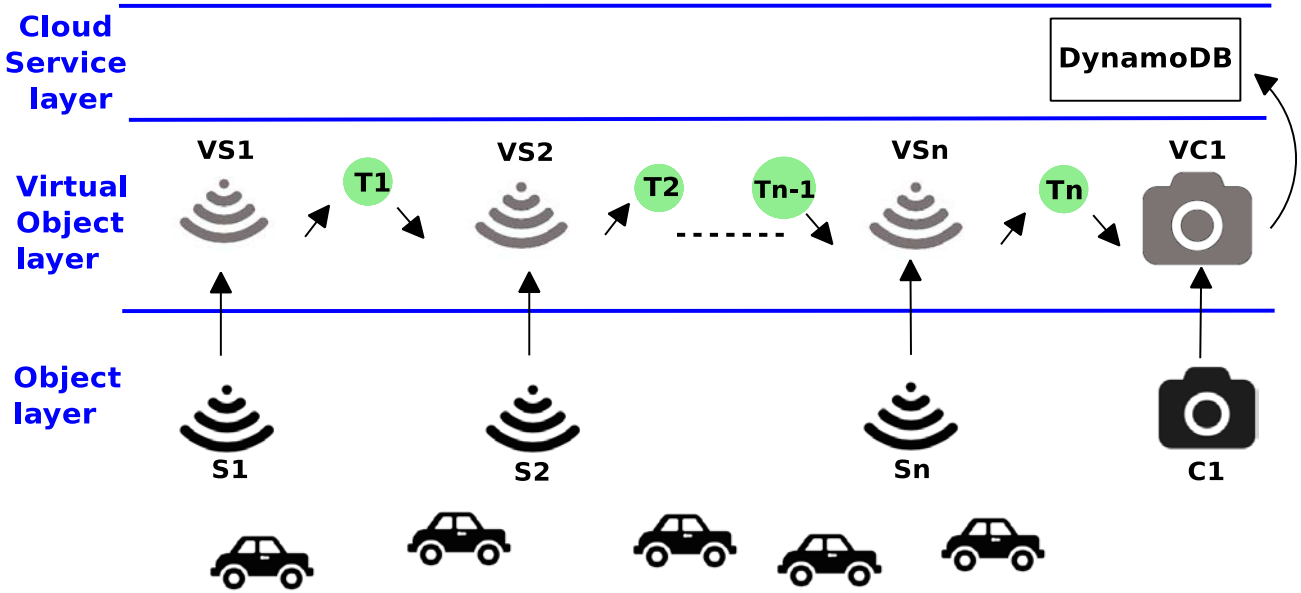
$$\text{Auth-Subscribe}(VO,T) \equiv (T,s) \in \text{Cap}(VO) \wedge (VO, s) \in \text{ACL}(T)$$

- The authorization rule for forwarding of published data by a topic's MB to a VO expressed as follows.

$$\text{Auth-Forward}(T, VO) \equiv VO \in \text{Subscribers}(T) \wedge T \in \text{Subscriptions}(VO)$$



A. ACL and Capability Based (ACL-Cap) Operational Model



ACL of T

$T1$	....	Tn-1	Tn
$VS1$, p	....	VSn-1, p	VSn, p
$VS2$, s	....	VSn, s	$VC1$, s

Cap of VO

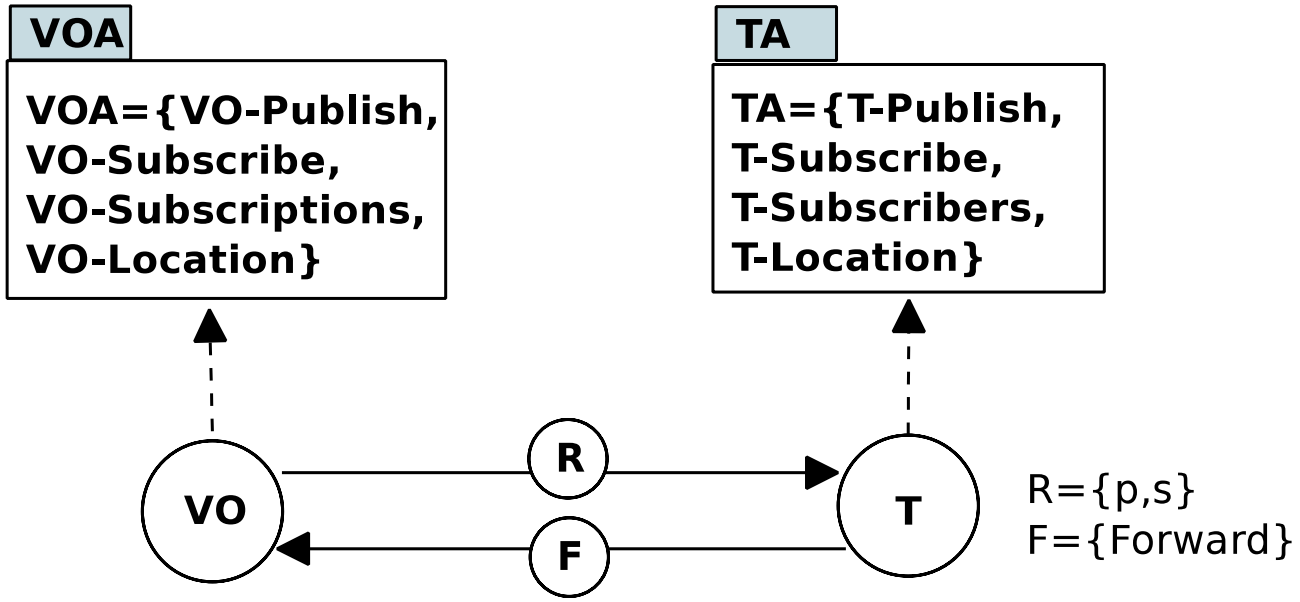
$VS1$	....	VSm	$VC1$
$T1$, p	....	Tn, p	Tn, s
	....	Tn-1, s	

B. ABAC Operational Model

- The operational models recognize sets of entities:
  - Virtual objects (VO) and topics (T)
  - A set of rights R={p,s} and F = {Forward}, as before
  - Sets of attributes, virtual object attributes (VOA) and topic attributes (TA) , as follows.

VOA = {VO-Publish, VO-Subscribe, VO-Subscriptions, VO-Location}

TA= {T-Publish, T-Subscribe, T-Subscribers, T-Location}



B. ABAC Operational Model

- The authorization rule for publish is expressed as follows.

$$\text{Auth-Publish}(VO,T) \equiv T \in \text{VO-Publish}(VO) \wedge VO \in \text{T-Publish}(T)$$

- The authorization rule for subscribe is expressed as follows.

