Access Controls in Smart Cars: Needs and Solutions

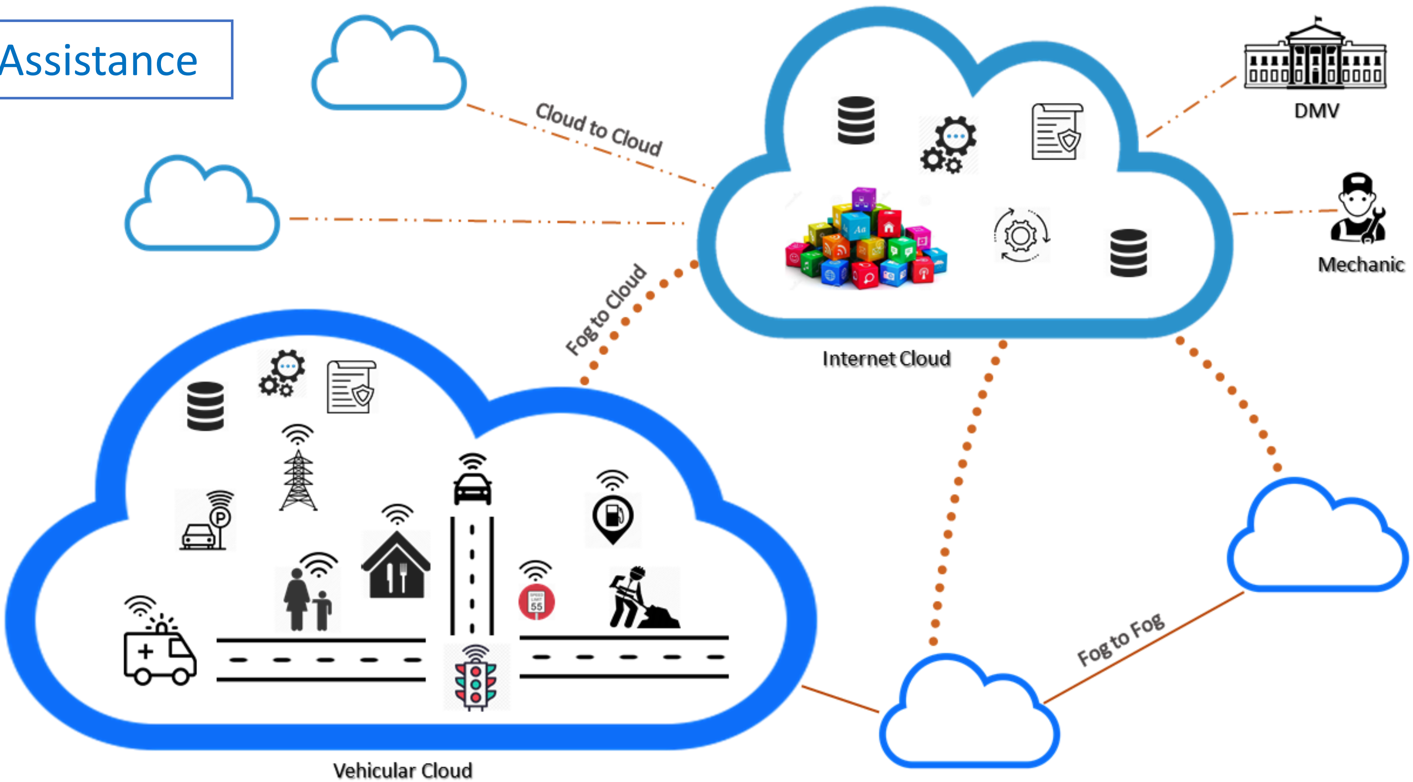
Maanak Gupta
Postdoctoral Research Fellow
Institute for Cyber Security
University of Texas at San Antonio

Guest Lecture CS 6393/4593
April 05, 2019

gmaanakg@yahoo.com
http://sites.google.com/view/maanakgupta

Smart Cars Ecosystem

Safety and Assistance

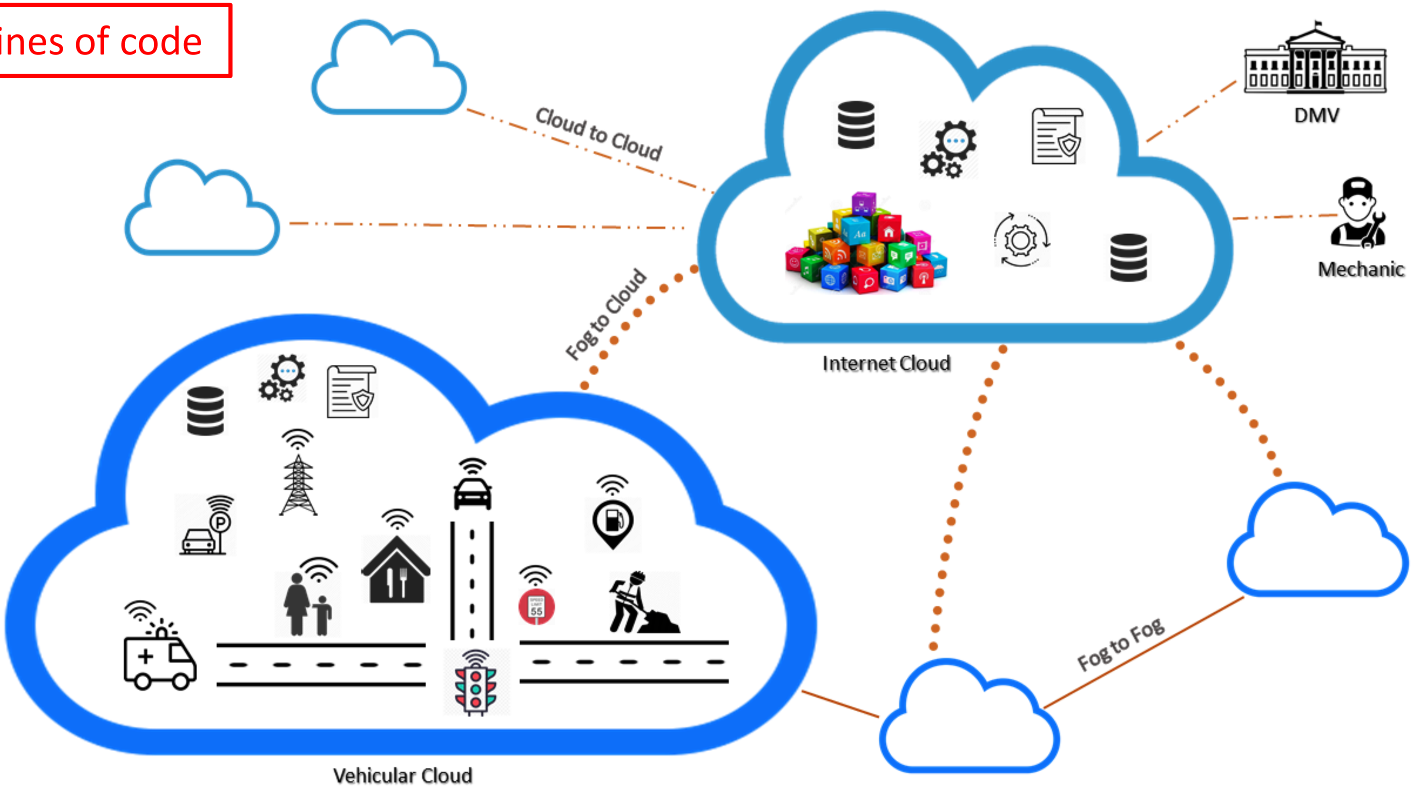


Information and Entertainment

High Mobility, Location Centric
Time Sensitive, Dynamic Pairing
Multiple Fog/Cloud Infrastructures

No More Isolated.!

100 million lines of code



Software Reliance , Broad Attack Surface, Untrusted Entities

The Perfect World.!

