

Secure Cloud Assisted Smart Cars and Big Data: Access Control Models and Implementation

Ph.D. Dissertation Defense

Maanak Gupta

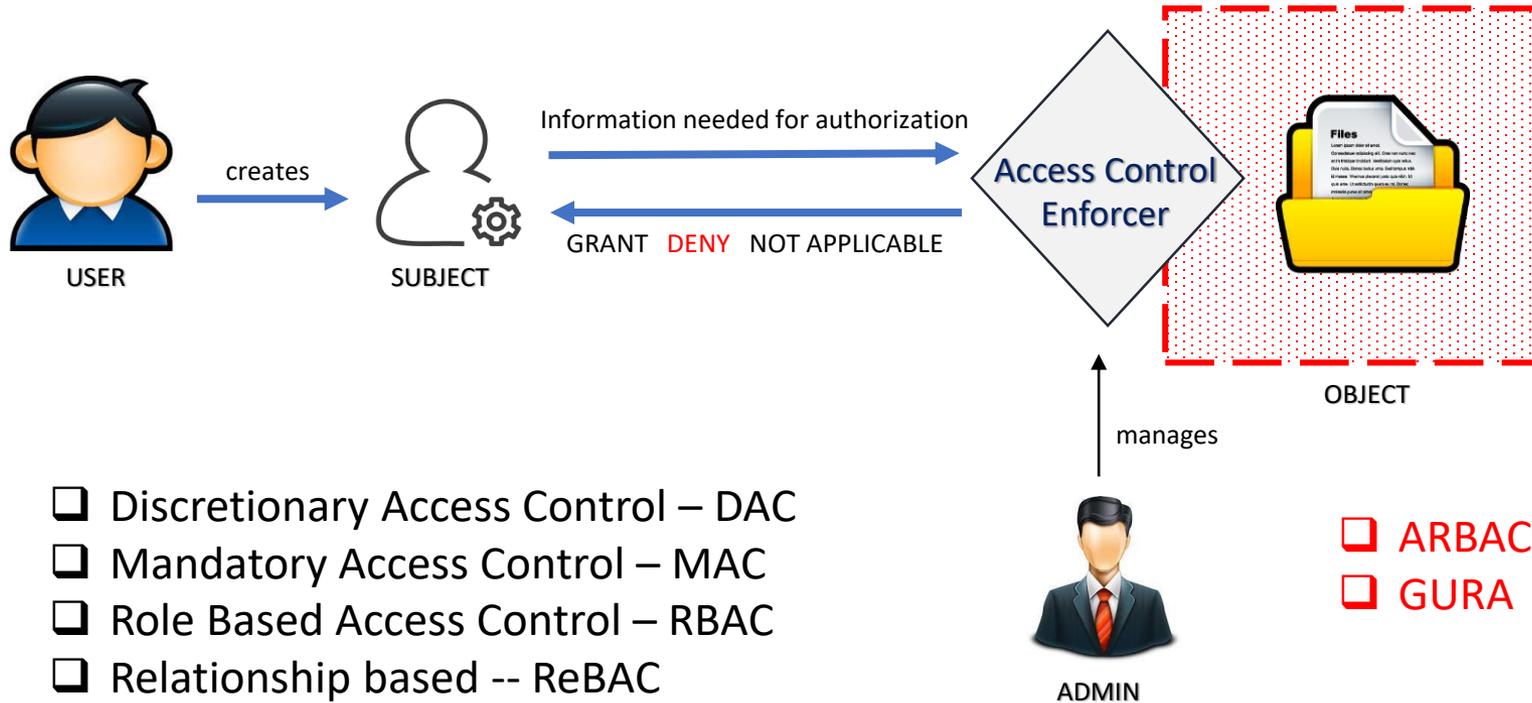
Institute for Cyber Security,
Department of Computer Science
The University of Texas at San Antonio

Committee:

Ravi Sandhu, Ph.D. (Advisor and Chair)
Murtuza Jadliwala, Ph.D.
Palden Lama, Ph.D.
Gregory B. White, Ph.D.
Ram Krishnan, Ph.D.

November 27, 2018

- Introduction and Motivation
- Group Based Attributes Administration and Analysis
- Access Control for Smart Cars
 - ❖ Extended ACO Architecture
 - ❖ Authorization Framework
 - ❖ Dynamic Groups and ABAC
- Big Data Security in Hadoop
 - ❖ Family of Access Control Models
 - ❖ HeAC, OT-RBAC, and HeABAC Model
- Conclusion and Future Work



- ARBAC97
- GURA

- Discretionary Access Control – DAC
- Mandatory Access Control – MAC
- Role Based Access Control – RBAC
- Relationship based -- ReBAC
- Attribute based -- ABAC
-
-
-

➤ Problem Statement

New and emerging technologies such as smart connected cars and multi-tenant big data platforms require innovative access control models.

➤ Thesis Statement

The established paradigms of role-based and attribute-based access control can be adapted and extended to provide fine-grained and dynamic authorization for cloud assisted smart cars and Hadoop big data framework.

Secure Cloud Assisted Smart Cars and Big Data: Access Control Models and Implementation