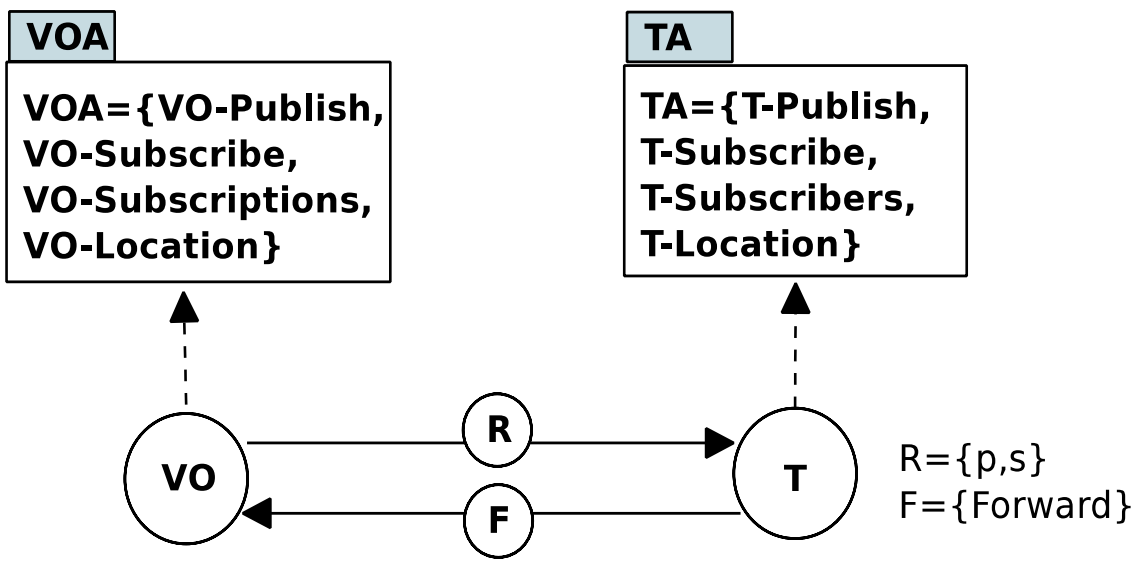
$$\text{Auth-Subscribe}(VO,T) \equiv T \in \text{VO-Subscribe}(VO) \wedge VO \in \text{T-Subscribe}(T)$$

- The authorization rule for forward published data is expressed as follows.

$$\text{Auth-Forward}(T, VO) \equiv T \in \text{VO-Subscriptions}(VO) \wedge VO \in \text{T-Subscribers}(T)$$

- We can conjunctively add the following condition to each of the three equations above.

$$\text{T-Location}(T) \approx \text{VO-Location}(VO)$$



Administrative Access Control for VO Communication

- Admins mean users who are authorized to control VO communication, by adjusting configuration of the operational model.
  - Administrative ACL Model
  - Administrative RBAC Model
  - Administrative ABAC Model

- For the ACL-Cap operational model:
  - Who is allowed to add or delete (VO,p) or (VO,s) from ACL of T?
  - Who is allowed to add or delete (T,p) or (T,s) from Capability list of VO?

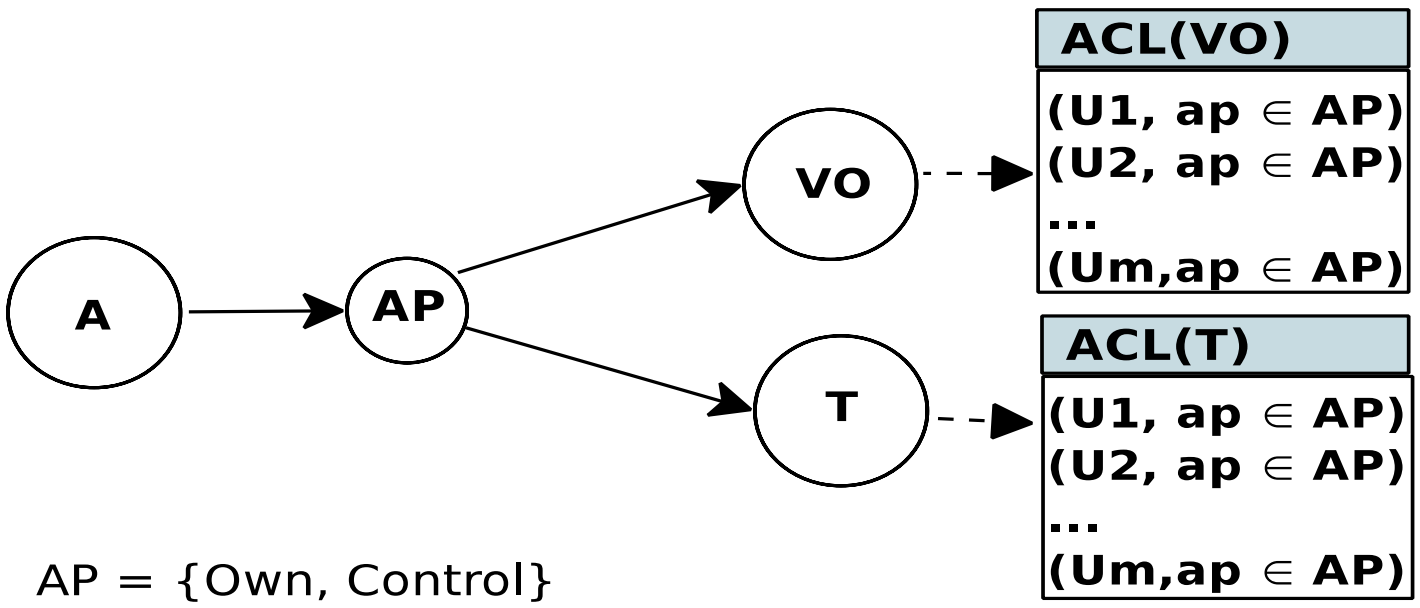
- For the ABAC operational model:
  - Who is allowed to assign or delete values to or from attributes of T?
  - Who is allowed to assign or delete values to or from attributes of VO?

A. Administrative ACL Model

- The administrative ACL model introduces a set of admin users (A) and admin permissions (AP) as follows.

