Access Control Models for Virtual Object Communication in Cloud-Enabled IoT

Asma Alshehri and Ravi Sandhu
Institute for Cyber Security &
Department of Computer Science at UTSA

18th IEEE Conference on Information Reuse and Integration (IRI)
San Diego, California
August 4, 2017

nmt366@my.utsa.edu,
ravi.sandhu@utsa.edu

www.ics.utsa.edu

INTERNET OF THINGS

GOAL

❖ Develop an initial set of access control models for IoT within a robust framework.

ACCESS CONTROL ORIENTED (ACO) ARCHITECTURE FOR IOT

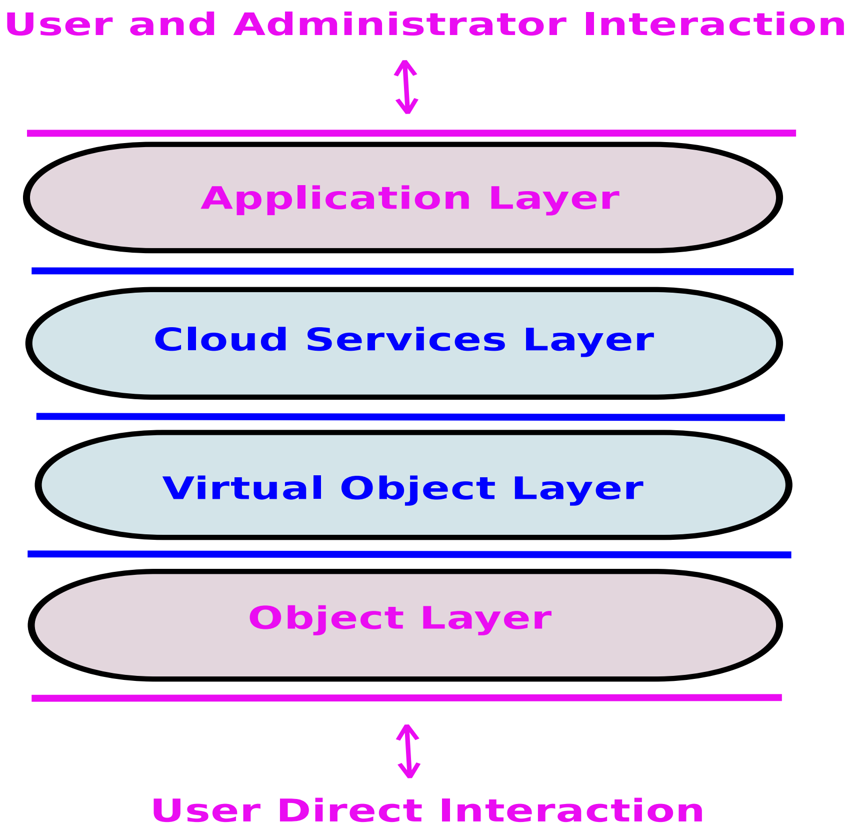


Figure 1. ACO Architecture for Cloud-Enabled IoT

[1] A. Alshehri and R. 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). IEEE, 2016, pp. 530–538.

THE PAPER GOAL

* Develop access control models for VO communication in two layers:

A - Operational models

B - Administrative models

OUTLINE

- Background
- Use case within ACO architecture
- Operational access control for VO communication
- Administrative access control for VO communication
- Current and future research
- Conclusion

BACKGROUND

- Access control models for IoT.
- The publish and subscribe communication paradigm

* The publish/subscribe paradigm has various implementation, primarily topic-based and content-based.