USER

operates on

(Read/write/execute/control)

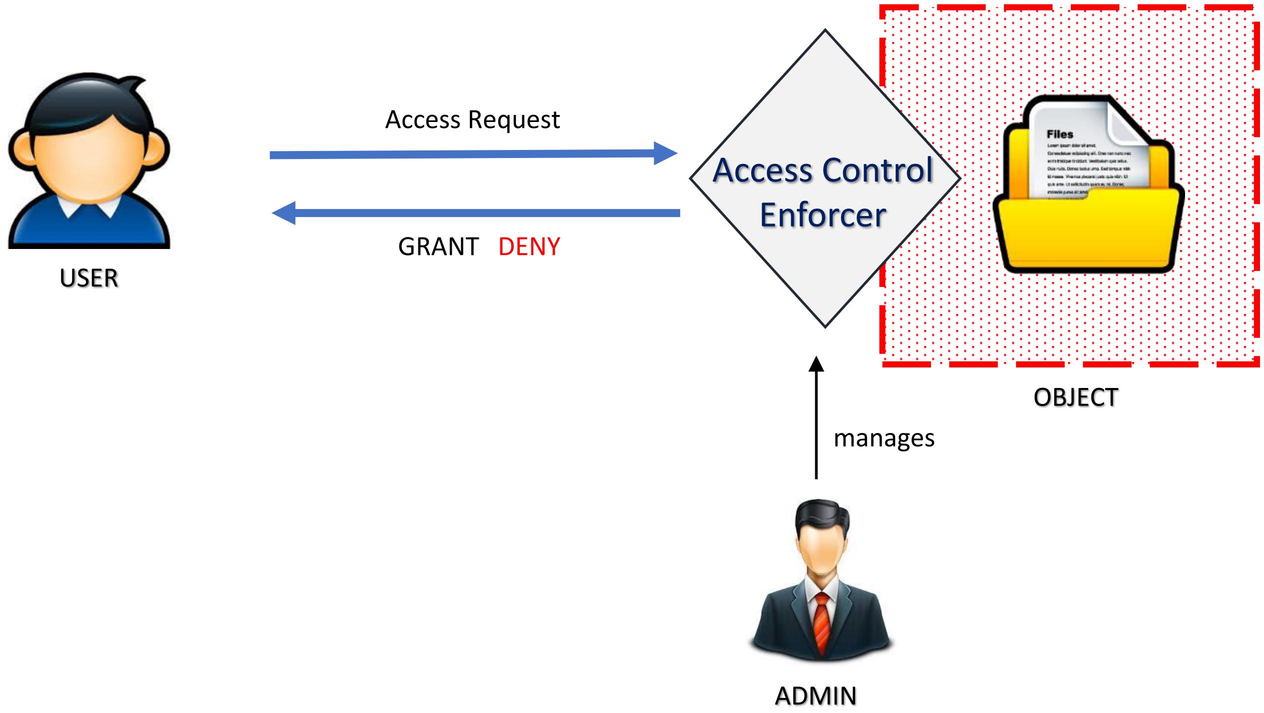
OBJECT

I **TRUST** my users.
Everything is Secure. !!

Confidentiality
Integrity
Availability

Thank YOU.!!

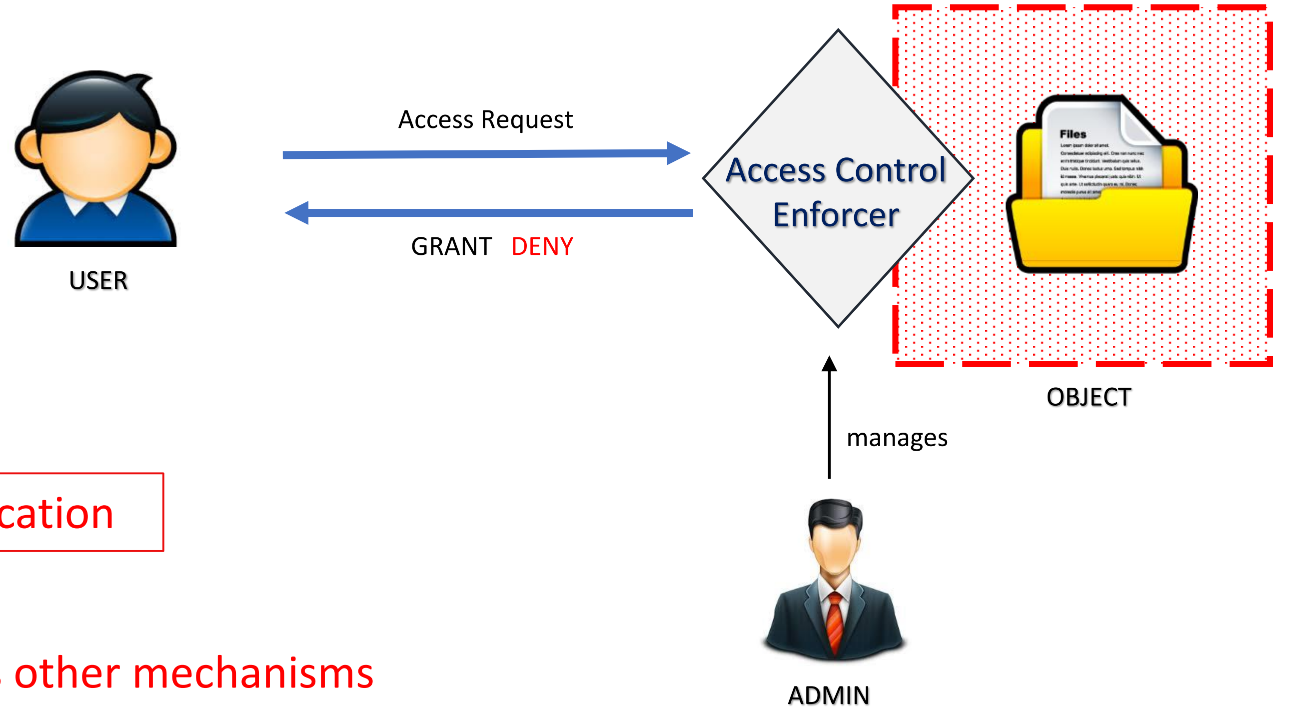
Access Control Mechanisms



A user [U] is allowed to perform an operation [OP] on an object [OB] if security policy [P] is satisfied.

Access Control Mechanisms

PROTECTION



Post Authentication

Complements other mechanisms

A user [U] is allowed to perform an operation [OP] on an object [OB] if security policy [P] is satisfied.

Attribute Based Access Control

- Three Dominant Models: DAC, MAC and RBAC.
- ABAC: Decision based on the attributes of entities
- Attributes are name value pair: age (Alice) → 29
- Core entities in ABAC include:
  - Users
  - Objects
  - Environment or Context
  - Operations

  Attributes
- Authorization Policies: determine rights just in time
  - retrieve attributes of relevant entities in request
- Enhance flexibility and fine grained access control
- NIST Guidelines to ABAC

Access Control Needs in Smart Cars

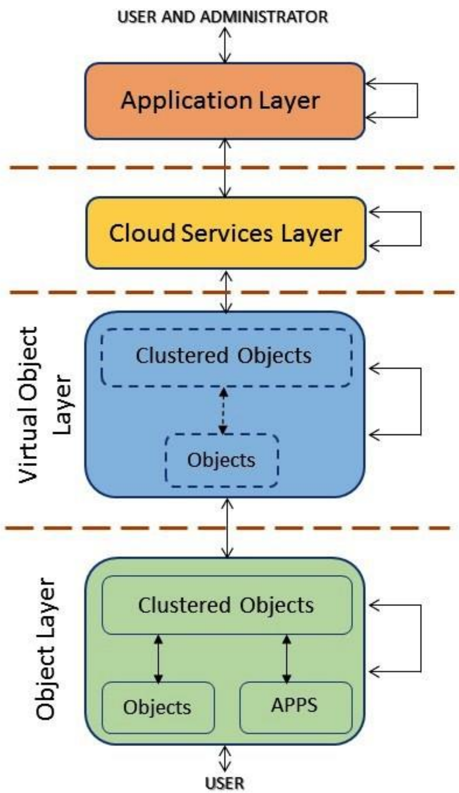
- On-Board Data, Applications and Sensors
- Third Party devices
- V2X fake messages
- User Privacy Preferences
- Over the Air updates
- Loss of Information in Cloud
- Location and time sensitivity of the services.
- In-vehicle communication

Scope of Contribution

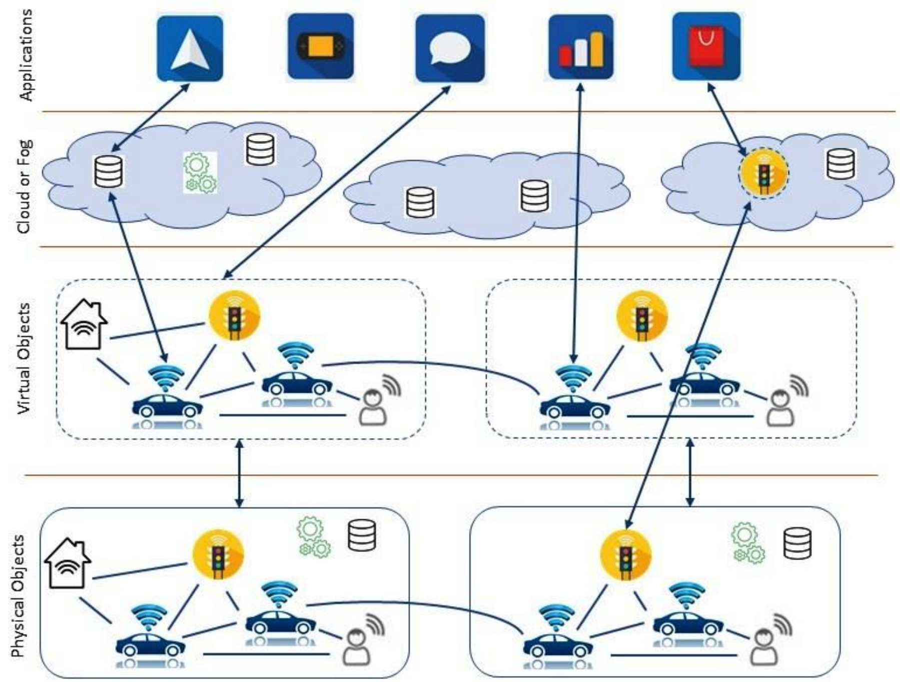
- Contribution
  - Access Control Oriented Architecture for Smart Cars.
  - Propose formalized ABAC model for cloud assisted applications.
  - Dynamic groups and user preferences.
  - Implementation of the model in AWS.