$$A = \{U1, .., Um\text{-}1, Um\}$$

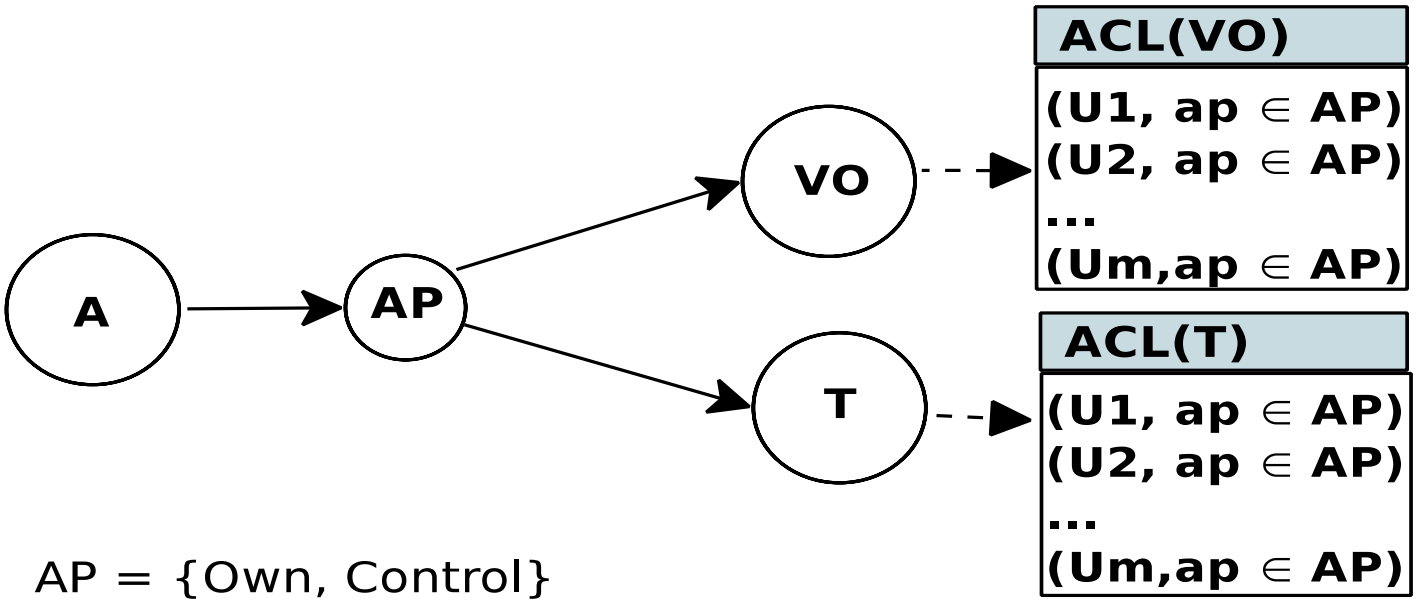
$$AP = \{Own, Control\}$$



A. Administrative ACL Model

- The authorization rule for admin user U to control T or VO as follow.

$$\text{Auth-Control}(U,T) \equiv (U,ap) \in ACL(T)$$
$$\text{Auth-Control}(U,VO) \equiv (U,ap) \in ACL(VO)$$



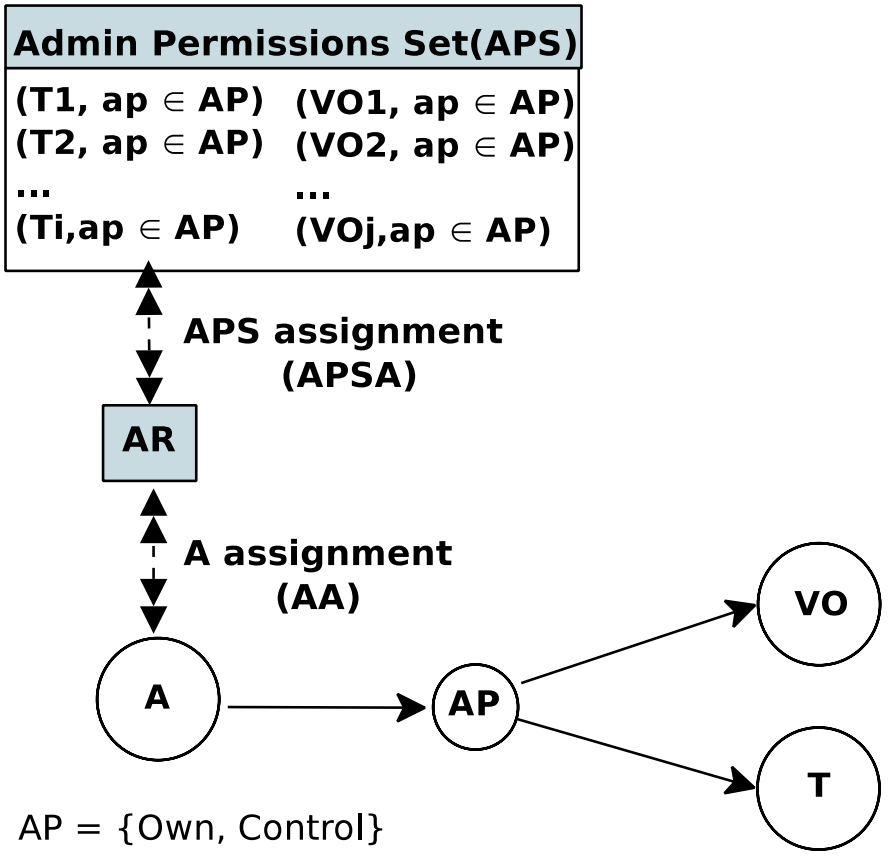
- Difficult to maintain

B. Administrative RBAC Model

- Additionally, RBAC introduces set of administrative roles (AR) and admin permissions set(APS) as follows.

  AR = {AR1, .., ARs},

  APS ={(VO×AP)∪ (T×AP)}, A set of VO-AP and T-AP pairs.



- Easier to maintain

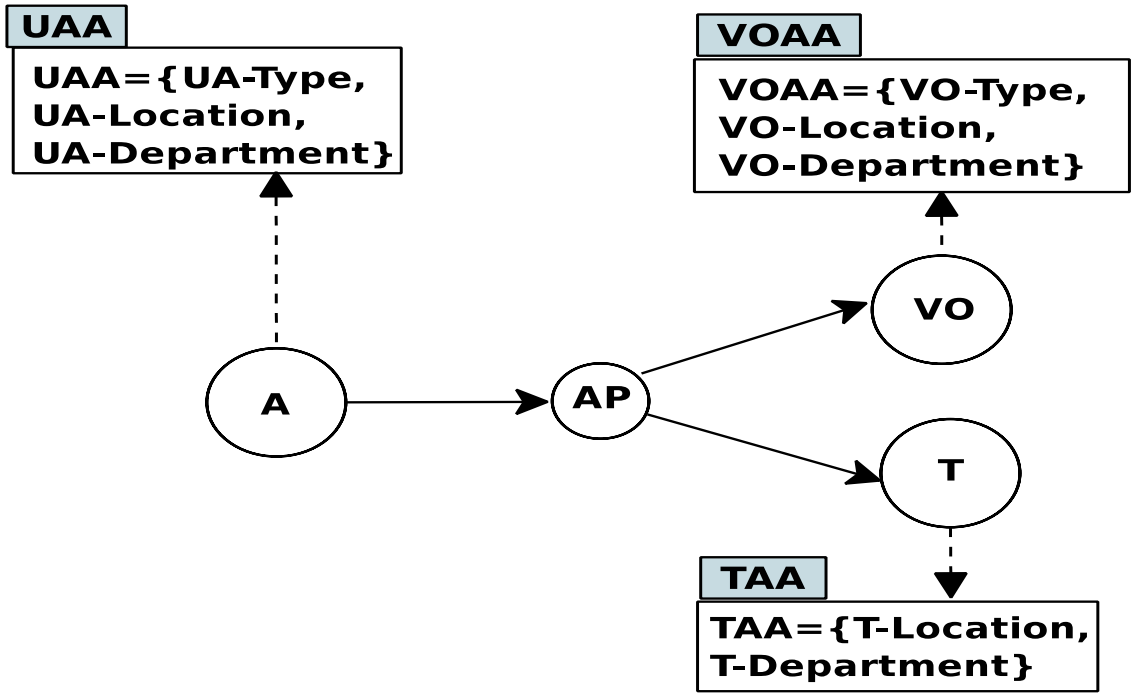
C. Administrative ABAC Model

- Additionally, ABAC introduces administrative attributes for topics (TAA), VOs (VOAA), and users (UAA), as follows.