USE CASE WITHIN ACO ARCHITECTURE

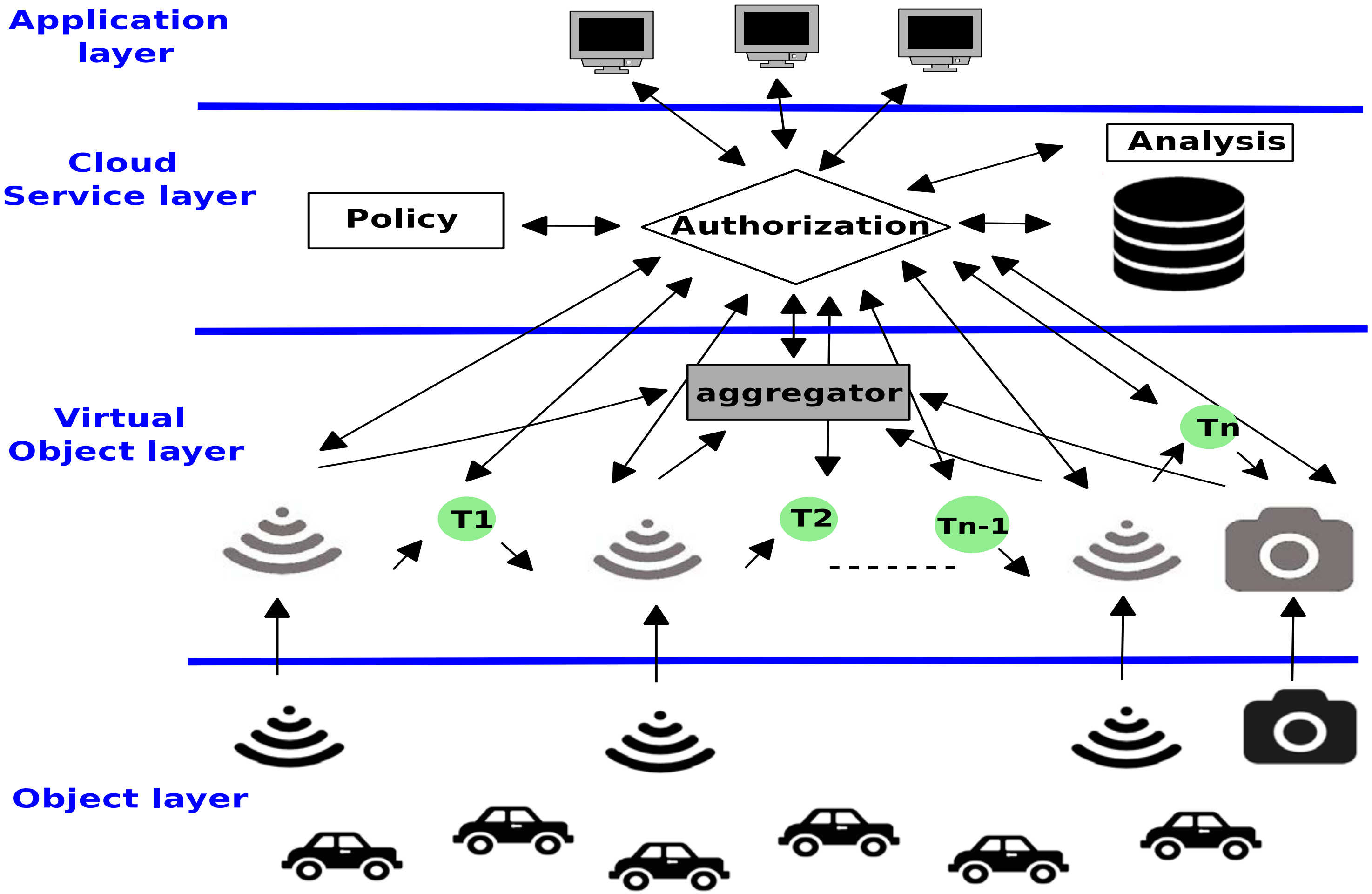
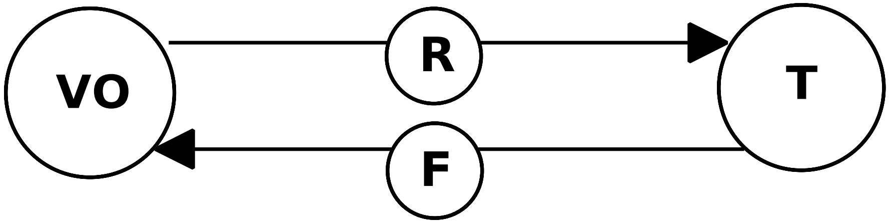