Group Based Attributes
Administration and
Analysis

Access Control
for Smart Cars

Big Data
Security in
Hadoop

GURAG
Administrative
Model

Reachability
Analysis

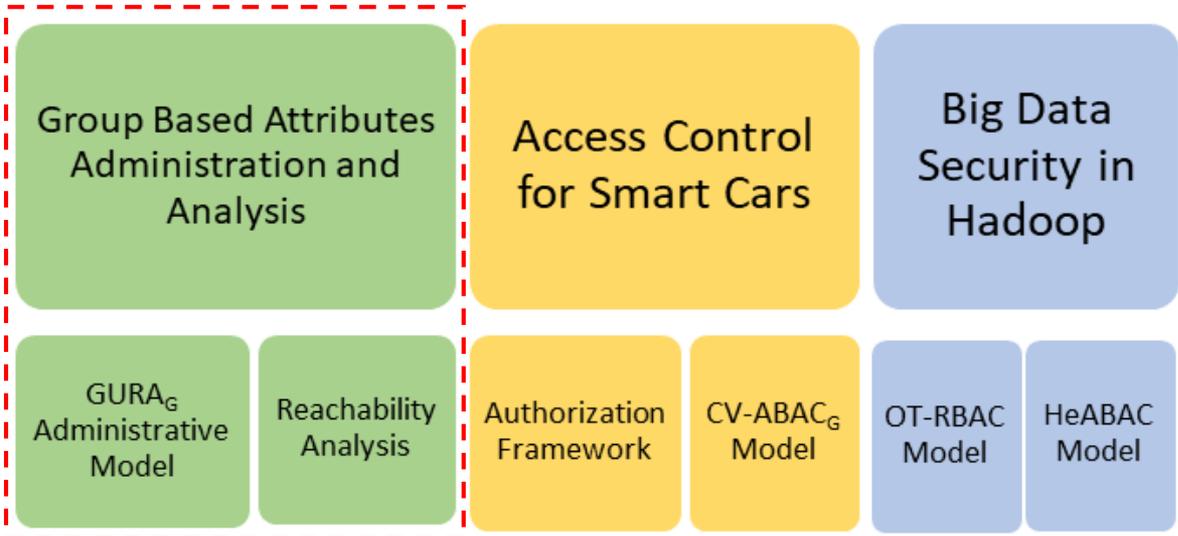
Authorization
Framework

CV-ABAC_G
Model

OT-RBAC
Model

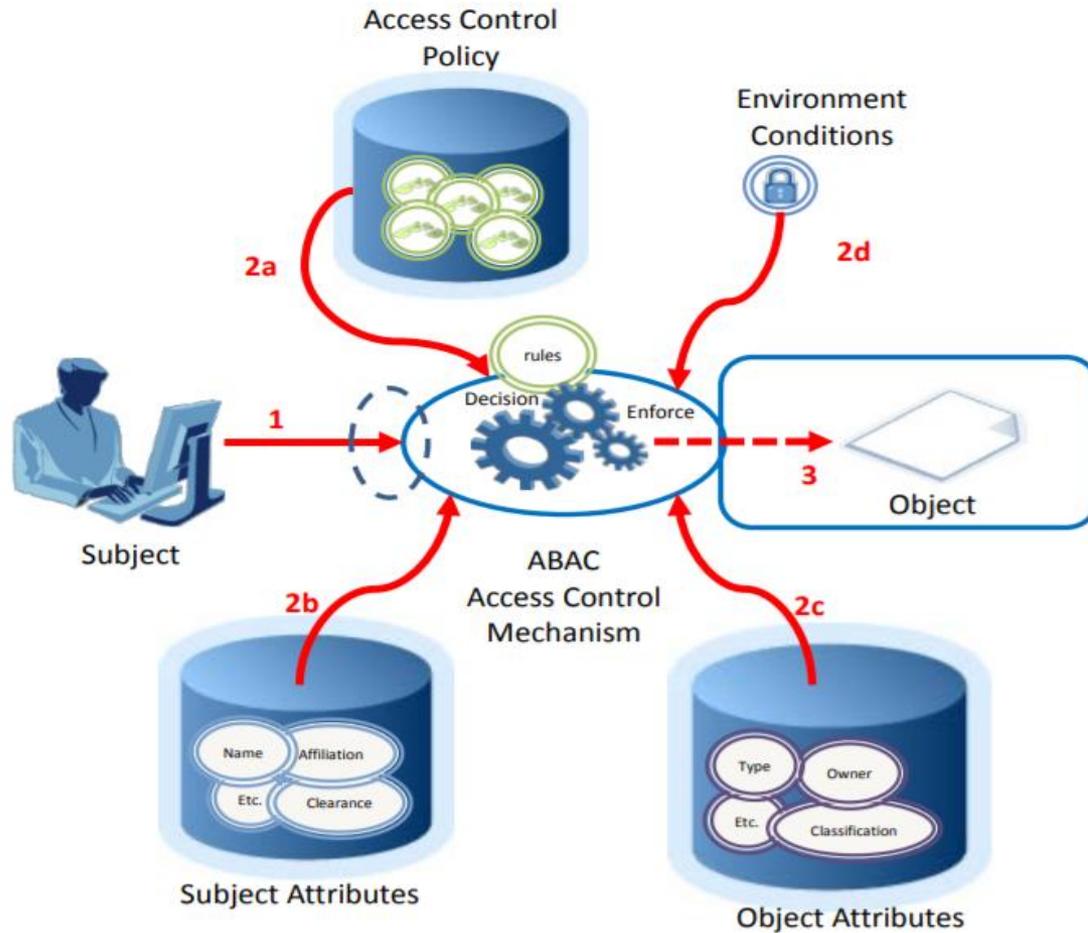
HeABAC
Model

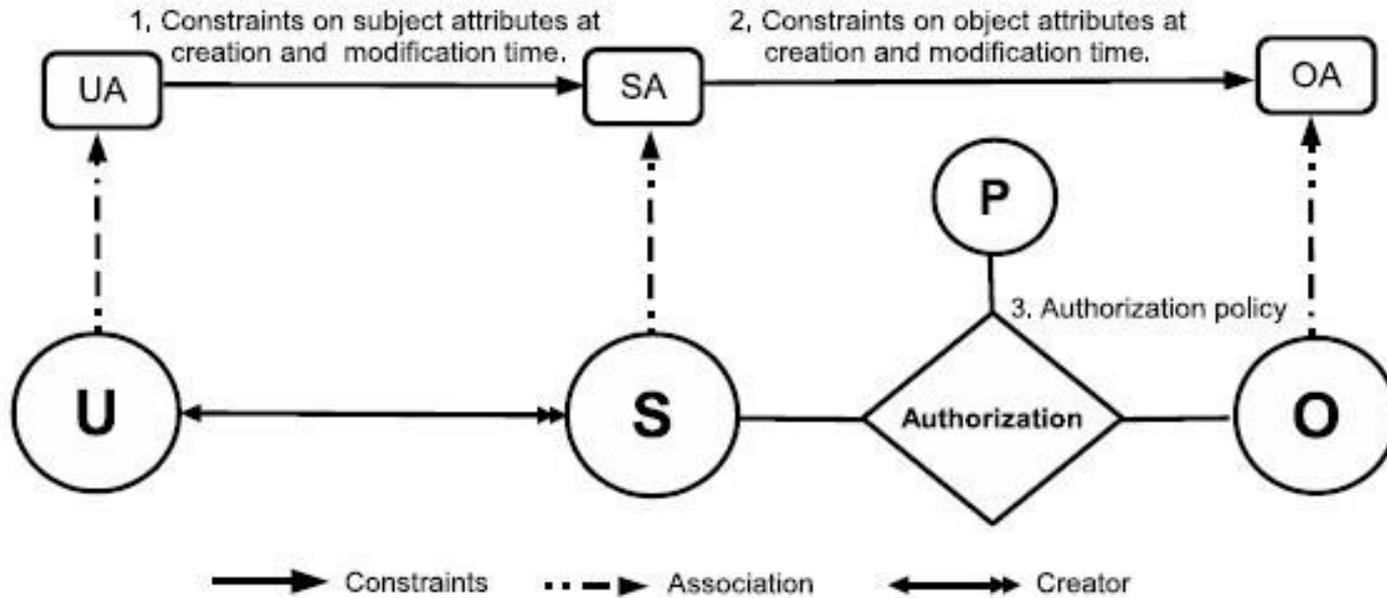
Secure Cloud Assisted Smart Cars and Big Data:
Access Control Models and Implementation



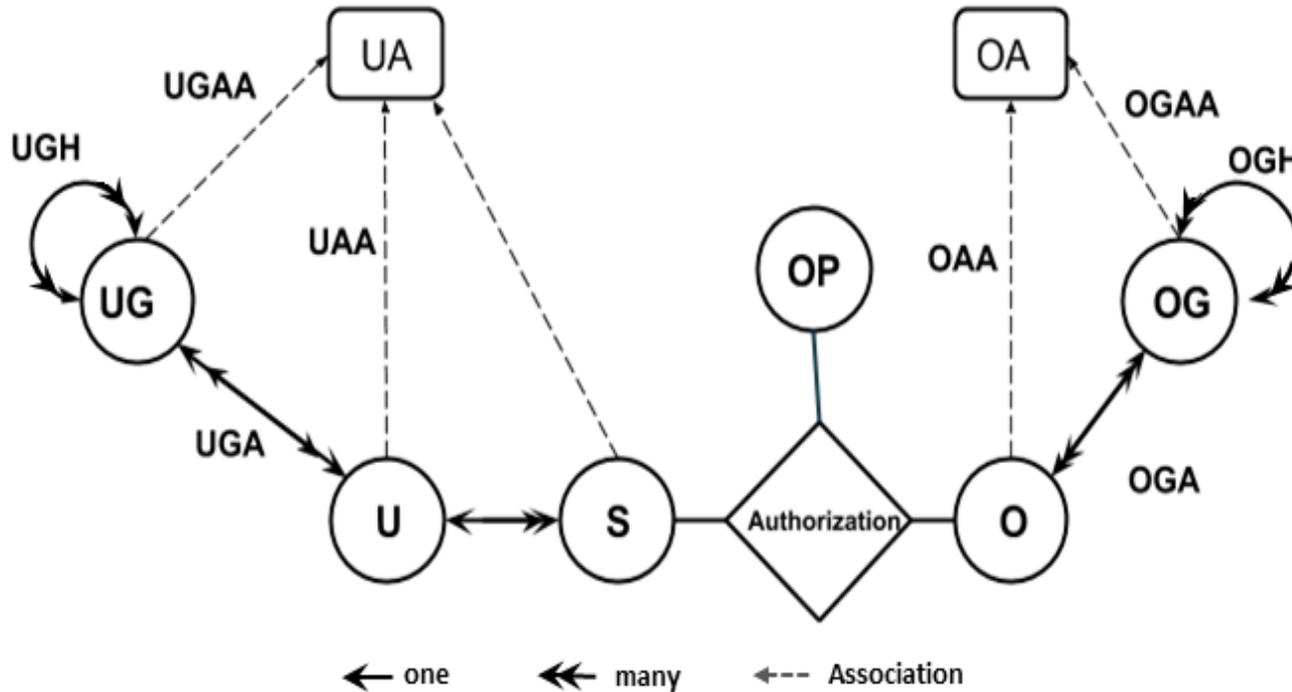
Group Based Attributes Administration and Analysis