- Scope
  - Single Central Cloud
  - No direct access and physical tampering
  - Communication Channel is encrypted.
  - Data in Cloud is secure
  - In-vehicle security not considered

Extended Access Control Oriented Architecture



E-ACO architecture

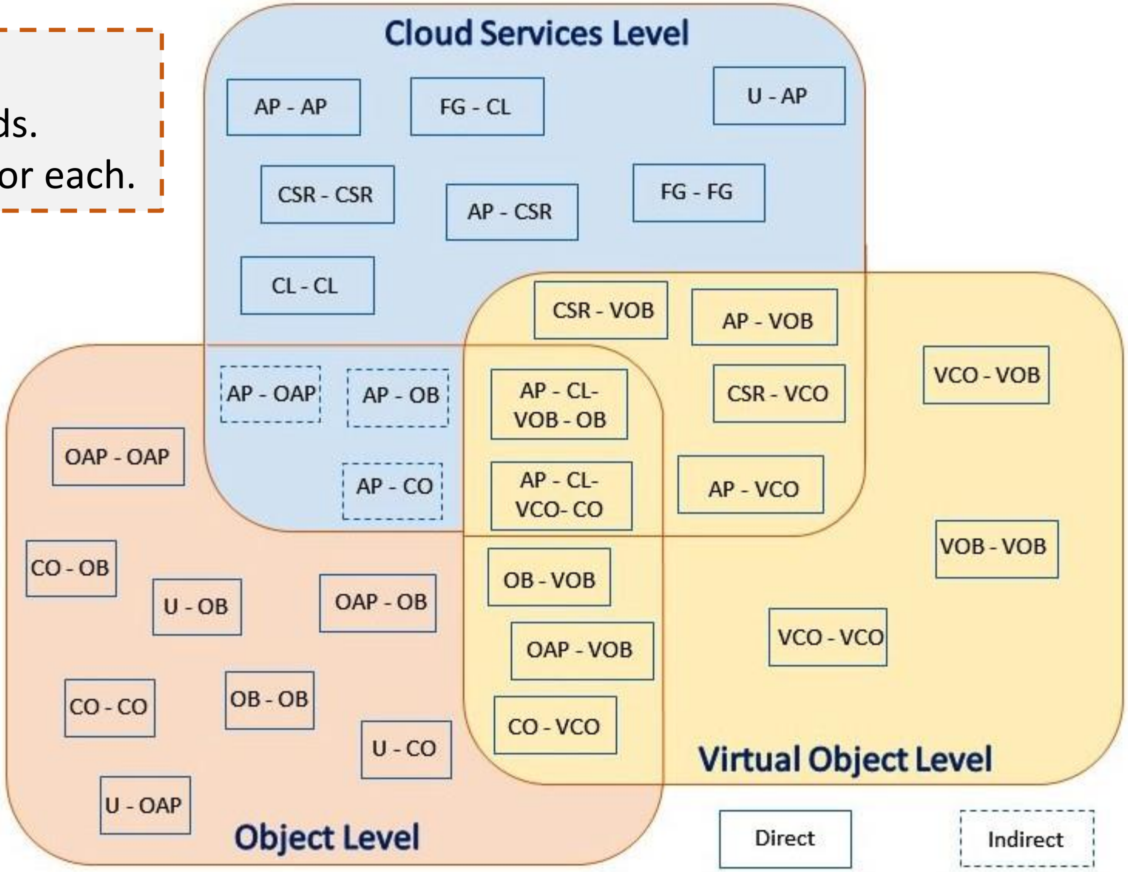


Vehicular IoT components in architecture

Authorization Framework

An Authorization Framework:

- Helps understand access control needs.
- Helps understand models suitability for each.

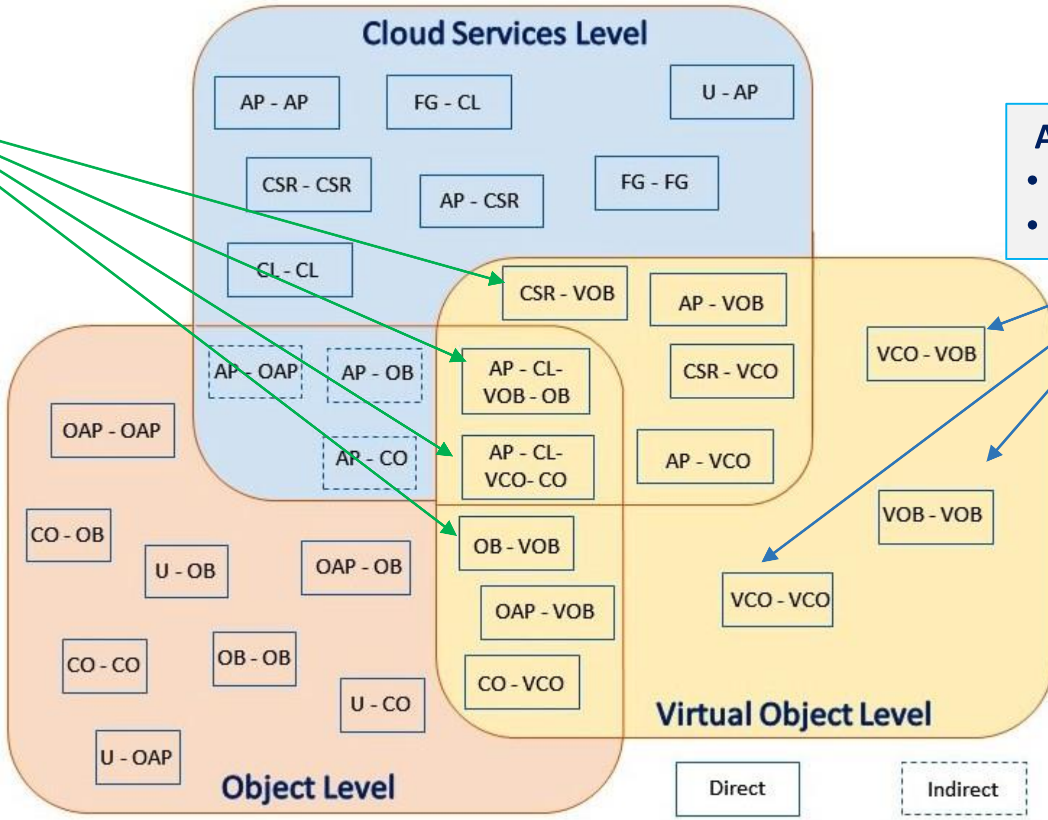


U: User **CO:** Clustered Objects **OB:** Objects **OAP:** Object Layer Applications **CL:** Cloud **FG:** Fog
CSR: Cloud Services **VCO:** Virtual Clustered Objects **VOB:** Virtual Objects **AP:** User Applications

Authorization Framework

AWS-IoTAC Model
- Policy Based
- Limited Attributes

AWS-IoT-ACMVO Model
- For Virtual Objects
- ACLs, RBAC, ABAC



U: User **CO:** Clustered Objects **OB:** Objects **OAP:** Object Layer Applications **CL:** Cloud **FG:** Fog
CSR: Cloud Services **VCO:** Virtual Clustered Objects **VOB:** Virtual Objects **AP:** User Applications