Figure 2. Sensing speeding cars within ACO Architecture

OPERATIONAL ACCESS CONTROL FOR VO COMMUNICATION

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

B. ABAC Operational Model



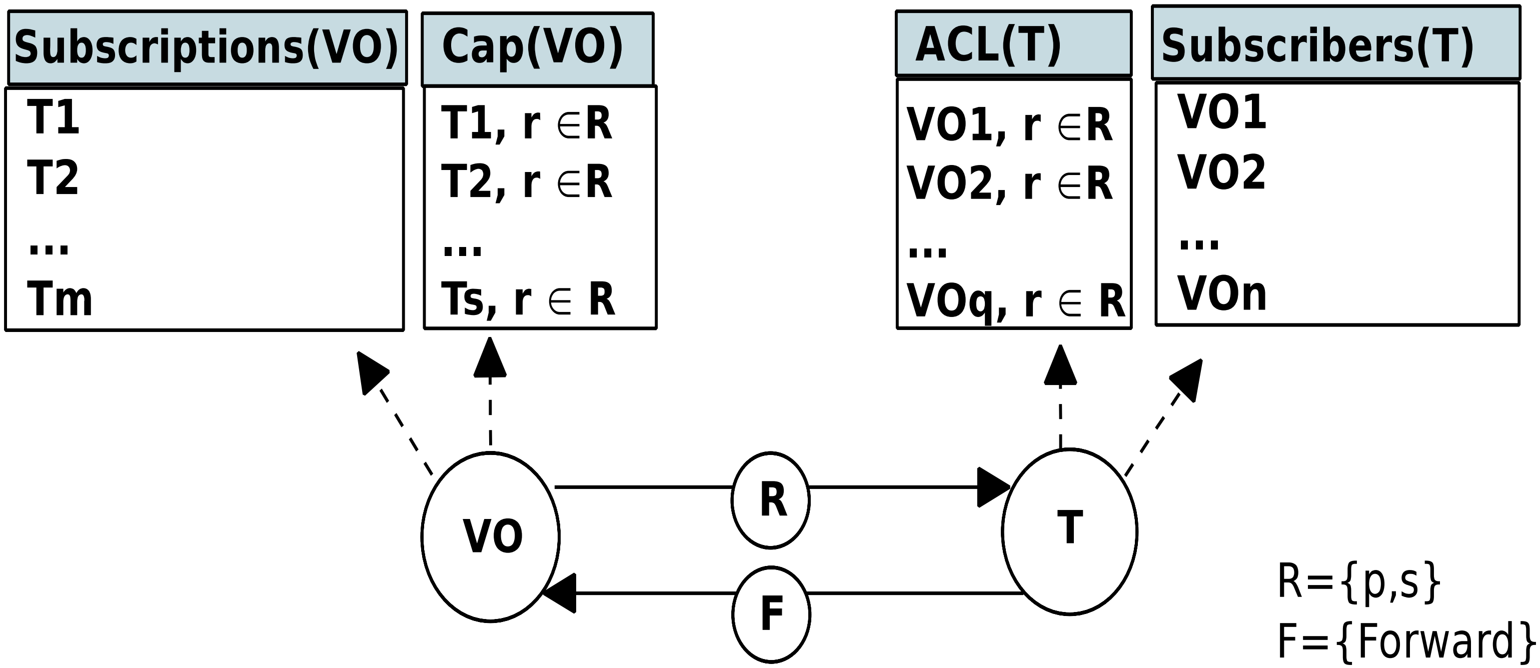
R={p,s}
F={Forward}

Four Questions:

- Which VOs are allowed to publish or send a subscription request to a topic's MB?
- Which MBs should VOs publish to or send a subscription request to?
- Which VOs should a topics MB forward data to?
- Which MBs 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={p,s}.
  - F={Forward}



Subscriptions(VO)
T1
T2
…
Tm

Cap(VO)
T1, r ∈R
T2, r ∈R
…
Ts, r ∈ R

ACL(T)
VO1, r ∈R
VO2, r ∈R
…
VOq, r ∈ R

Subscribers(T)
VO1
VO2
…
VOn

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

Figure 3. The ACL-Cap Model

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

- The authorization rule for publish is expressed as follows.