TAA = {T-Location, T-Department}

VOAA = {VO-Type, VO-Location, VO-Department}

UAA = {UA-Type, UA-Location, UA-Department}



C. Administrative ABAC Model

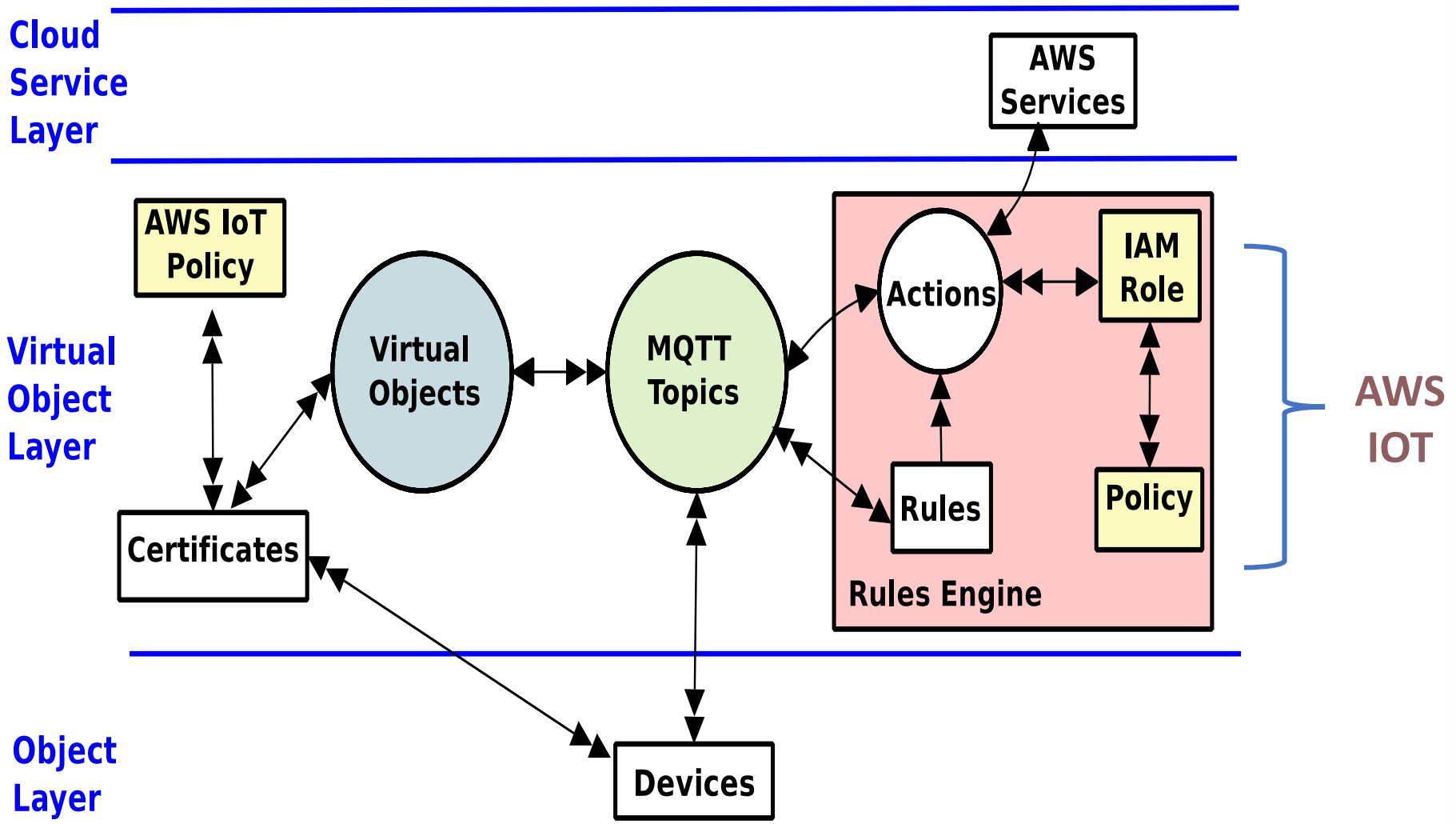
- Authorize users who have own or control permission to control sensors and cameras from the same department and close location

$$\text{Auth-Control}(U,VO) \equiv$$
$$(\text{UA-Type}(U) = \text{Own} \vee \text{UA-Type}(U) = \text{Control}) \wedge$$
$$\text{UA-Department}(U) = \text{VO-Department}(VO) \wedge$$
$$(\text{VO-type} = \text{sensor} \vee \text{VO-type} = \text{camera}) \wedge$$
$$\text{UA-location} \approx \text{VO-Location}(VO)$$

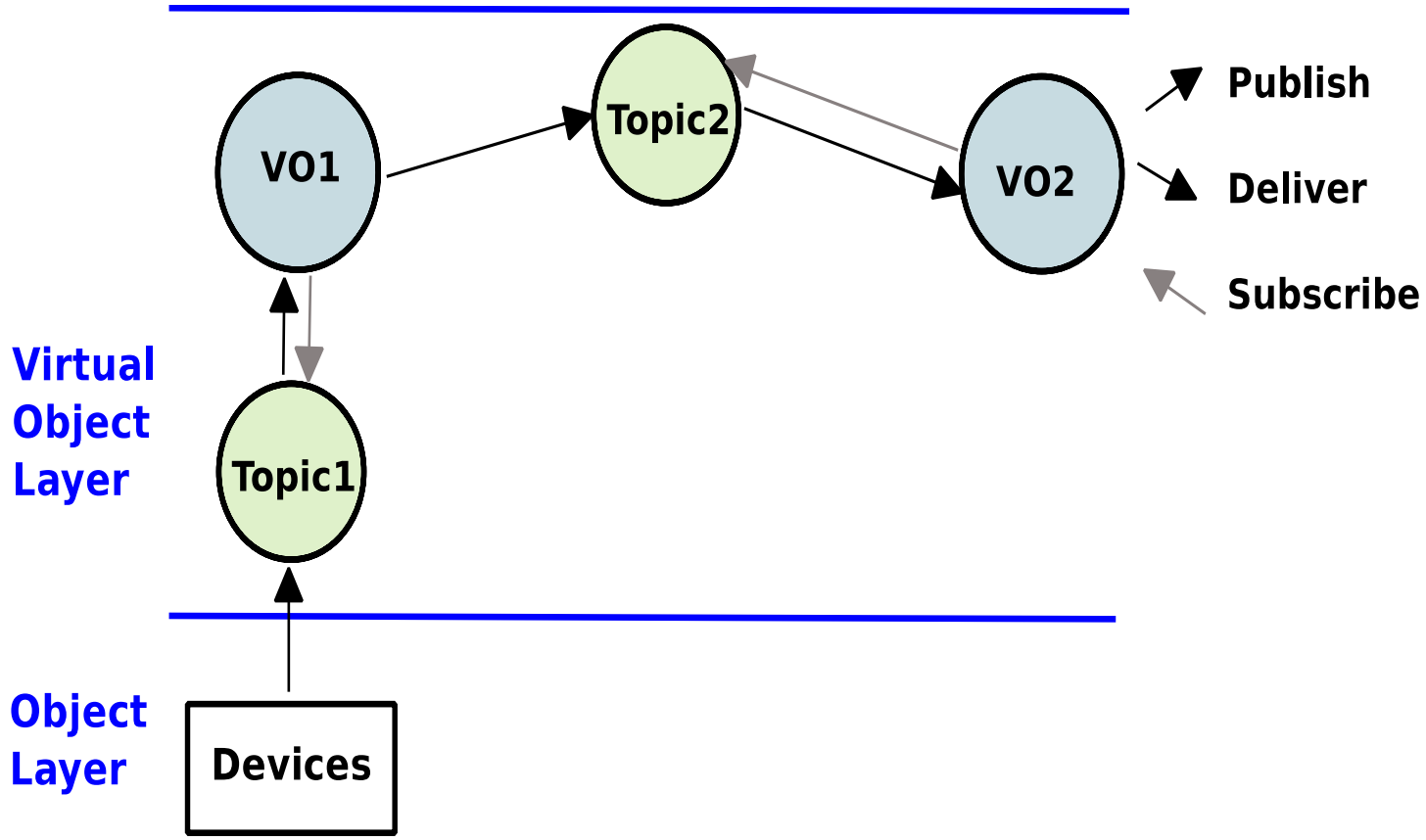
- Flexible, scalable, and adaptable:
  - Identity, roles, and resource information of ACL and RBAC into attributes
  - incorporating collected data for making a decision