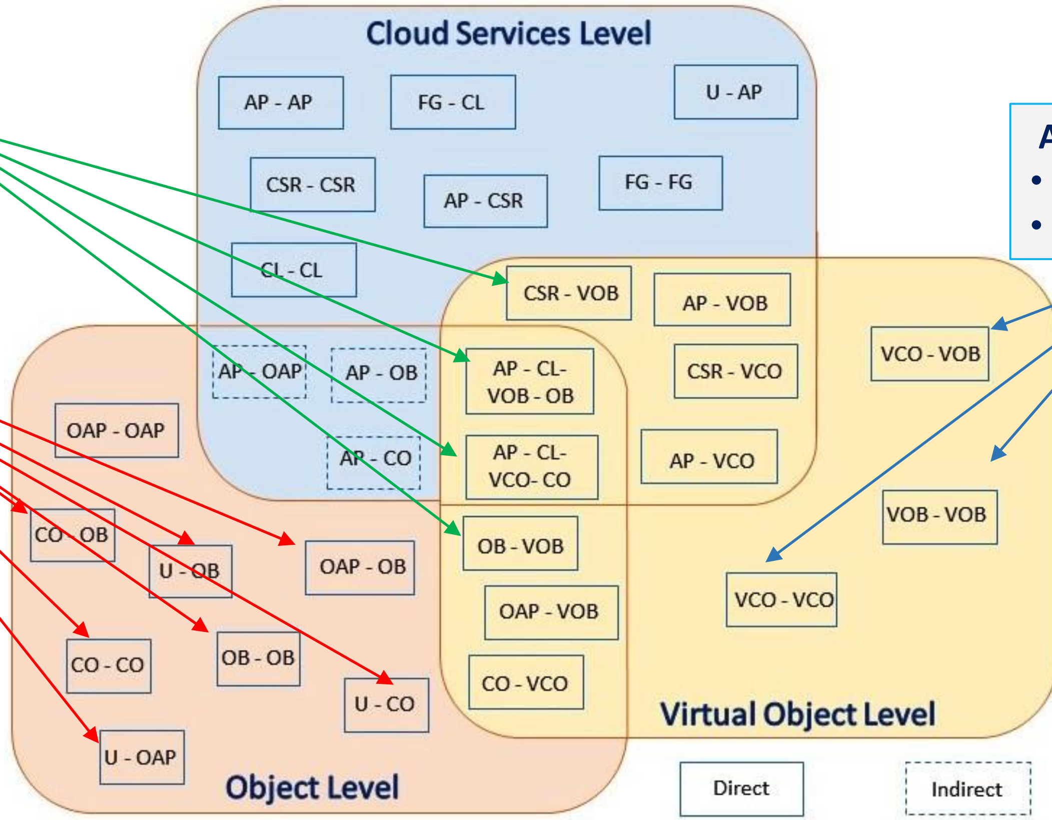
Authorization Framework

AWS-IoTAC Model
- Policy Based
- Limited Attributes

Our Solution
- Pure ABAC
- User Privacy

Cloud Supported

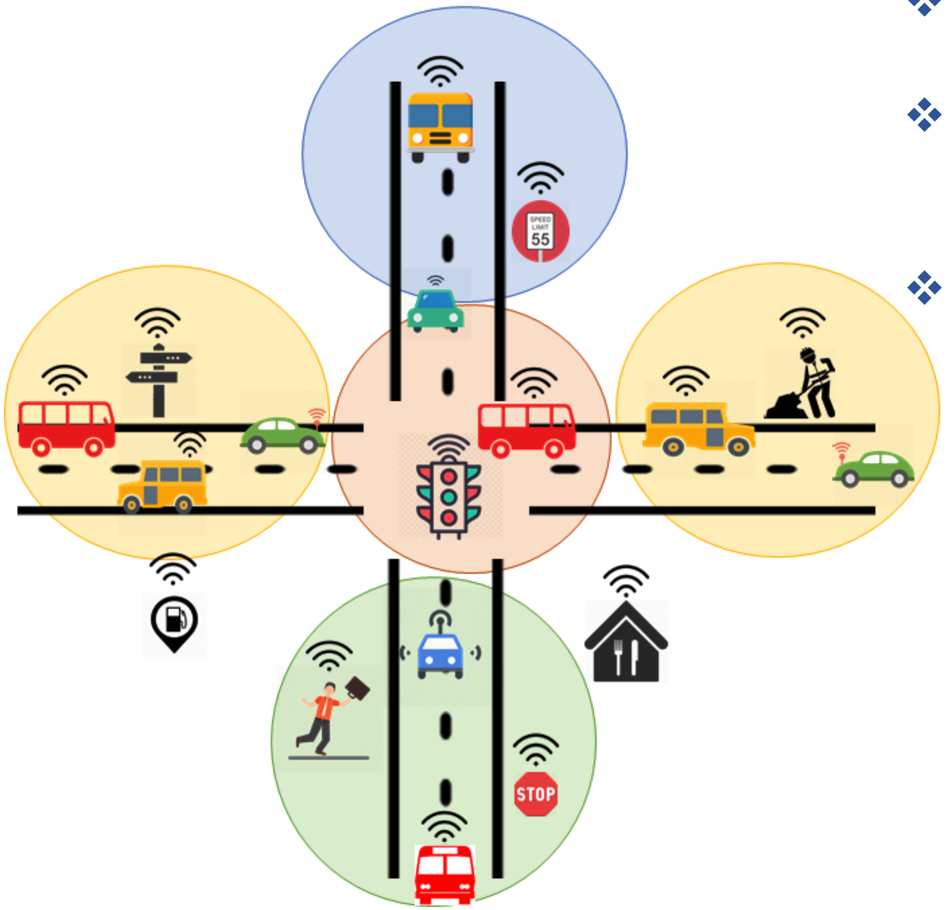
AWS-IoT-ACMVO Model
- For Virtual Objects
- ACLs, RBAC, ABAC



U: User **CO:** Clustered Objects **OB:** Objects **OAP:** Object Layer Applications **CL:** Cloud **FG:** Fog
CSR: Cloud Services **VCO:** Virtual Clustered Objects **VOB:** Virtual Objects **AP:** User Applications

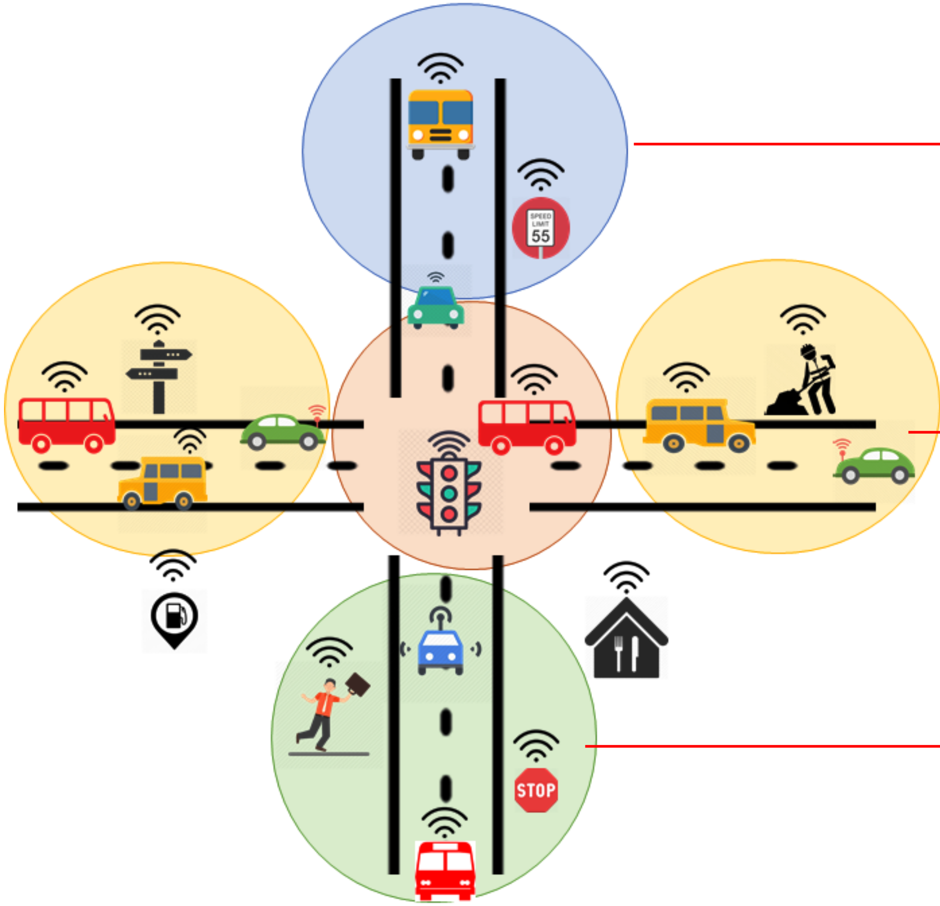
World Leading Research with Real World Impact!