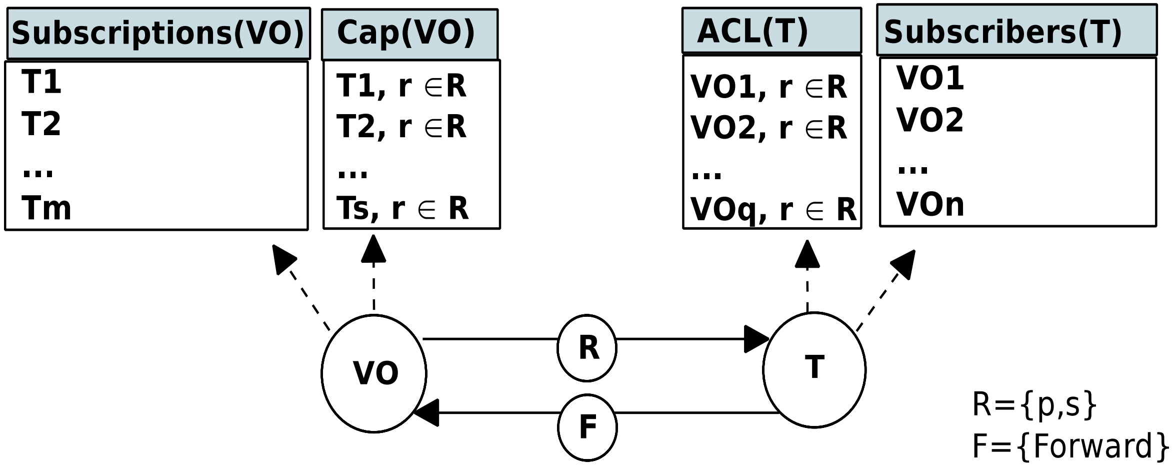
$$\textit{Auth-Publish}(VO,T) \equiv (T,p) \in Cap(VO) \land (VO, p) \in ACL(T)$$

- The authorization rule for subscribe is expressed as follows.

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

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

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



Subscriptions(VO)
T1
T2
…
Tm

Cap(VO)
T1, r ∈R
T2, r ∈R
…
Ts, r ∈ R

ACL(T)
VO1, r ∈R
VO2, r ∈R
…
VOq, r ∈ R

Subscribers(T)
VO1
VO2
…
VOn

Figure 3. The ACL-Cap Model

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

- The authorization rule for publish is expressed as follows.

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

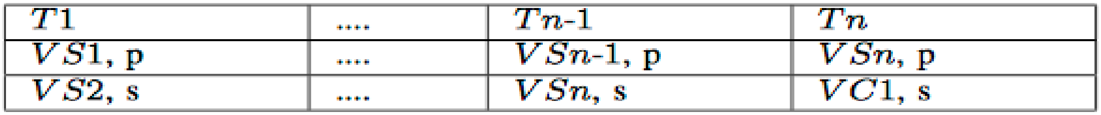
- The authorization rule for subscribe is expressed as follows.

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

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

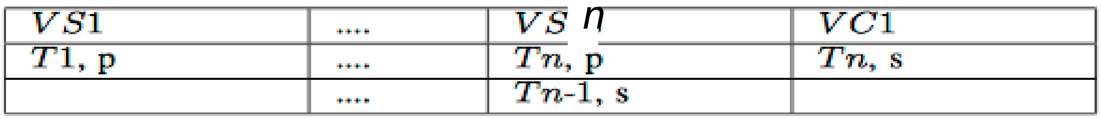
$$\text{Auth-Forward}(\text{T, VO}) \equiv \text{VO} \in \text{Subscribers}(\text{T}) \wedge \text{T} \in \text{Subscriptions}(\text{VO})$$

Table I
ACL OF TOPICS



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

Table II
CAPABILITY LIST OF VOs



$VS1$	....	VS n	$VC1$
$T1$, 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}