1. **Maanak Gupta** and Ravi Sandhu, “The GURAG Administrative Model for User and Group Attribute Assignment.” In Proceedings of the 10th International Conference on Network and System Security (NSS), Taipei, Taiwan, September 28-30, 2016, pages 318-332.
2. **Maanak Gupta** and Ravi Sandhu, “Reachability Analysis for Role-Based Administration of Group and User Attributes.” To be submitted to IEEE Trans. on Dependable and Secure Computing.





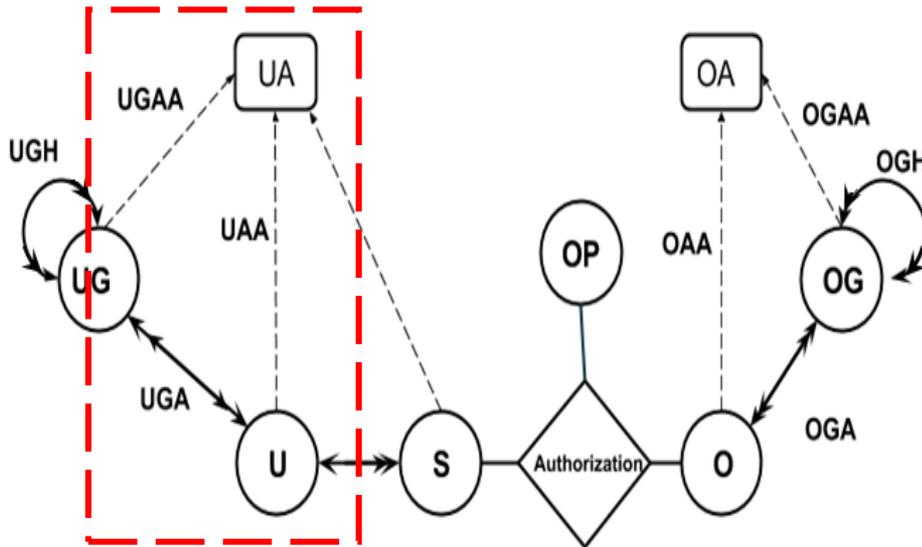
Can be configured to do simple forms of DAC, MAC, RBAC
(Jin, Krishnan, Sandhu 2012)



➤ Hierarchical Group and Attribute Based Access Control (HGABAC)

- ❖ Introduces User and Object Groups
- ❖ Simplifies administration of attributes

Servos and Osborn, 2015



UAA: User Attribute Assignment
 UGAA: User Group Attribute Assignment
 UGA: User to User-Group Assignment

Administrative Relations

- User Attribute Assignment (**UAA**) & User-Group Attribute Assignment (**UGAA**):
For each att_u in UA,

$$\text{canAdd}_{att_u} \subseteq AR \times \text{EXPR}(UA) \times 2^{\text{Range}(att_u)}$$

$$\text{canDelete}_{att_u} \subseteq AR \times \text{EXPR}(UA) \times 2^{\text{Range}(att_u)}$$

- User to User-Group Assignment (**UGA**):

$$\text{canAssign} \subseteq AR \times \text{EXPR}(UA \cup UG) \times 2^{UG}$$

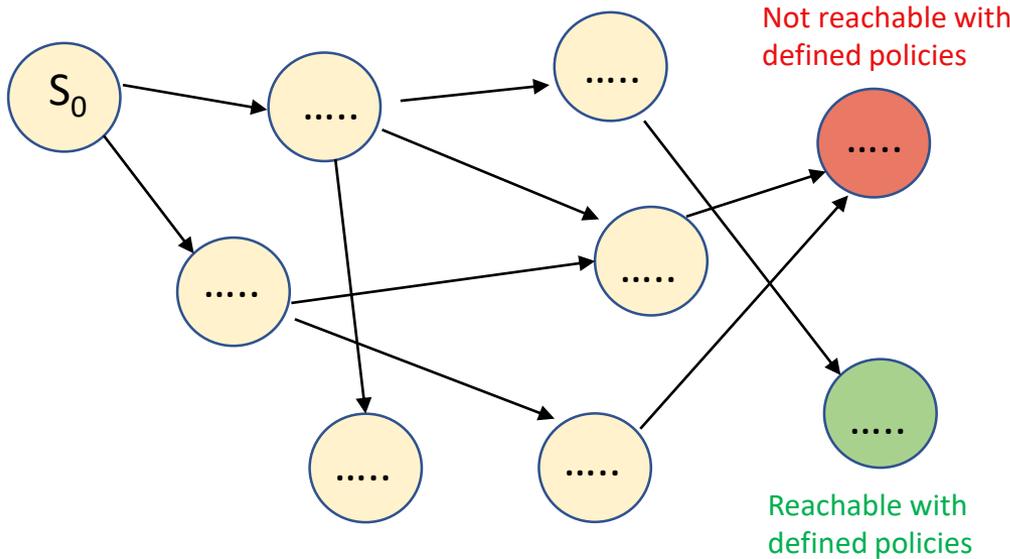
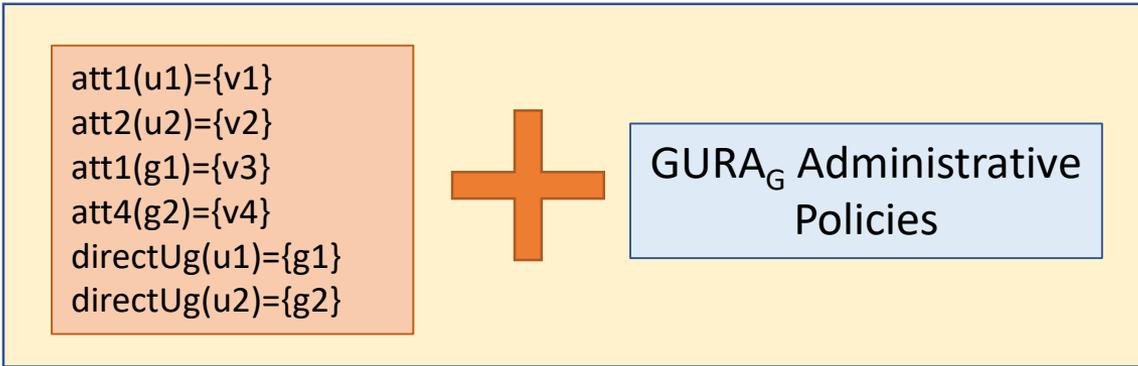
$$\text{canRemove} \subseteq AR \times \text{EXPR}(UA \cup UG) \times 2^{UG}$$