Location Groups



- Categorizing wide locations into smaller groups.
- Vehicles dynamically become member based on current GPS, vehicle-type or individual user preferences.
- Ensure relevance of alerts and notifications

Attributes and Alerts



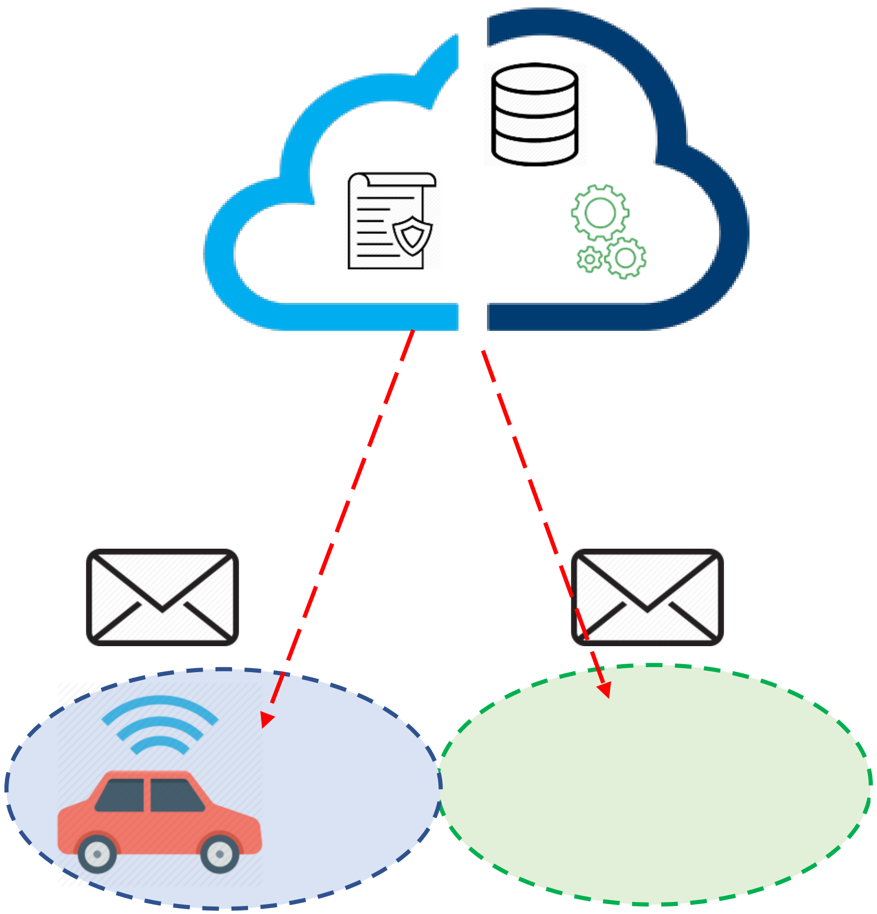
Speed Limit: 50 mph
Deer Threat: ON
Ice on Road: NO

Speed Limit: 30 mph
Flood Warning: ON
Road Work: ON

Speed Limit: 20 mph
School Zone: ON
Amber Alert: ABC123

Vehicle moves and are assigned to different groups and inherits their attributes/alerts.

Using Location Groups



Speed Limit: 50 mph
Deer Threat: ON
Ice on Road: NO

Speed Limit: 30 mph
Flood Warning: ON
Road Work: ON

Administrative Questions:

- How the attributes or alerts of groups are updated?
- How are moving entities assigned to groups?
- How groups hierarchy is created?

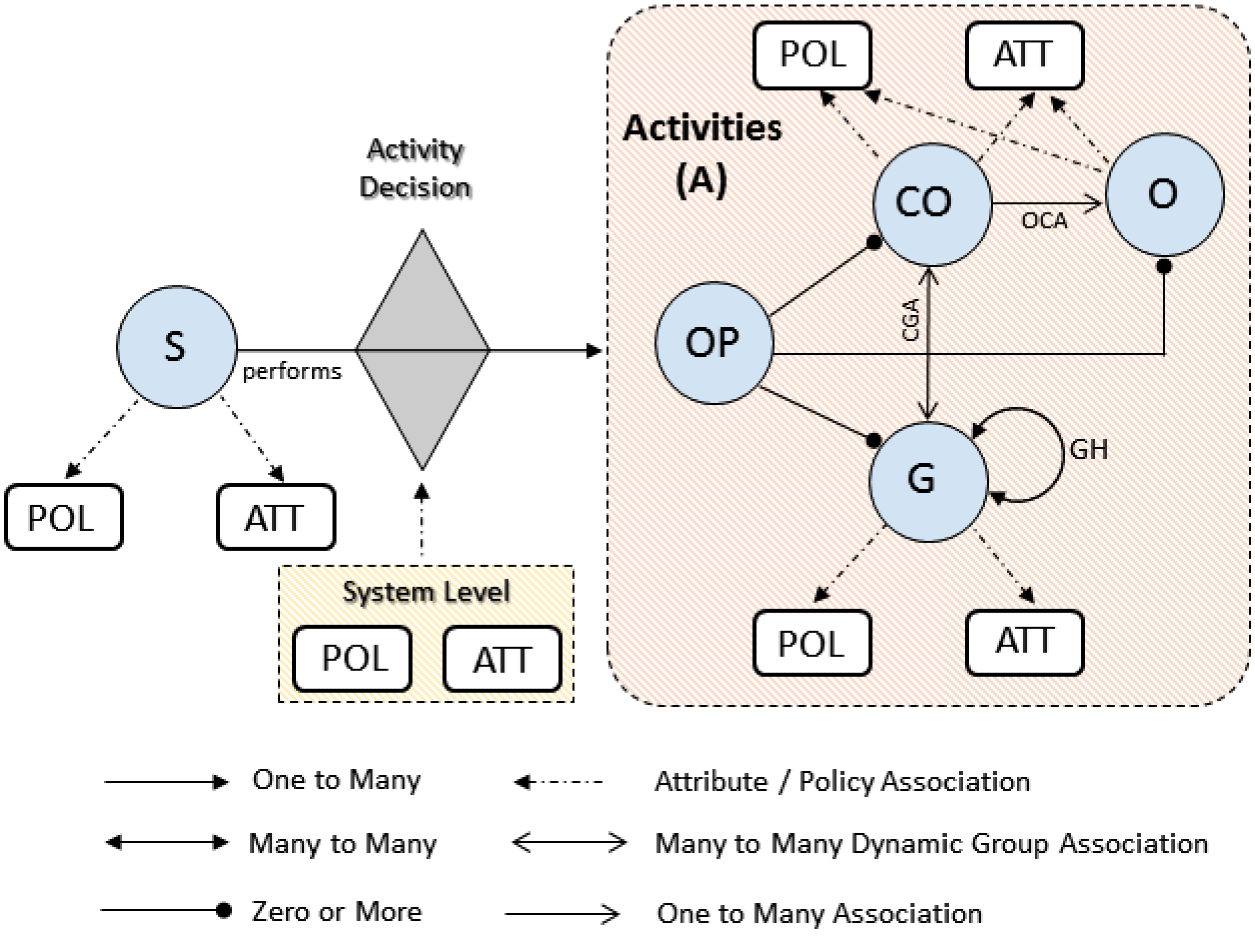
Operational Questions:

- How attributes and groups are used to provide security?
- How user privacy preferences are considered?