Access Control Models for VO Communication and Implementation in AWS IoT

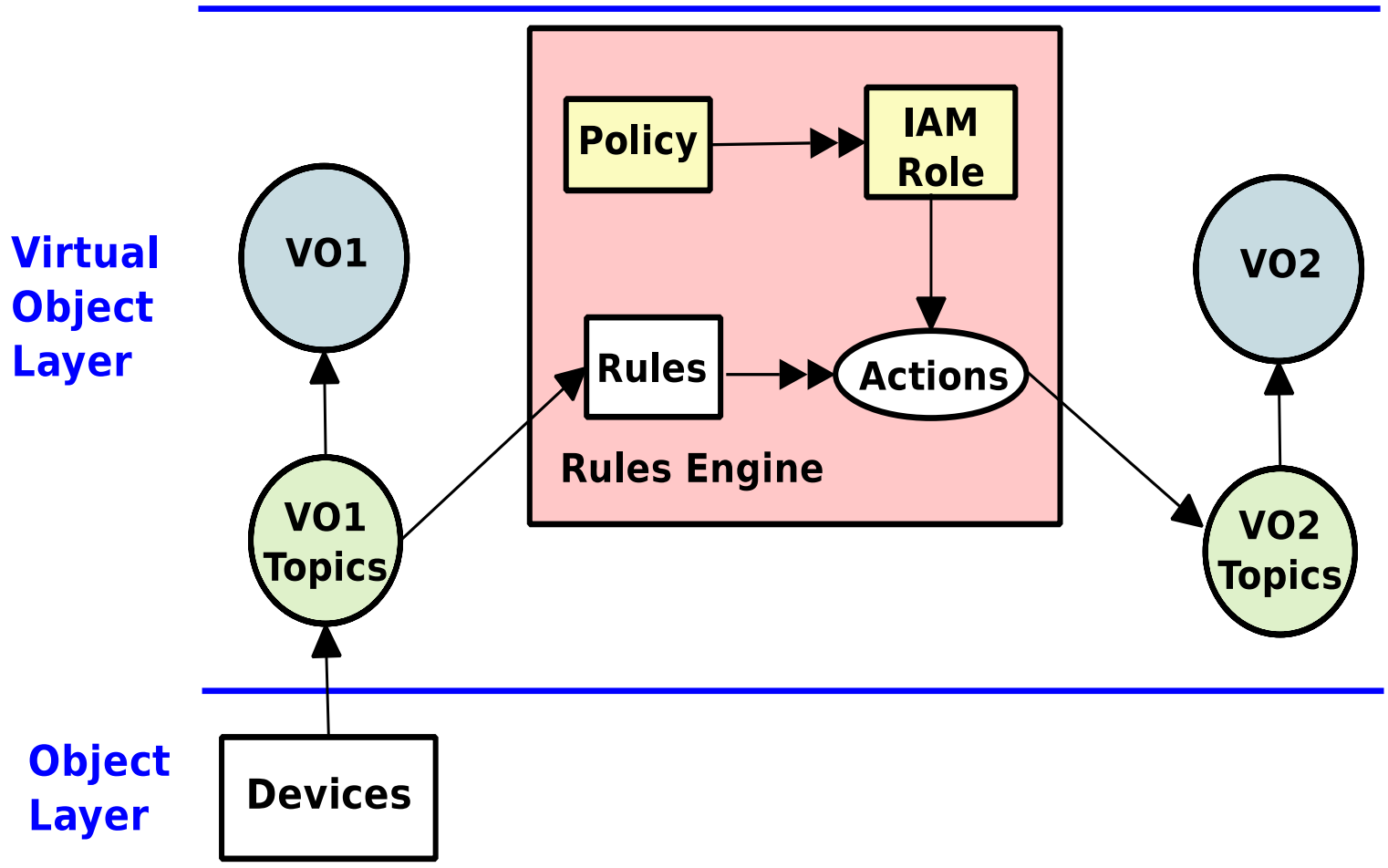
The AWS-IoT-ACMVO Model for AWS IoT



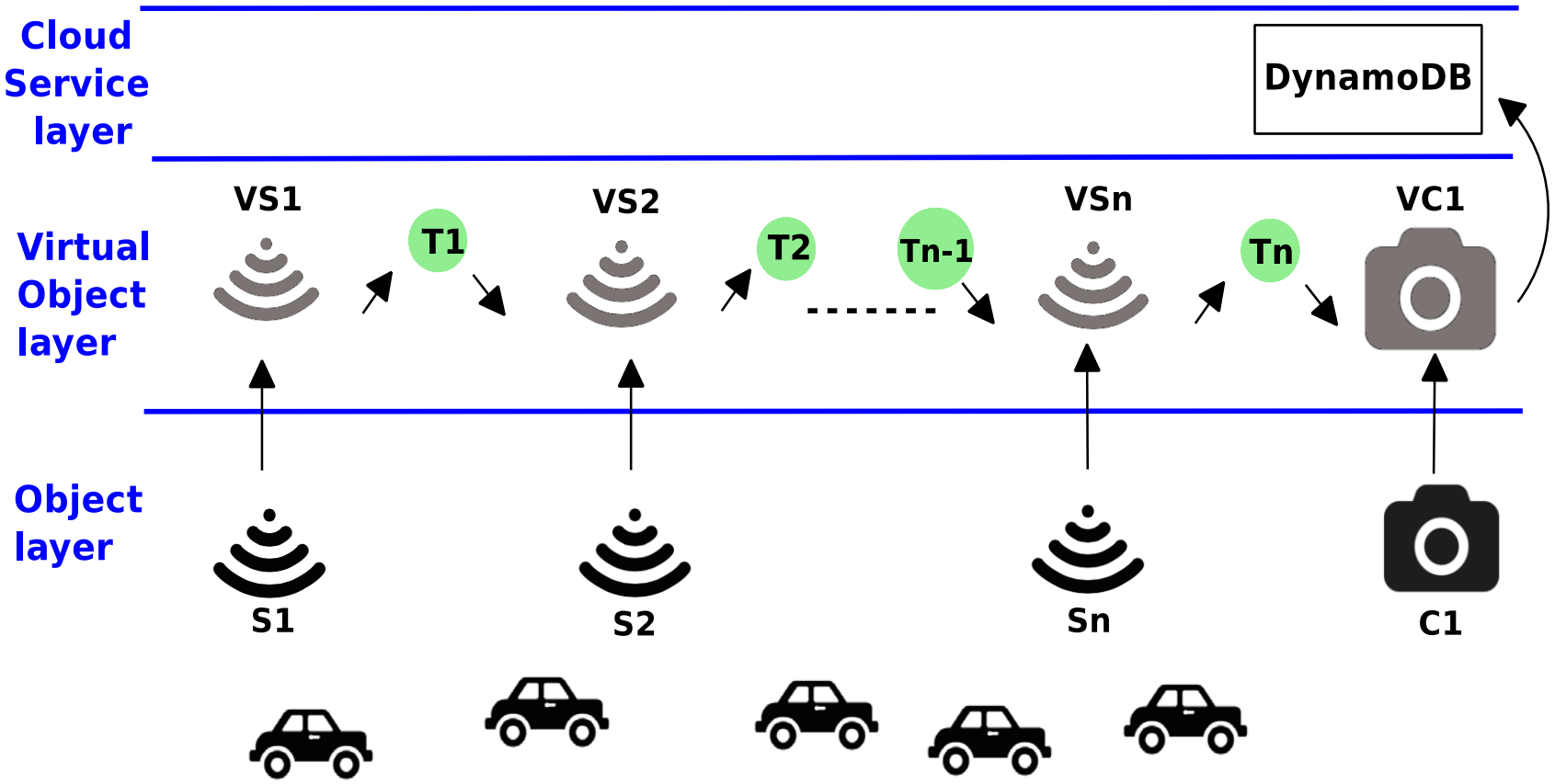
The Publish/Subscribe Topic-Based Scheme