❑ Administrators request to

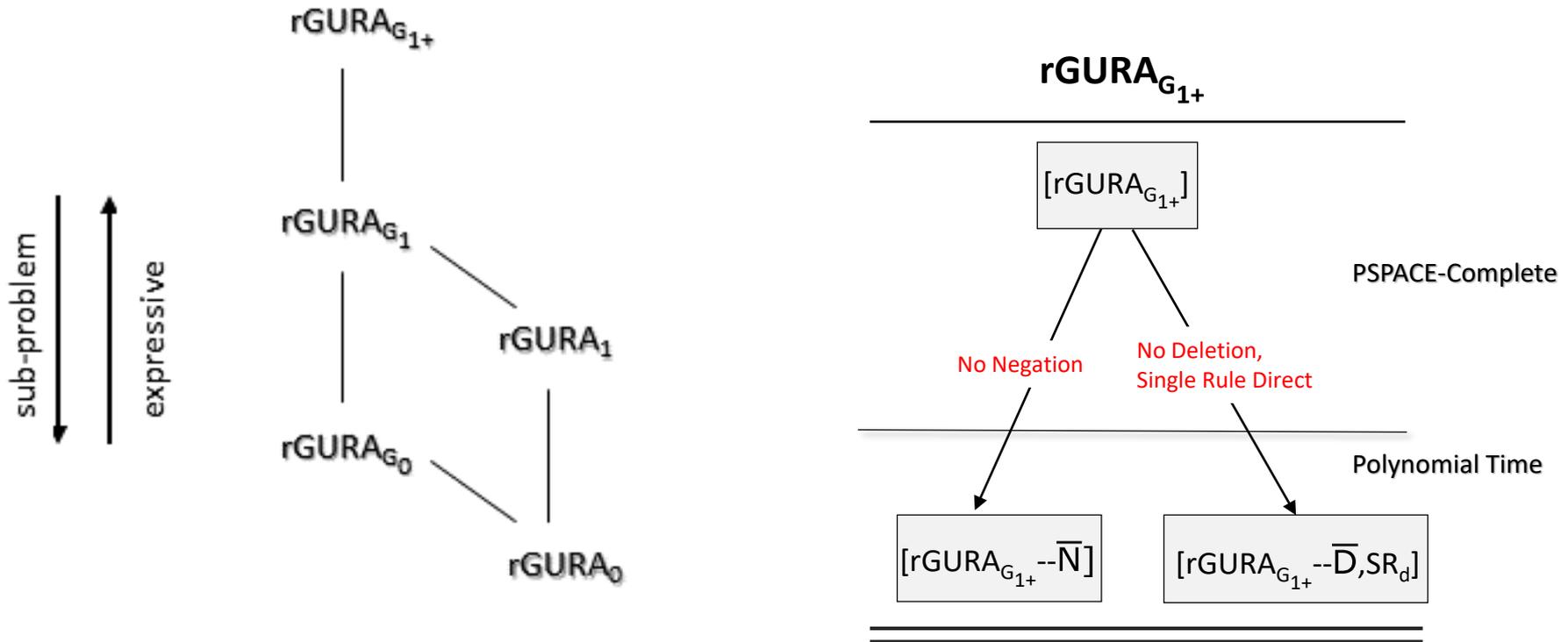
- **add** or **delete** attributes of users
- **add** or **delete** attributes of user groups
- **assign** or **remove** users from user groups

❑ Administrative Policies

- UAA -- Administrative users with [**administrative roles**] can [**modify**] value [**value**] to [**attribute name**] attribute of a user if [**condition**].
- UGAA -- Administrative users with [**administrative roles**] can [**modify**] value [**value**] to [**attribute name**] attribute of a user groups if [**condition**].
- UGA -- Administrative users with [**administrative roles**] can [**modify**] membership in user-group [**group name**] of a user if [**condition**].

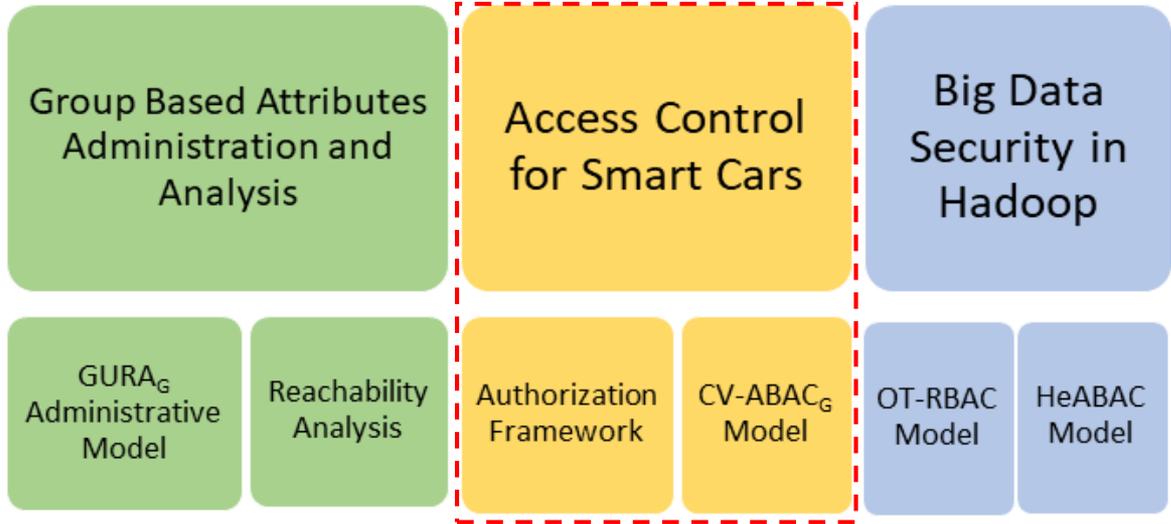


If there exists a state where user **u1** have effective values for **att1** contain **x** and for **att2** is equal to **y**?



- ❑ $rGURAG$ is different from $GURAG$ only in **condition** specification language in rules.
- ❑ Only **conjunction** and **negation** is allowed.