{"state": {"reported": {"Latitude": "29.4769353",
"Longitude":"-98.5018237"}}}

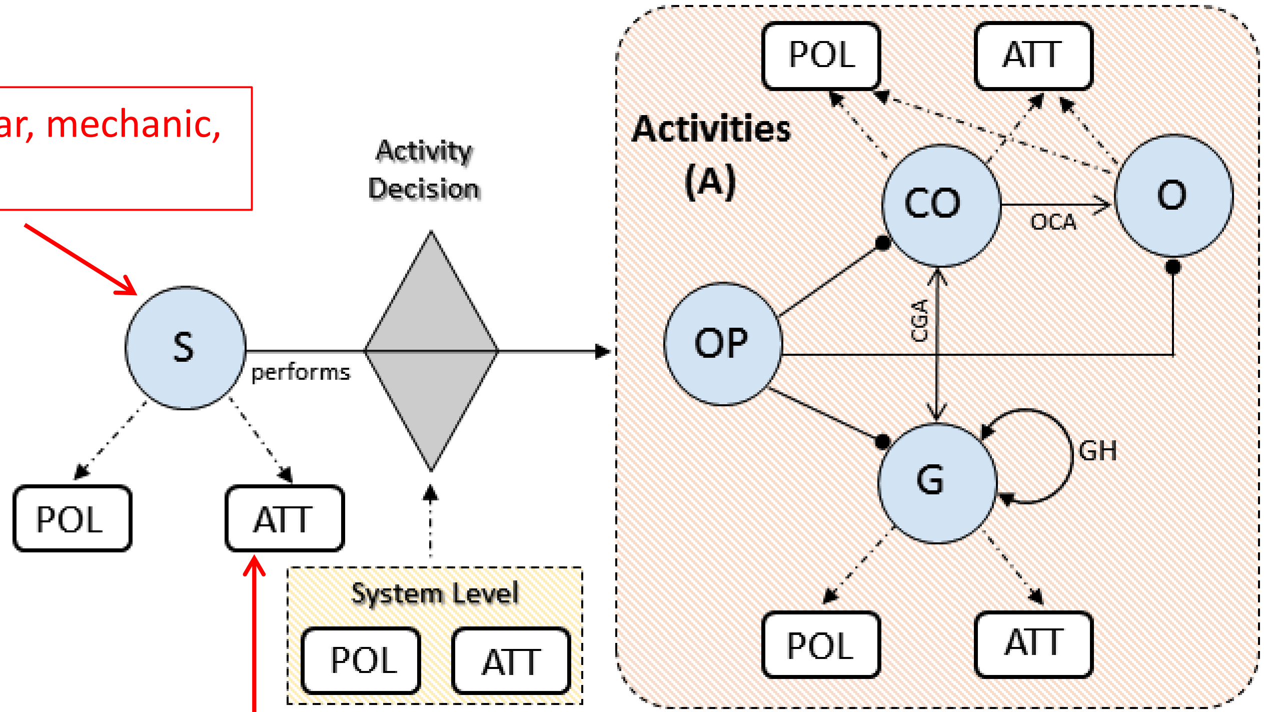
Reported MQTT message

CV-ABAC$_G$ Model



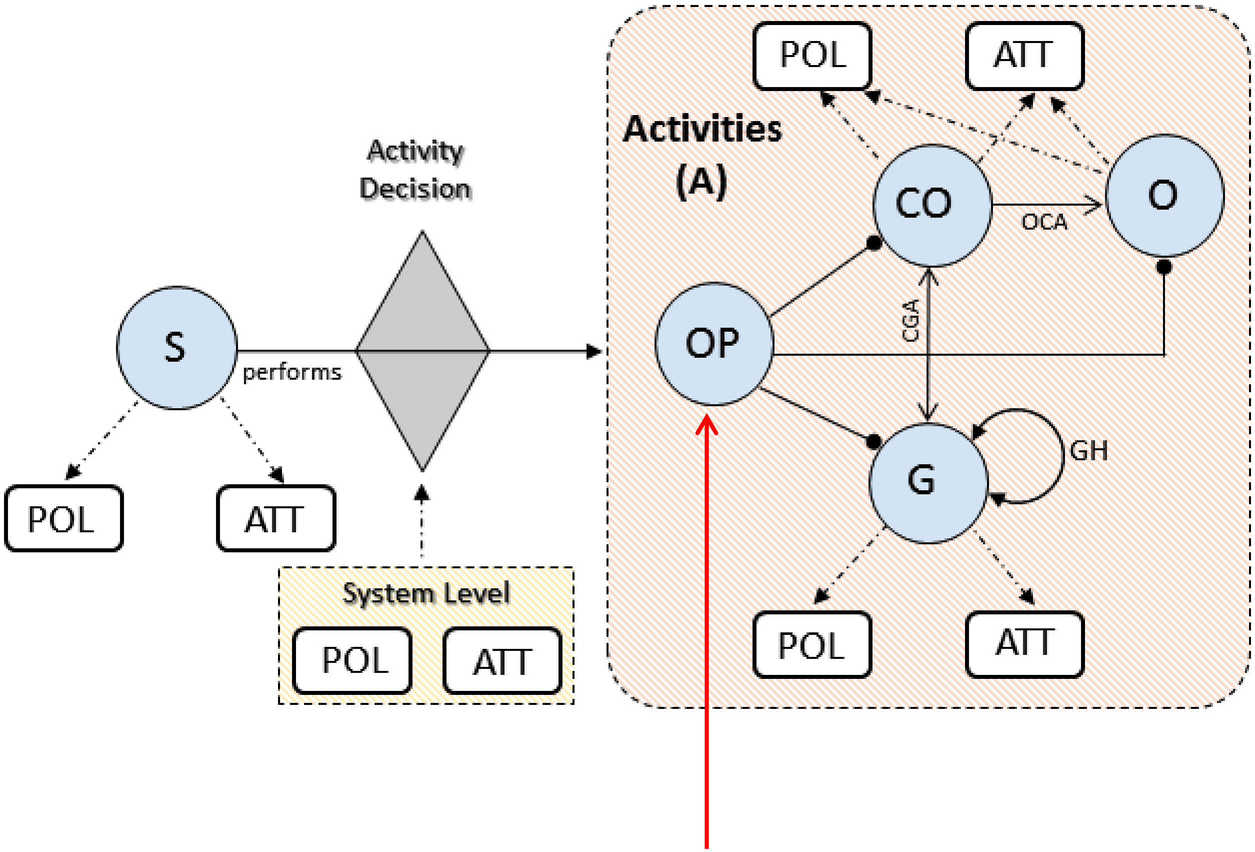
Model Components

user, sensor, car, mechanic, restaurant



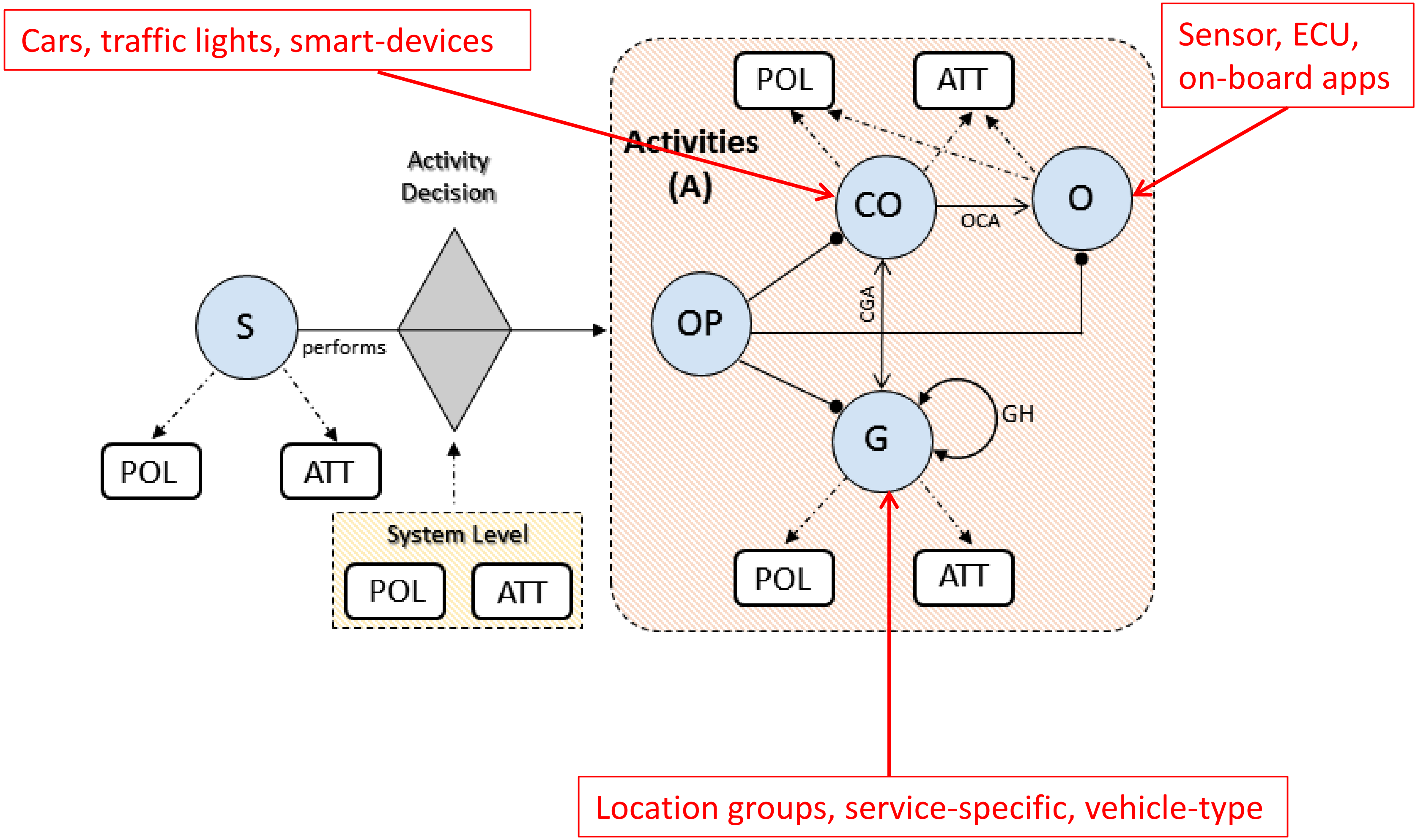
{ location, size, IP, direction, speed, VIN, cuisine-type}