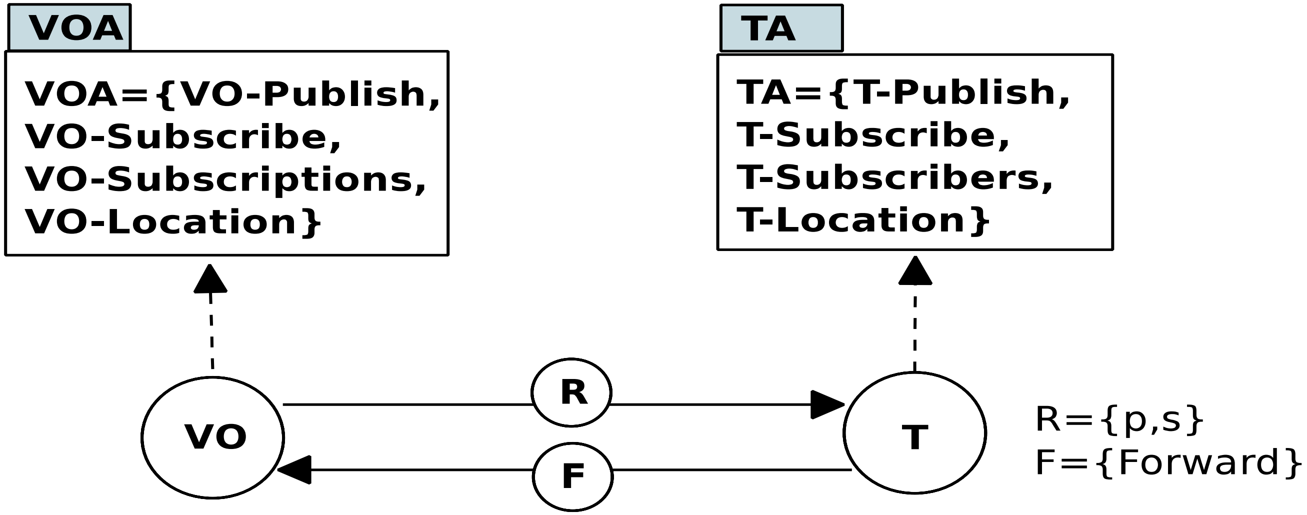

VOA
VOA={VO-Publish, VO-Subscribe, VO-Subscriptions, VO-Location}
TA
TA={T-Publish, T-Subscribe, T-Subscribers, T-Location}
VO
R
F
T
R={p,s}
F={Forward}

Figure 4. ABAC Operational Model

B. ABAC Operational Model

- The authorization rule for publish is expressed as follows.

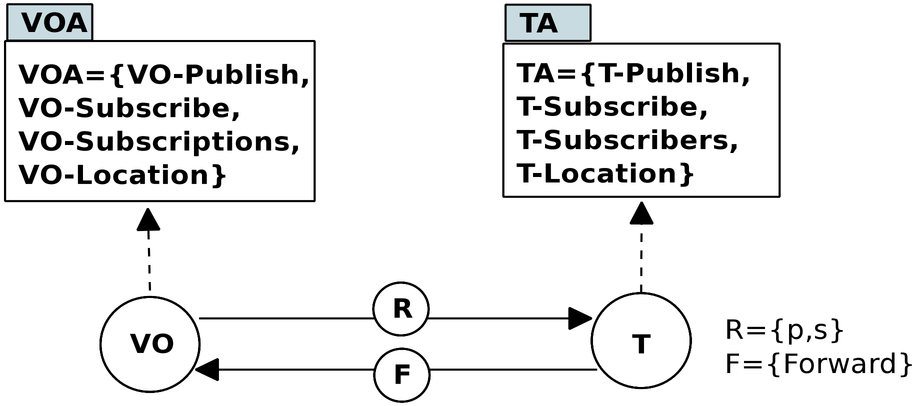
$$\text{Auth-Publish}(VO,T) \equiv T \in \text{VO-Publish}(VO) \wedge VO \in \text{T-Publish}(T)$$

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

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



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

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

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

Figure 4. ABAC Operational Model

- 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.
  A. Administrative ACL Model
  B. Administrative RBAC Model
  C. 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/from attributes of T?
- Who is allowed to assign or delete values to/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.