Secure Cloud Assisted Smart Cars and Big Data: Access Control Models and Implementation

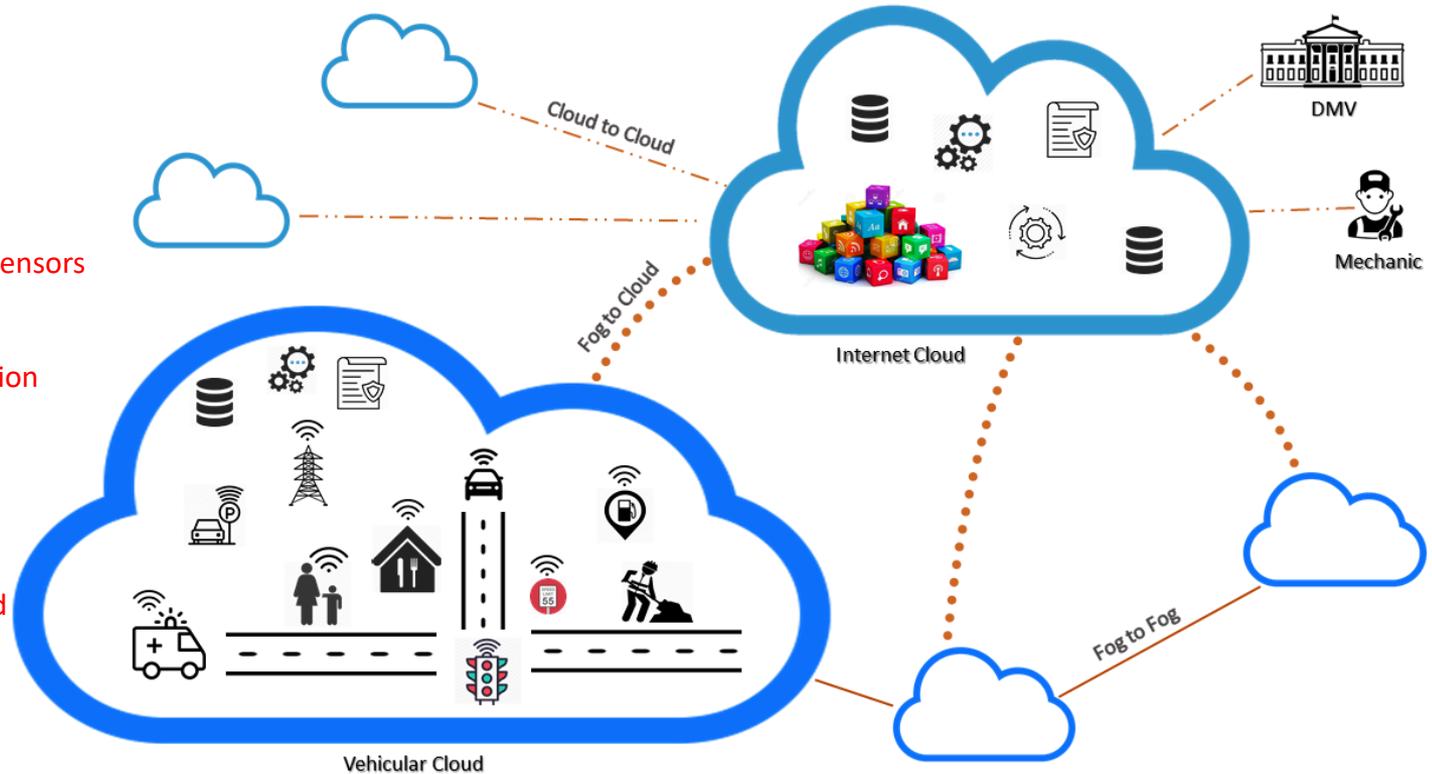


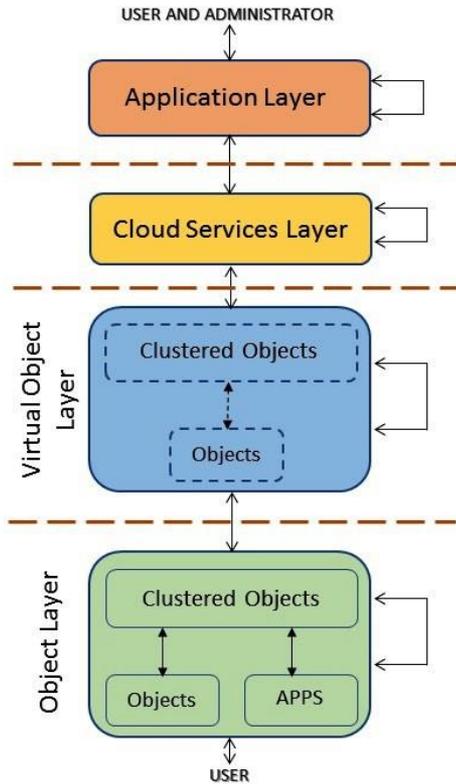
Access Control for Smart Cars

1. **Maanak Gupta** and Ravi Sandhu, “Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things.” In Proceedings of the 23rd ACM Symposium on Access Control Models and Technologies (SACMAT), Indianapolis, Indiana, June 13-15, 2018, pages 193-204.
2. **Maanak Gupta**, James Benson, Farhan Patwa, and Ravi Sandhu, “Dynamic Groups and Attribute Based Access Control for Next Generation Smart Cars.” (To Appear) In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY), Dallas, Texas, Mar 25-27, 2019.

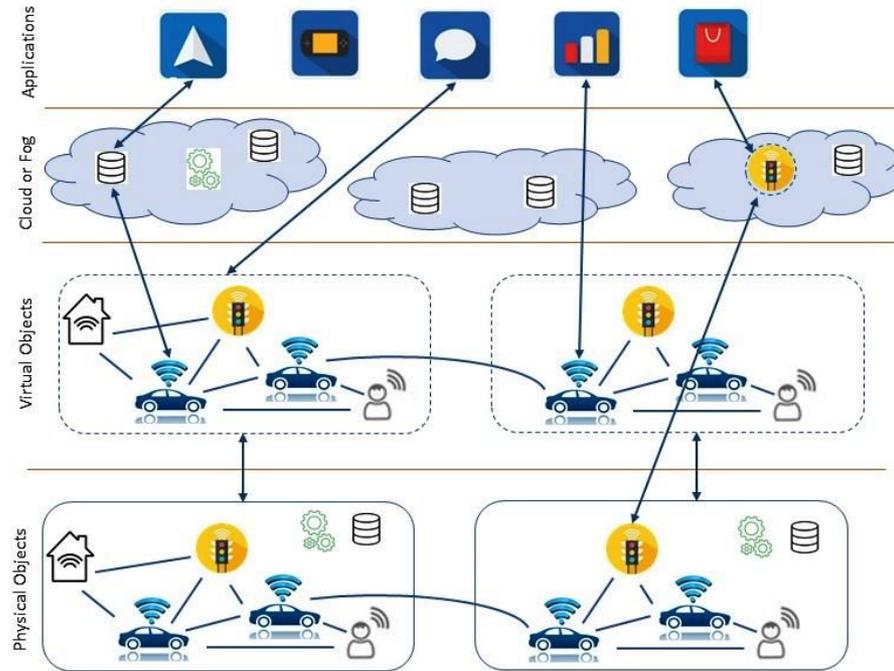


- On-Board Application and Sensors
- Over the Air updates
- V2X fake messages
- In-vehicle ECU communication
- Personal Data
- Third Party devices
- User Privacy Preferences
- Spoofing, Ransomware, Injection...
- Loss of Information in Cloud