Model Components



{ read, write, control, notify, administrative actions }

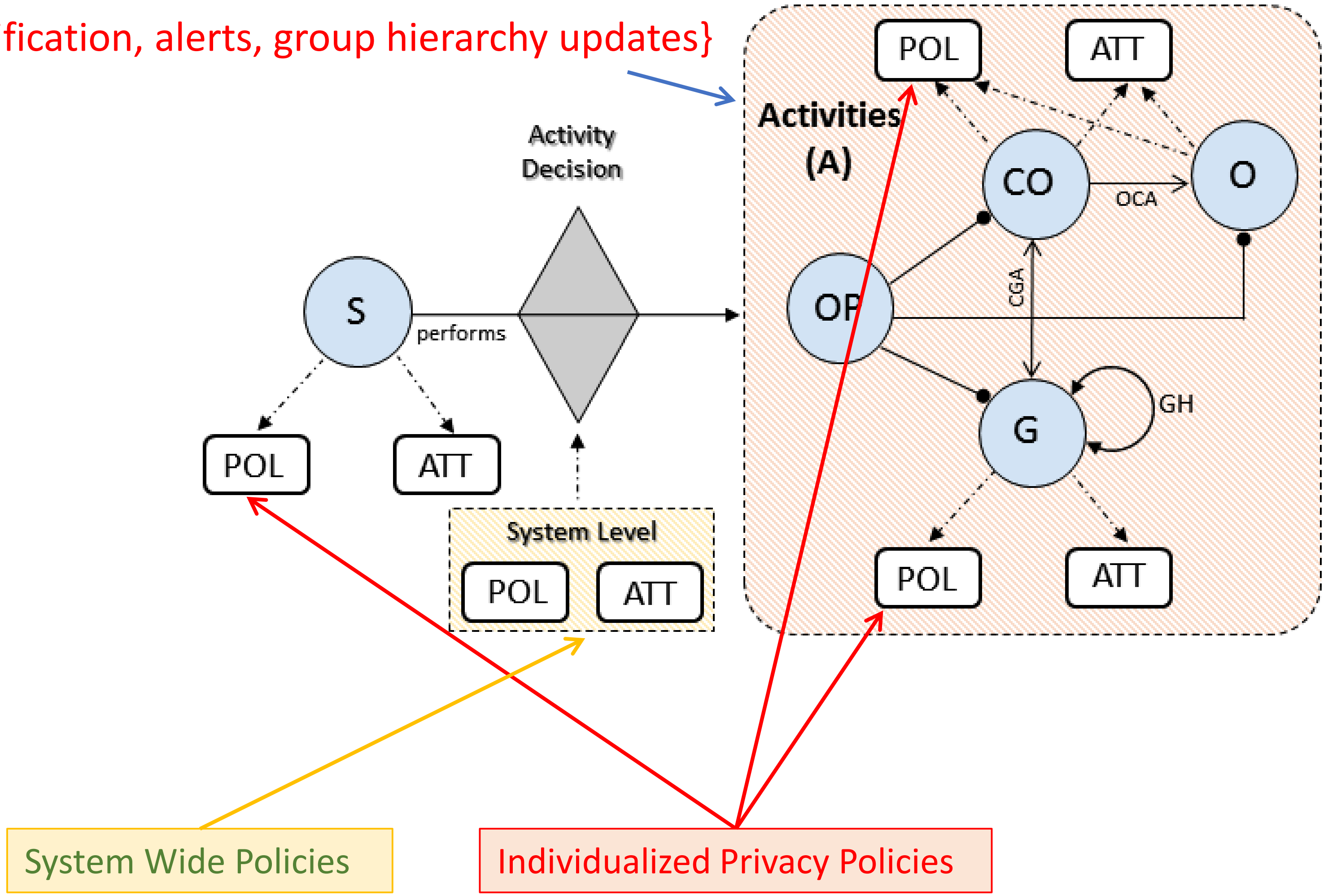
Model Components



Model Components

Operational and Administrative Activities

{notification, alerts, group hierarchy updates}



Formal Specification

Basic Sets and Functions

– S, CO, O, G, OP are finite sets of sources, clustered objects, objects, groups and operations respectively [blue circles in Figure 4].
– A is a finite set of activities which can be performed in system.
– ATT is a finite set of attributes associated with S, CO, O, G and system-wide. Attribute Function
– For each attribute att in ATT, Range(att) is a finite set of atomic values.
– attType: ATT = {set, atomic}, defines attributes to be set or atomic valued. Attribute Type
– Each attribute att in ATT maps entities in S, CO, O, G to attribute values. Formally,

$$\mathrm{att} : S \cup CO \cup O \cup G \cup \{\text{system-wide}\} \rightarrow \begin{cases} \mathrm{Range(att)} \cup \{\perp\} & \text{if attType(att) = atomic} \\ 2^{\mathrm{Range(att)}} & \text{if attType(att) = set} \end{cases}$$

– POL is a finite set of authorization policies associated with individual S, CO, O, G.
– directG : CO $\rightarrow$ G, mapping each clustered object to a system group, equivalently CGA $\subseteq$ CO $\times$ G.
– parentCO : O $\rightarrow$ CO, mapping each object to a clustered object, equivalently OCA $\subseteq$ O $\times$ CO.
– GH $\subseteq$ G $\times$ G, a partial order relation $\geq_g$ on G. Equivalently, parentG : G $\rightarrow 2^G$, mapping group to a set of parent groups in hierarchy.

Group Hierarchy

Attribute Mapping

Formal Specification

Effective Attributes of Groups, Clustered Objects and Objects (Derived Functions)

– For each attribute att in ATT such that attType(att) = set:

- $\text{effG}_{\text{att}} : G \rightarrow 2^{\text{Range(att)}}$, defined as $\text{effG}_{\text{att}}(g_i) = \text{att}(g_i) \cup (\bigcup_{g \in \{g_j | g_i \geq_g g_j\}} \text{effG}_{\text{att}}(g))$.
- $\text{effCO}_{\text{att}} : CO \rightarrow 2^{\text{Range(att)}}$, defined as $\text{effCO}_{\text{att}}(co) = \text{att}(co) \cup \text{effG}_{\text{att}}(\text{directG}(co))$.
- $\text{effO}_{\text{att}} : O \rightarrow 2^{\text{Range(att)}}$, defined as $\text{effO}_{\text{att}}(o) = \text{att}(o) \cup \text{effCO}_{\text{att}}(\text{parentCO}(o))$.

– For each attribute att in ATT such that attType(att) = atomic:

- $\text{effG}_{\text{att}} : G \rightarrow \text{Range(att)} \cup \{\perp\}$, defined as $\text{effG}_{\text{att}}(g_i) = \begin{cases} \text{att}(g_i) & \text{if } \forall g' \in \text{parentG}(g_i).\ \text{effG}_{\text{att}}(g') = \perp \\ \text{effG}_{\text{att}}(g') & \text{if } \exists\ \text{parentG}(g_i).\ \text{effG}_{\text{att}}(\text{parentG}(g_i)) \neq \perp \text{ then select} \\ & \text{parent } g' \text{ with } \text{effG}_{\text{att}}(g') \neq \perp \text{ updated most recently.} \end{cases}$
- $\text{effCO}_{\text{att}} : CO \rightarrow \text{Range(att)} \cup \{\perp\}$, defined as $\text{effCO}_{\text{att}}(co) = \begin{cases} \text{att}(co) & \text{if } \text{effG}_{\text{att}}(\text{directG}(co)) = \perp \\ \text{effG}_{\text{att}}(\text{directG}(co)) & \text{otherwise} \end{cases}$
- $\text{effO}_{\text{att}} : O \rightarrow \text{Range(att)} \cup \{\perp\}$, defined as $\text{effO}_{\text{att}}(o) = \begin{cases} \text{att}(o) & \text{if } \text{effCO}_{\text{att}}(\text{parentCO}(o)) = \perp \\ \text{effCO}_{\text{att}}(\text{parentCO}(o)) & \text{otherwise} \end{cases}$

Attributes more Dynamic

Attributes Inheritance

Policy Language

Authorization Functions (Policies)

– Authorization Function: For each op ∈ OP, $\text{Auth}_{op}(s : S, ob : CO \cup O \cup G)$ is a propositional logic formula returning true or false, which is defined using the following policy language:

- $\alpha ::= \alpha \wedge \alpha \mid \alpha \vee \alpha \mid (\alpha) \mid \neg\alpha \mid \exists\, x \in \text{set}.\alpha \mid \forall\, x \in \text{set}.\alpha \mid \text{set} \vartriangle \text{set} \mid \text{atomic} \in \text{set} \mid \text{atomic} \notin \text{set}$
- $\vartriangle ::= \subset \mid \subseteq \mid \not\subseteq \mid \cap \mid \cup$
- $\text{set} ::= \text{eff}_{att}(i) \mid att(i)$ for $att \in ATT$, $i \in S \cup CO \cup O \cup G \cup \{\text{system-wide}\}$, $attType(att) = \text{set}$
- $\text{atomic} ::= \text{eff}_{att}(i) \mid att(i) \mid \text{value}$ for $att \in ATT$, $i \in S \cup CO \cup O \cup G \cup \{\text{system-wide}\}$, $attType(att) = \text{atomic}$

❖ Administrators in the police department can send alert to location-groups in city limits.