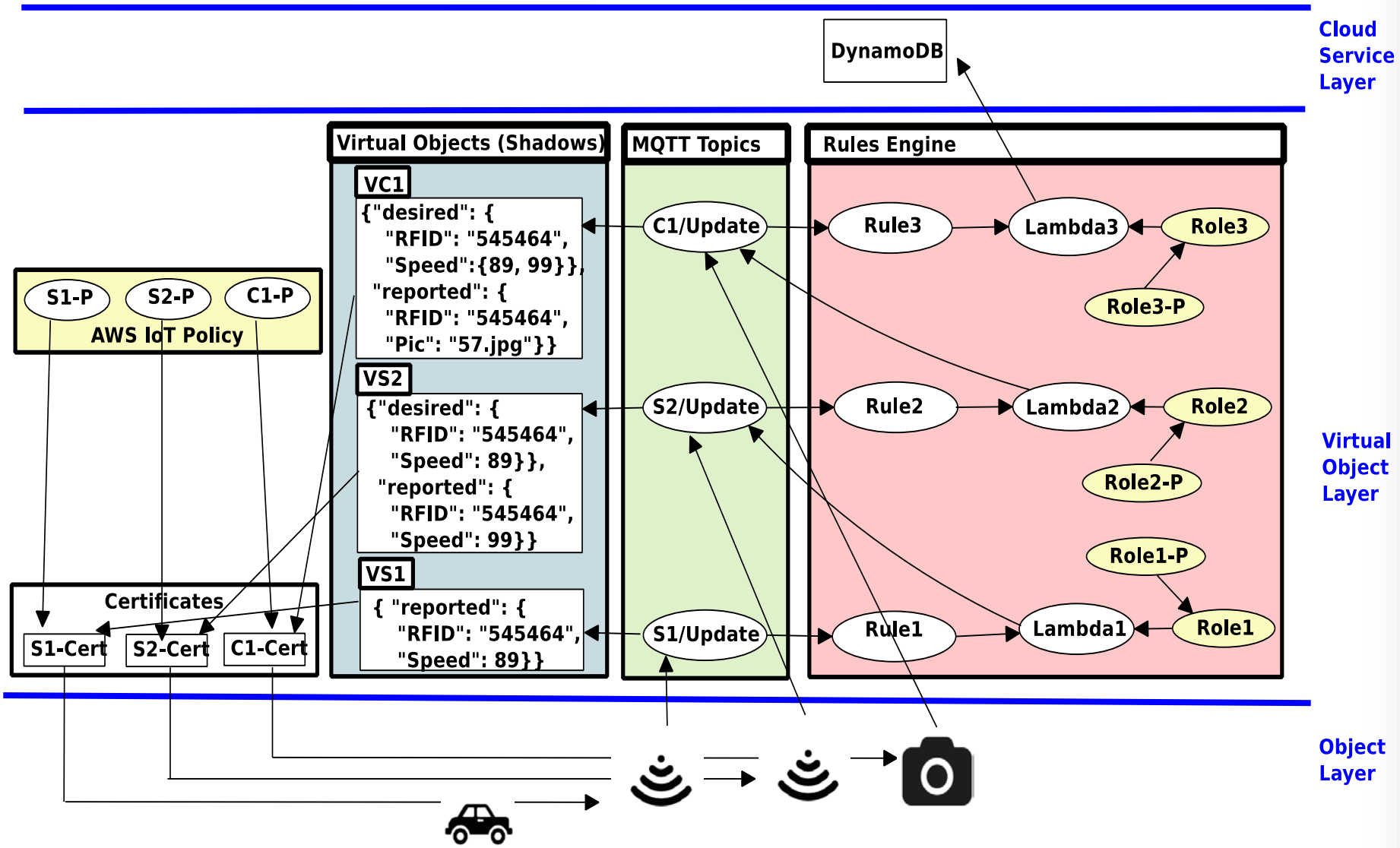
Communication Channel in AWS IoT



The Sensing Speeding Cars Use Case



Sensing the Speed of One Car with two sensors



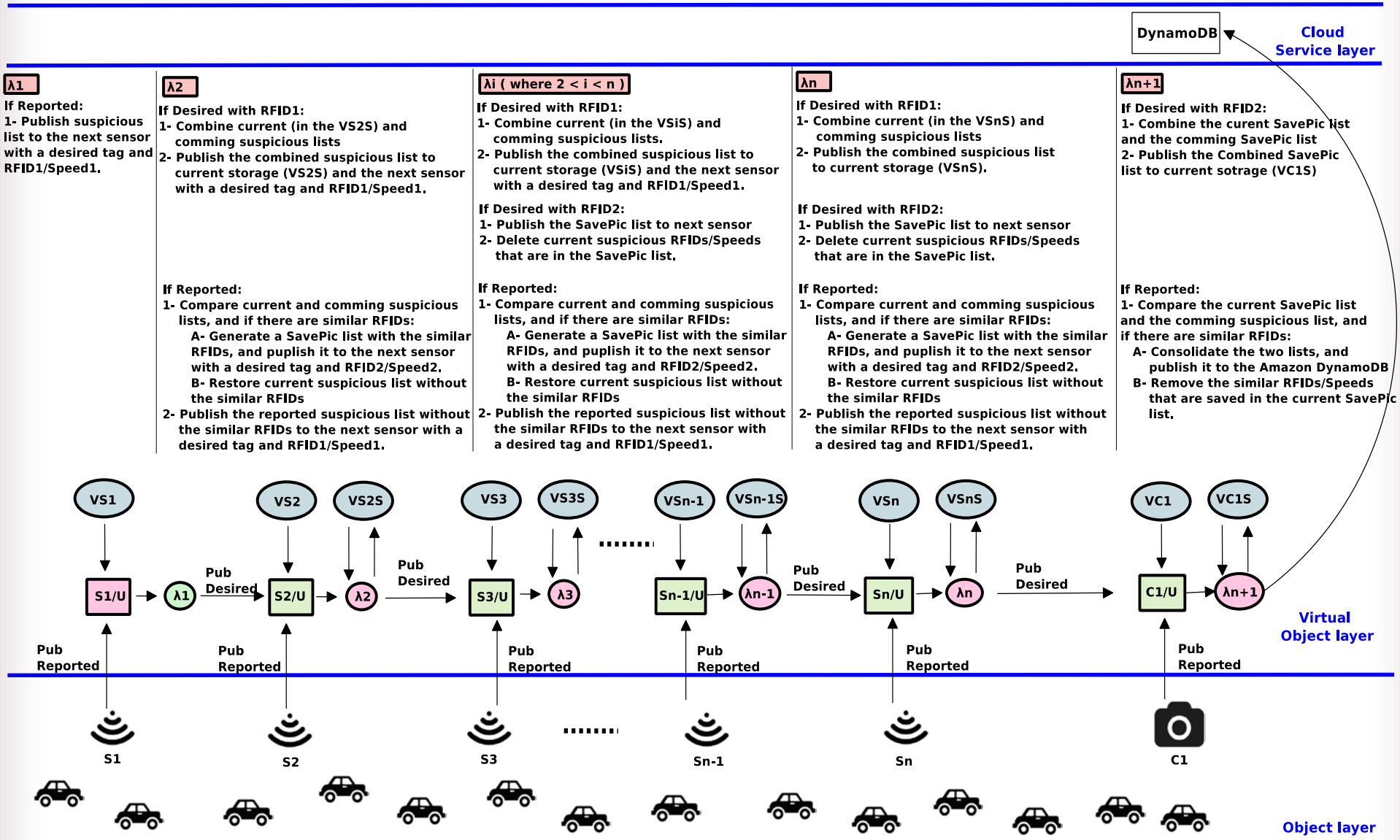
Role2 Policy that is Attached to Role2


```
{