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

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

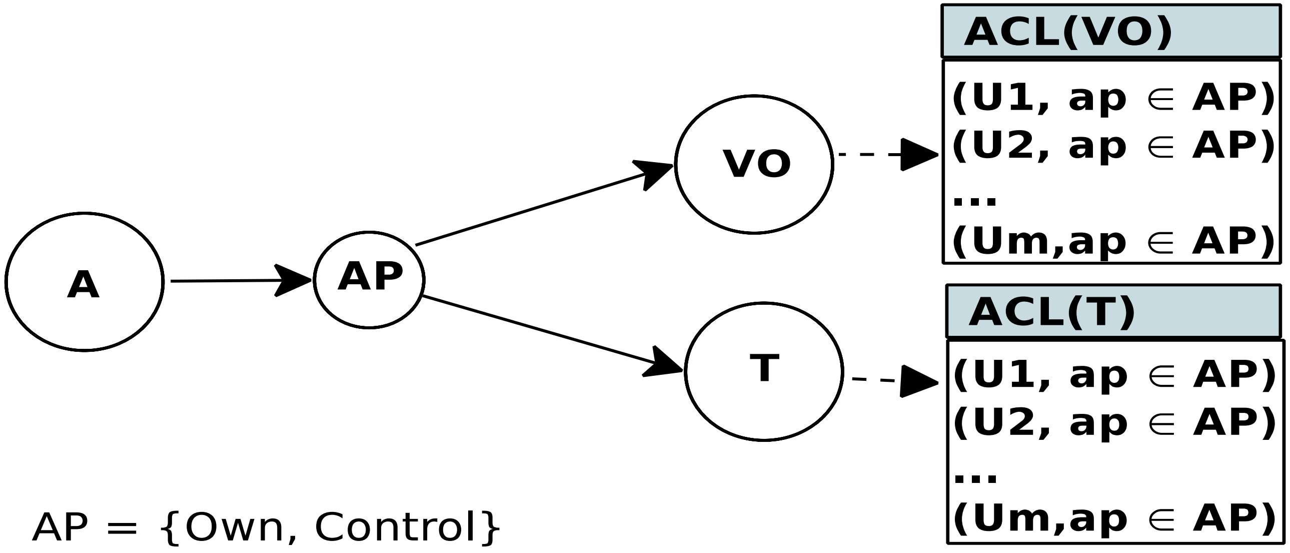


Figure 5. Administrative ACL

A. Administrative ACL Model

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

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

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

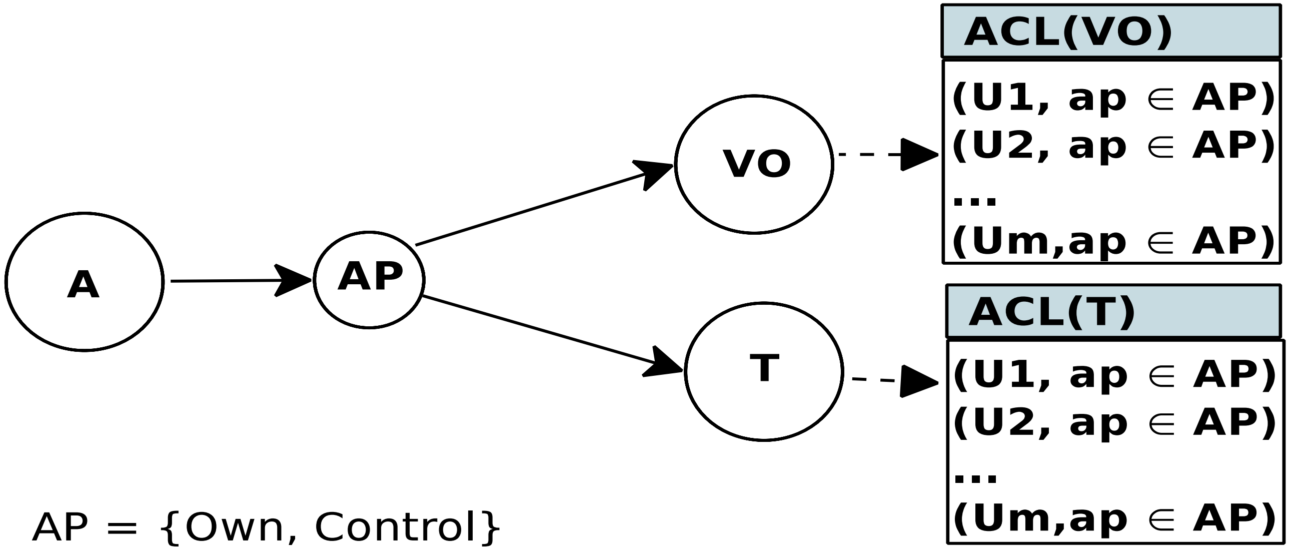
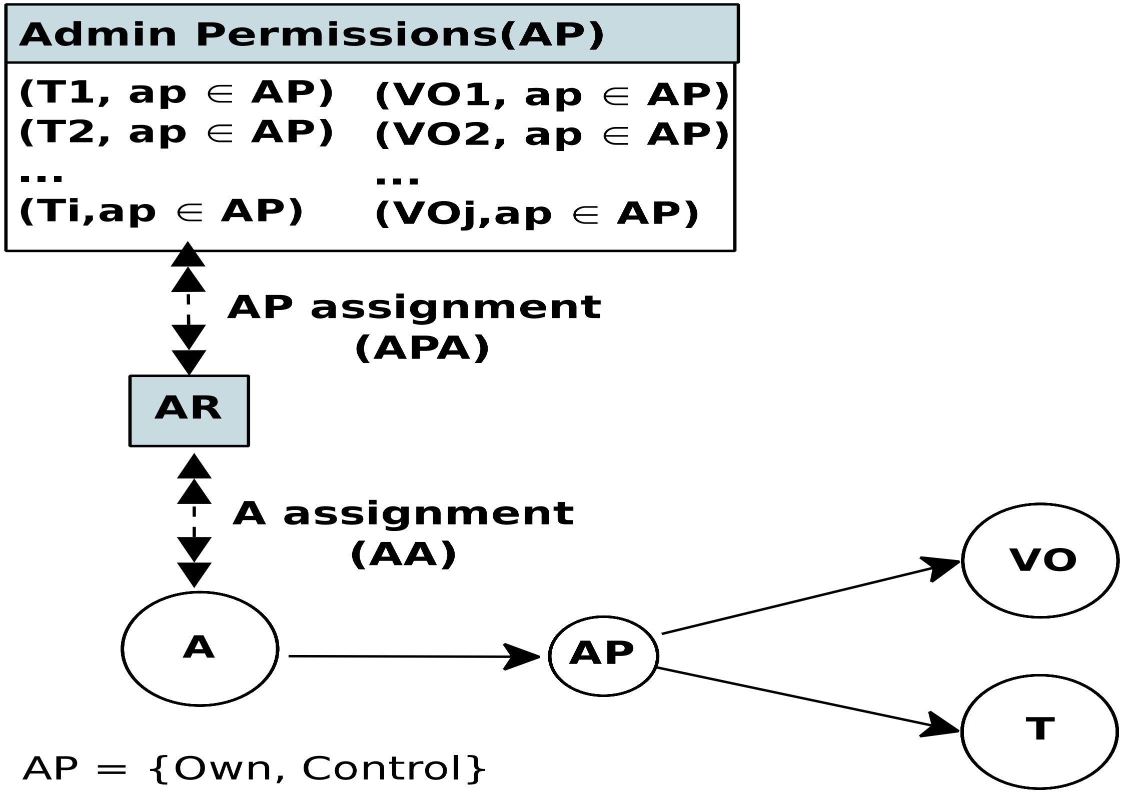


Figure 5. Administrative ACL

B. Administrative RBAC Model

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

$$AR = \{AR1, .., ARs\},$$
$$AP = (VO \times AP) \cup (T \times AP)$$



Admin Permissions(AP)

(T1, ap ∈ AP) (VO1, ap ∈ AP)
(T2, ap ∈ AP) (VO2, ap ∈ AP)
... ...
(Ti,ap ∈ AP) (VOj,ap ∈ AP)

AP = {Own, Control}

Figure 6. Administrative RBAC

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 = {U-Type, U-Location, U-Department}