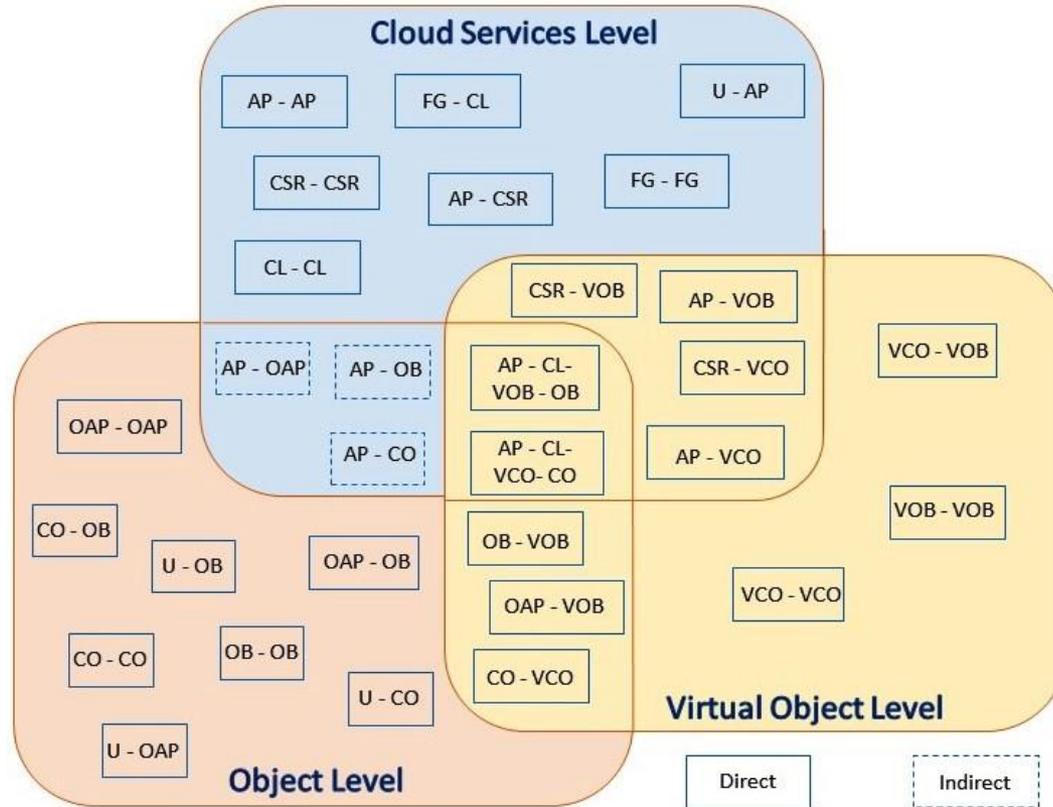




a) Extended ACO Architecture for Connected Car and IoV

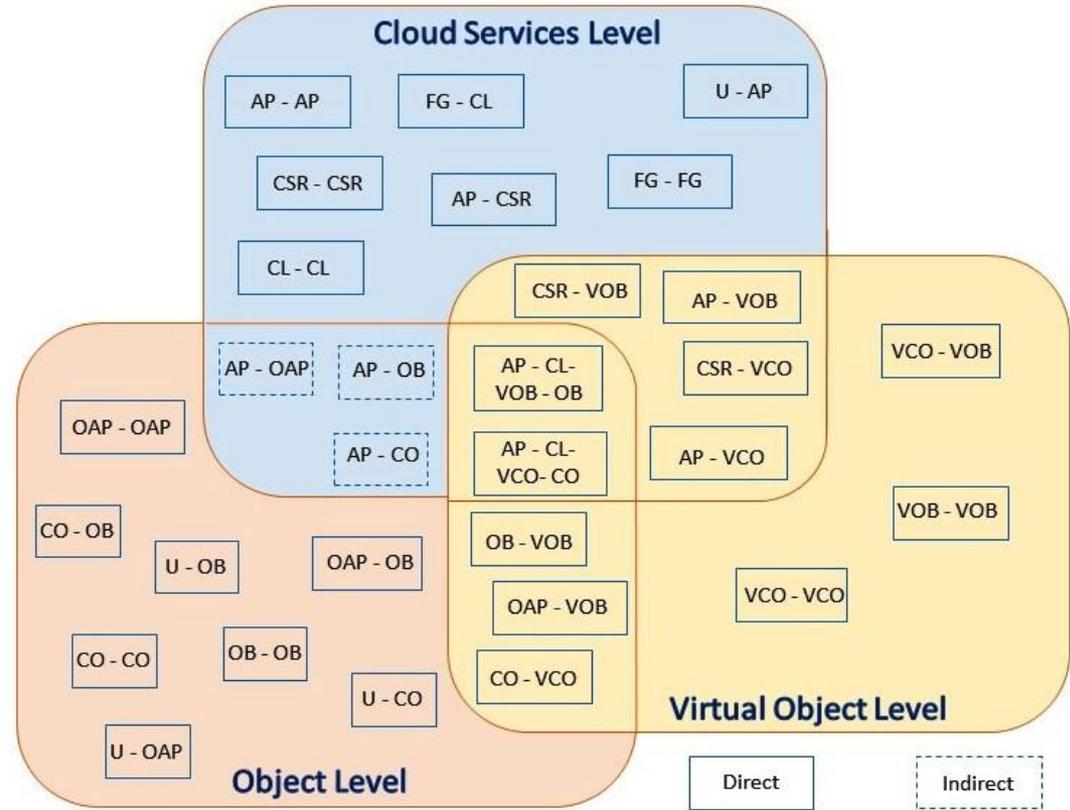


b) Connected Car and Vehicular IoT Components in Extended ACO Layers

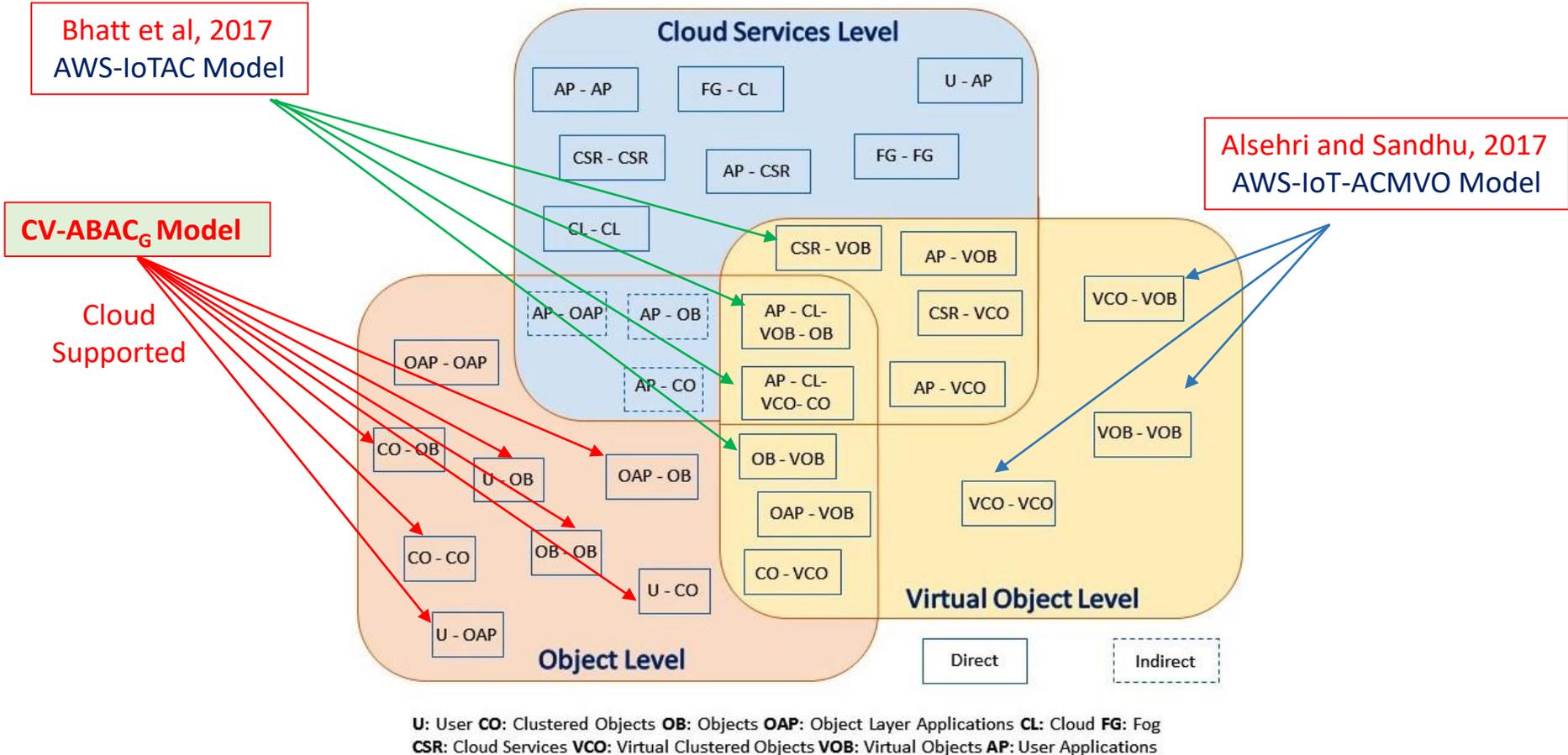


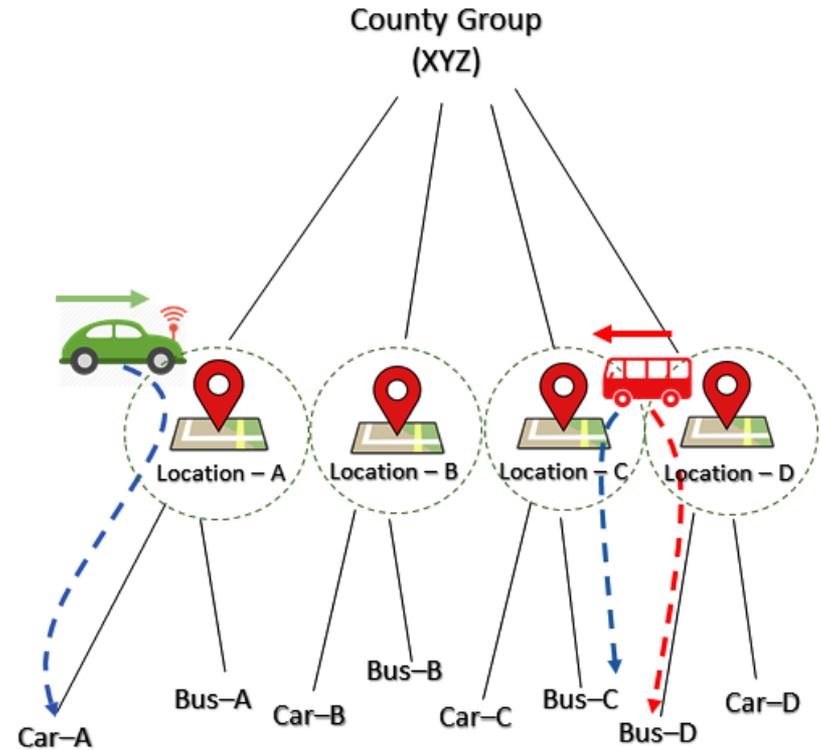
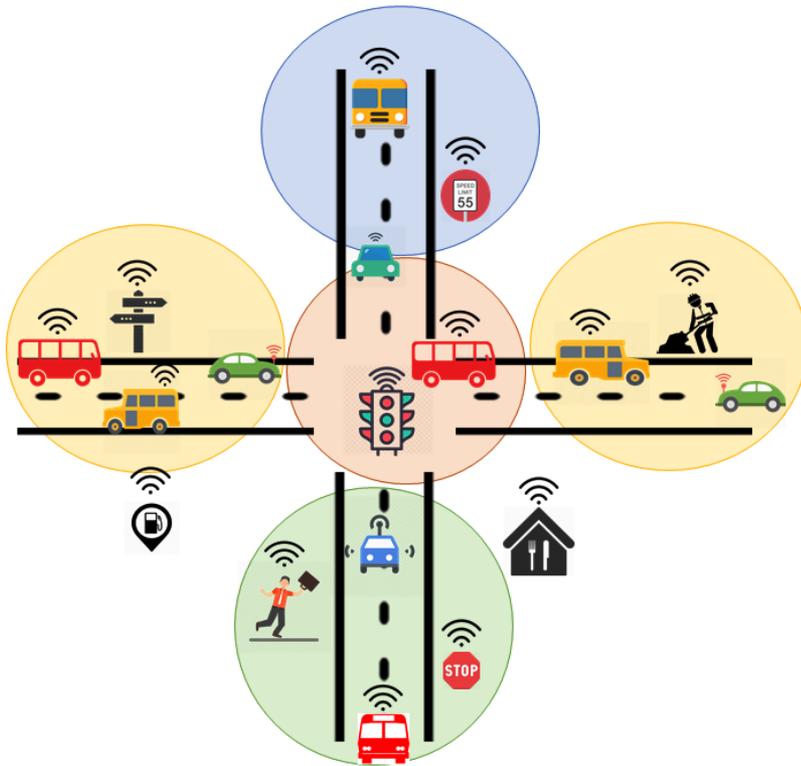
U: User **CO:** Clustered Objects **OB:** Objects **OAP:** Object Layer Applications **CL:** Cloud **FG:** Fog
CSR: Cloud Services **VCO:** Virtual Clustered Objects **VOB:** Virtual Objects **AP:** User Applications

- Static vs Dynamic
- What kind of relationship they have?
 - Owner, Manufacturer, Friend...
- Multi-Layered
- Groups Based
- Trusted Interaction
 - How I trust you?
 - Previous interaction..?
- ABAC, ReBAC Models
- Who will administer?
- Data in Cloud, cross cloud sharing. How?