   "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"
      }
   ]
}
```

Sensing the Speed of Multiple Cars with Multiple sensors

I·C·S The Institute for Cyber Security

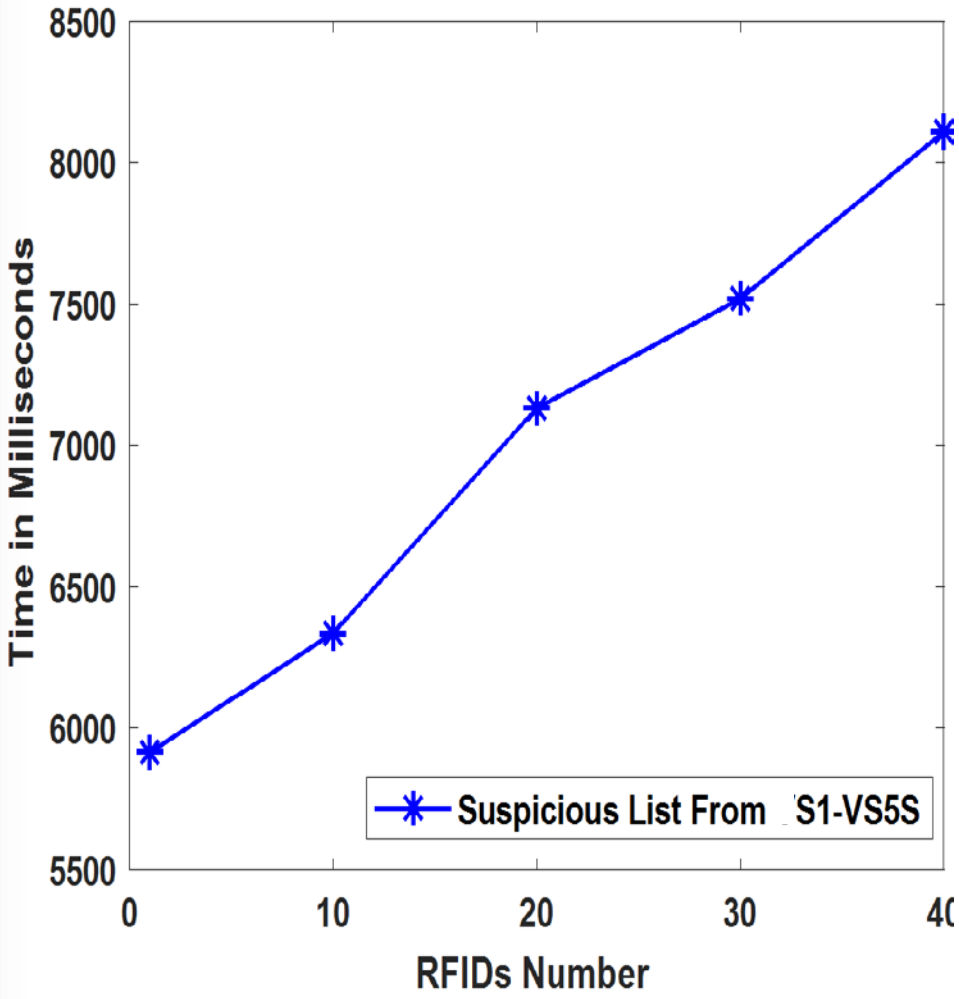
C·SPECC Center for Security and Privacy Enhanced Cloud Computing