$\text{Auth}_{alert}(u{:}U, g{:}G)$ :: dept (u) Police ∧ parent-city(g) = Austin ∧
Austin ∈ jursidiction (u).

❖ Only mechanic in the technician department from Toyota-X dealership must be able to read sensor in Camry LE. Further, this operation must be done between time 9 am to 6 pm.

$\text{Auth}_{read}(u{:}U, co{:}CO)$ :: role (u) Technician ∧ employer(u) = Toyota-X ∧
make (co) = Toyota ∧ model(co) = Camry LE ∧
operation_time(u) ∈ {9am,10,11…6pm}

Activity Authorization Decision

Authorization Decision

– A source $s \in S$ is allowed to perform an activity $a \in A$, stated as Authorization$(a : A, s : S)$, if the required policies needed to allow the activity are included and evaluated to make final decision. These multi-layer policies must be evaluated for individual operations ($op_i \in OP$) to be performed by source $s \in S$ on relevant objects ($x_i \in CO \cup O \cup G$).

Formally, $\text{Authorization}(a : A, s : S) \Rightarrow \text{Auth}_{op_1}(s : S, x_1), \text{Auth}_{op_2}(s : S, x_2), \ldots\ldots\ldots\ldots, \text{Auth}_{op_n}(s : S, x_3)$

Evaluate all relevant policies to make a decision

A restaurant in group A must be allowed to send notifications to all vehicles in location group A and group B.

System defined

DECISION

User Preference

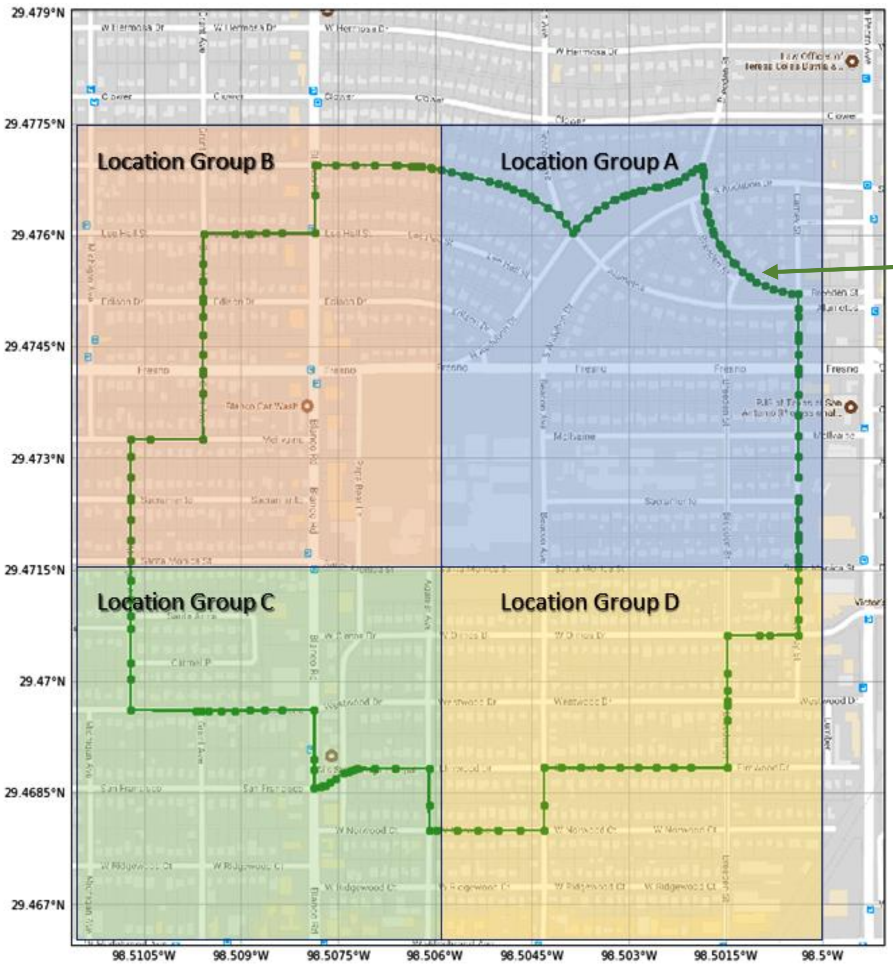
I only want notifications from Cheesecake factory.

Implementation in Amazon Web Services (AWS)

I·C·S The Institute for Cyber Security

Vehicles and Groups

C·SPECC Center for Security and Privacy Enhanced Cloud Computing



4 Location Groups (static demarcation)

Vehicles movement (coordinates generated using Google API)

```
('Received new coordinates from:', 'Vehicle-1')
Sun May 27 02:56:30 2018
  Location A
     Car-A : [u'Vehicle-1', u'Vehicle-2']
     Bus-A : []
  Location B
     Car-B : []
     Bus-B : [u'Vehicle-6']
  Location C
     Car-C : [u'Vehicle-3', u'Vehicle-4']
     Bus-C : []
  Location D
     Car-D : []
     Bus-D : [u'Vehicle-5']
```

Snapshot (table keeps changing)

Implemented Policies

Administrative Policy

- Road side motion sensor with [id = 1] and current GPS in group [Location-A] can only [modify] attribute [Deer Threat] to value [ON, OFF] for group [Location-A].

Operational Policy

Restaurant Notification Use Case

System Defined Policy

- A restaurant located within group [Location-A] can only [send notifications] to members of groups [Location-A, Location-B].

User Preferences

- Send notifications only between [7 pm to 9 pm] only on [Wednesdays].

Performance Metrics

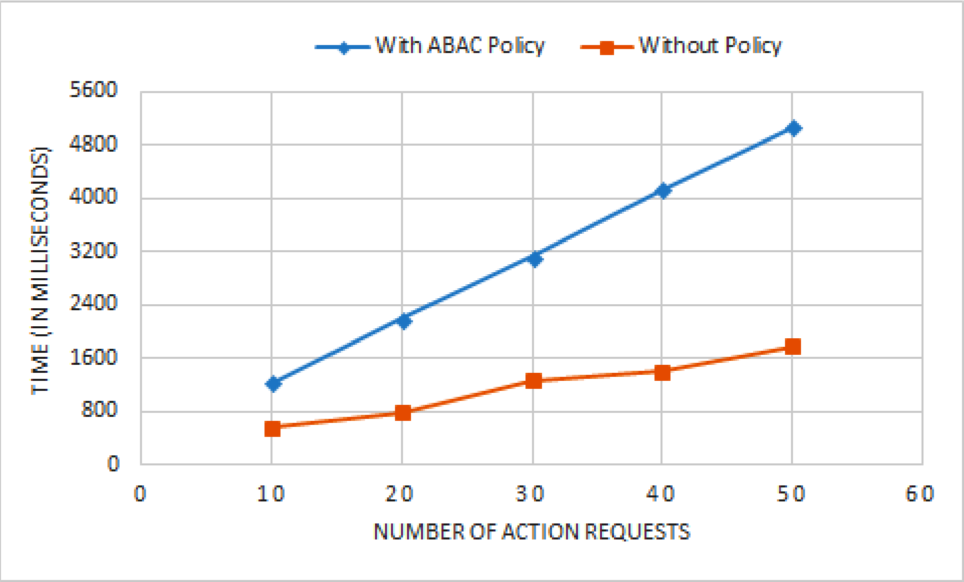
Number of Requests	Policy Enforcer Execution Time (in ms)
10	0.0501
20	0.1011
30	0.1264
40	0.1630
50	0.1999

Policy Enforcement Time

	CARS NOTIFIED	
n^{th} Request	With ABAC Policy	Without Policy
41^{st}	20	50
42^{nd}	30	50
43^{rd}	50	50
44^{th}	30	50
45^{th}	20	50
46^{th}	30	50

Relevance of Alerts and Notifications

Performance Metrics



Comparing Policy vs No Policy Execution Time

Lets Talk ..!!

Questions, Comments or Concerns

gmaanakg@yahoo.com

https://sites.google.com/view/maanakgupta