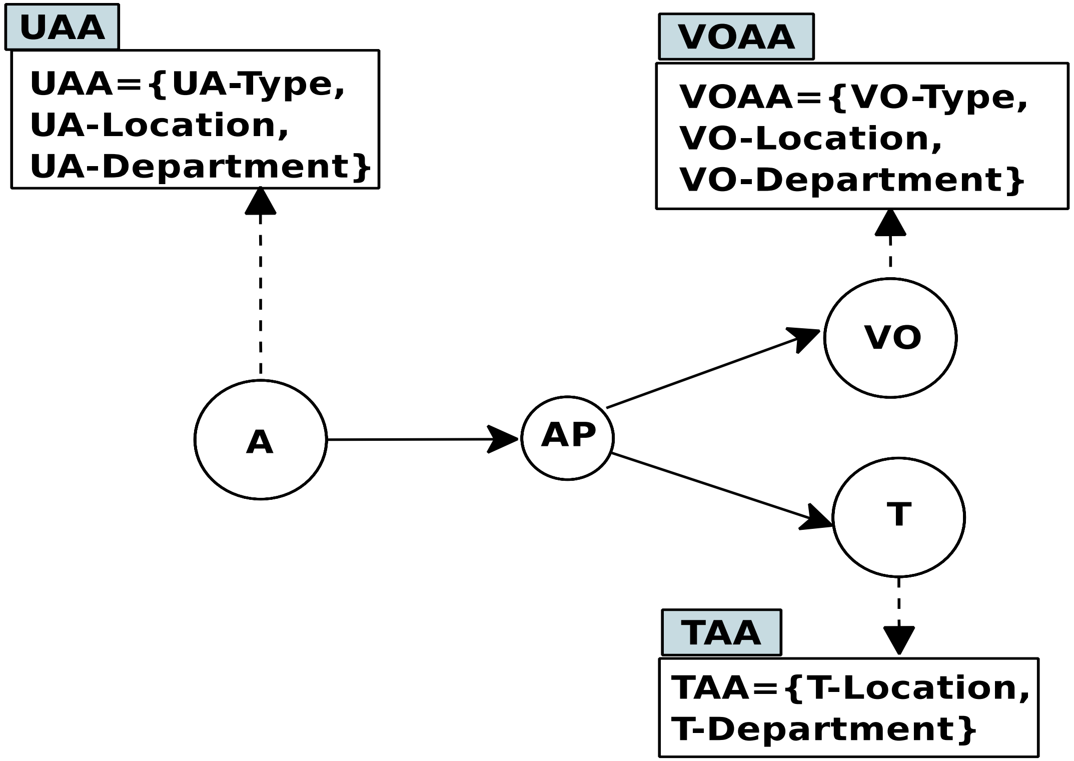

UAA
UAA={UA-Type, UA-Location, UA-Department}
VOAA
VOAA={VO-Type, VO-Location, VO-Department}
VO
A
AP
T
TAA
TAA={T-Location, T-Department}

Figure 9. Administrative ABAC

C. Administrative ABAC Model

The authorization to use the Control permission with respect to virtual objects or topics is specified as follows.

$$
\begin{gathered}
Auth\text{-}Control(U,VO) \equiv \\
(U\text{-}Type(U) = Own \lor U\text{-}Type(U) = Control) \land \\
U\text{-}Department(U\ ) = VO\text{-}Department(VO) \land \\
(VO\text{-}type = sensor \lor VO\text{-}type = camera) \land \\
U\text{-}location \approx VO\text{-}Location(VO)
\end{gathered}
$$

$$
\begin{gathered}
Auth\text{-}Control(U,T) \equiv \\
(U\text{-}Type(U) = Own \lor U\text{-}Type(U) = Control) \land \\
U\text{-}Department(U) = T\text{-}Department(T) \land \\
U\text{-}location = T\ \text{-}Location(T\ )
\end{gathered}
$$

CURRENT AND FUTURE REASEARCH

- Current Research:
  - Studying VO communication within AWS IoT.
  - Studying the access control model of VO communication within AWS IoT

- Future research:
  - Proposing access control models for User and Virtual Object communication.
  - Proposing access control models for data accumulated within Virtual objects and cloud services.

CONCLUSION

* Develop access control models for VO communication in two layers:

A - Operational models

- ❑ ACL and Capability Based (ACL-Cap) Operational Model
- ❑ ABAC Operational Model

B - Administrative models

- ❑ Administrative ACL Model
- ❑ Administrative RBAC Model
- ❑ Administrative ABAC Model

Thanks!