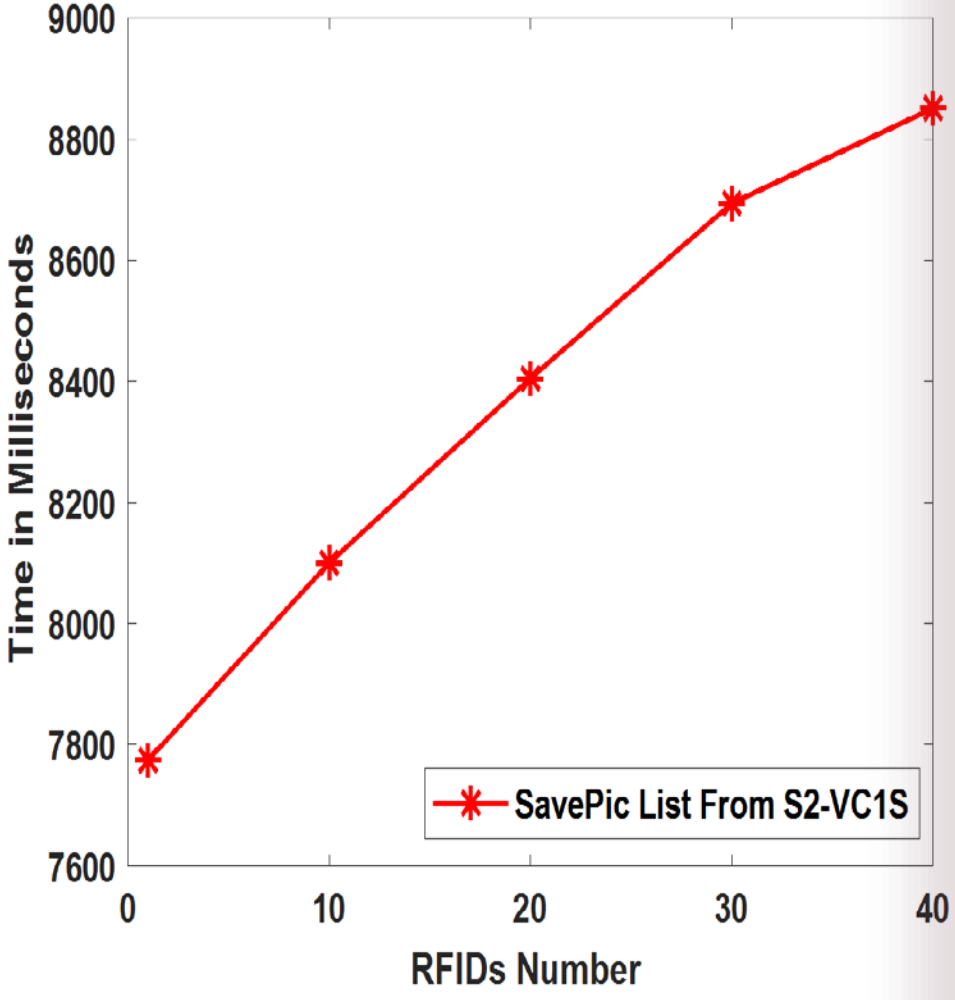


World-Leading Research with Real-World Impact!

UTSA Computer Science

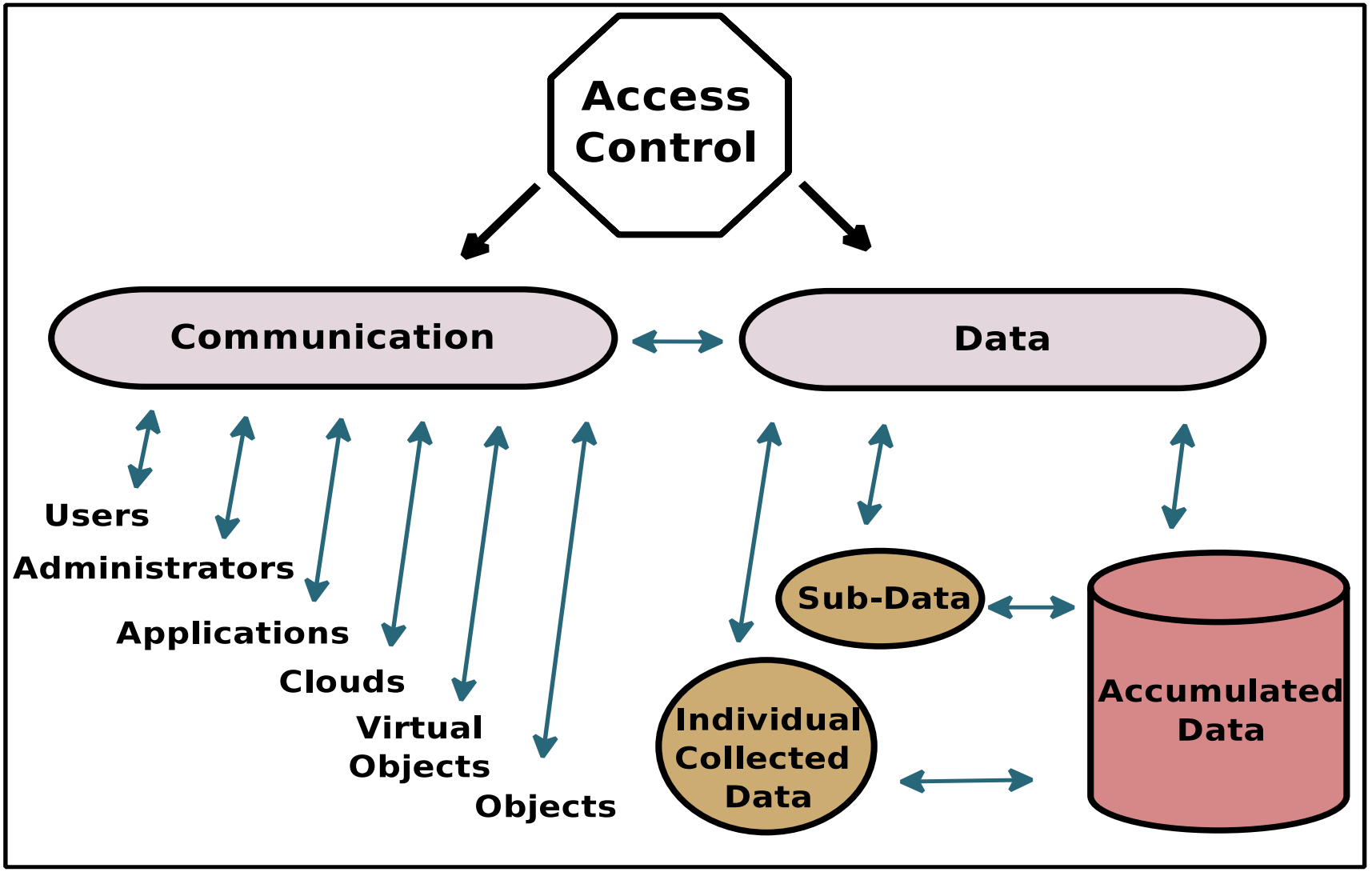
Performance





Conclusion and Future Work

Future Work



Conclusion

1. ACO Architecture for Cloud-Enabled IoT
   - ❖ Integrating the Cloud
   - ❖ Integrating virtual object
2. Access Control Models for VO Communications within ACO
   - ❖ Operational models
   - ❖ Administrative models
3. Access Control Models for VO Communications in AWS IoT

Publications

Dissertation published papers:

- 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 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, James Benson, Farhan Patwa, and Ravi Sandhu. Access control model for virtual objects (shadows) communication for aws internet of things. In Proceedings of the Eighth ACM on Conference on Data and Application Security and Privacy. ACM, 2018.

Other published papers:

- Asma Alshehri and Ravi Sandhu. On the relationship between finite domain ABAM and PreUCON_A. In International Conference on Network and System Security, pages 333–346, 2016.

Questions