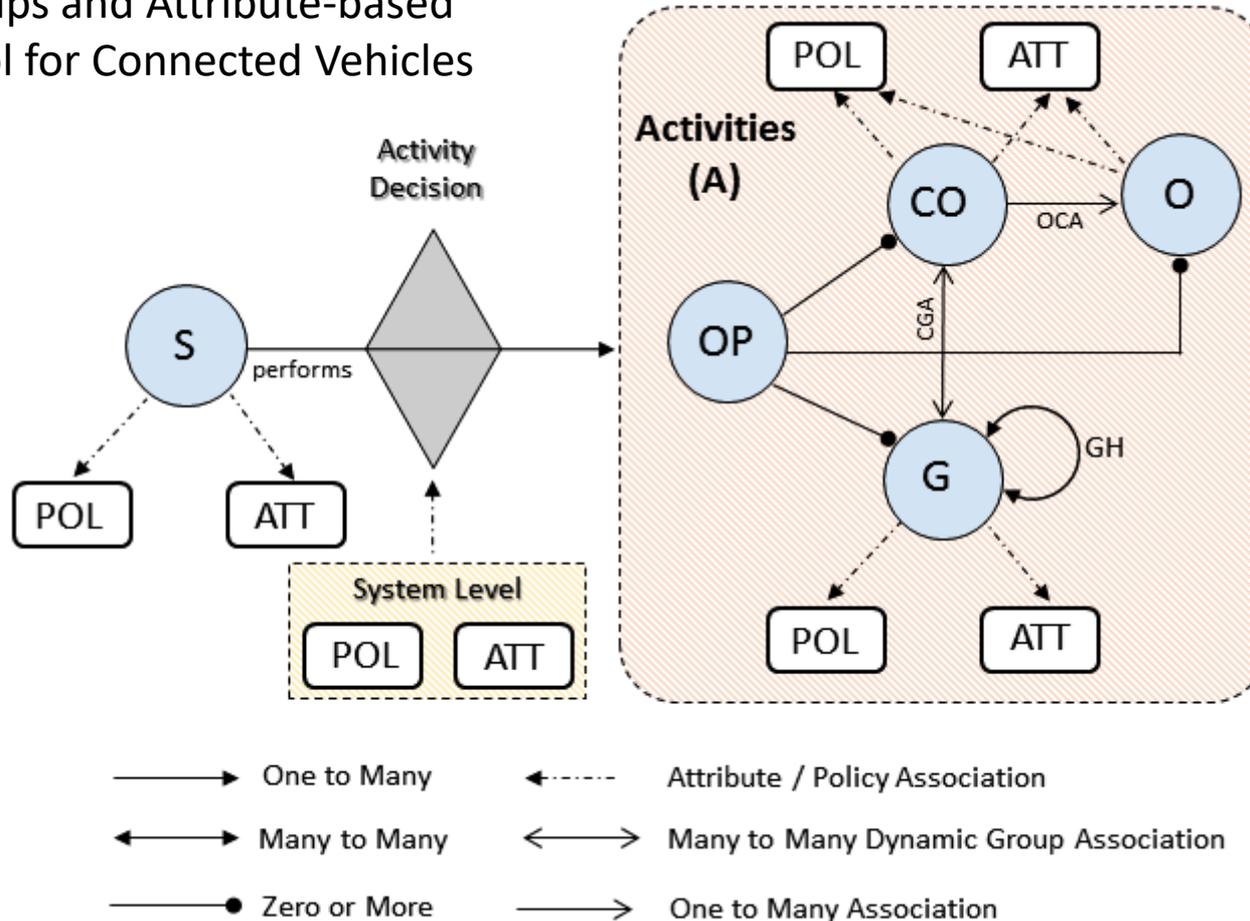


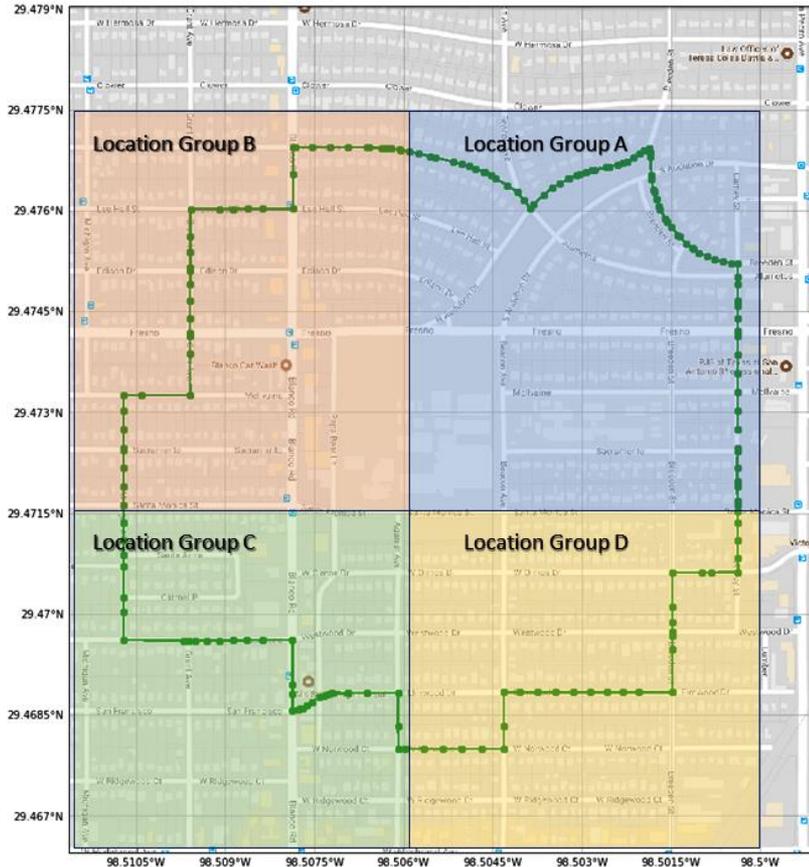
U: User **CO:** Clustered Objects **OB:** Objects **OAP:** Object Layer Applications **CL:** Cloud **FG:** Fog
CSR: Cloud Services **VCO:** Virtual Clustered Objects **VOB:** Virtual Objects **AP:** User Applications





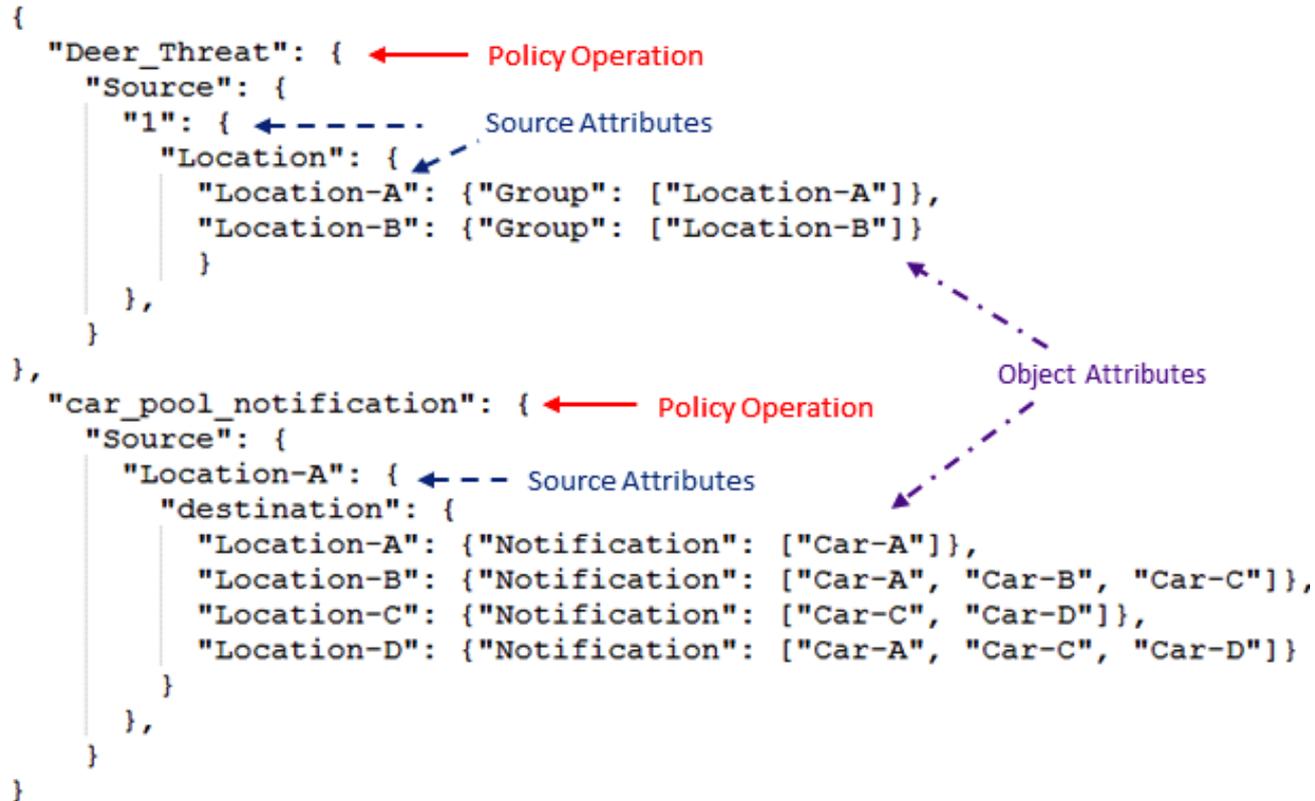
Dynamic Groups and Attribute-based Access Control for Connected Vehicles

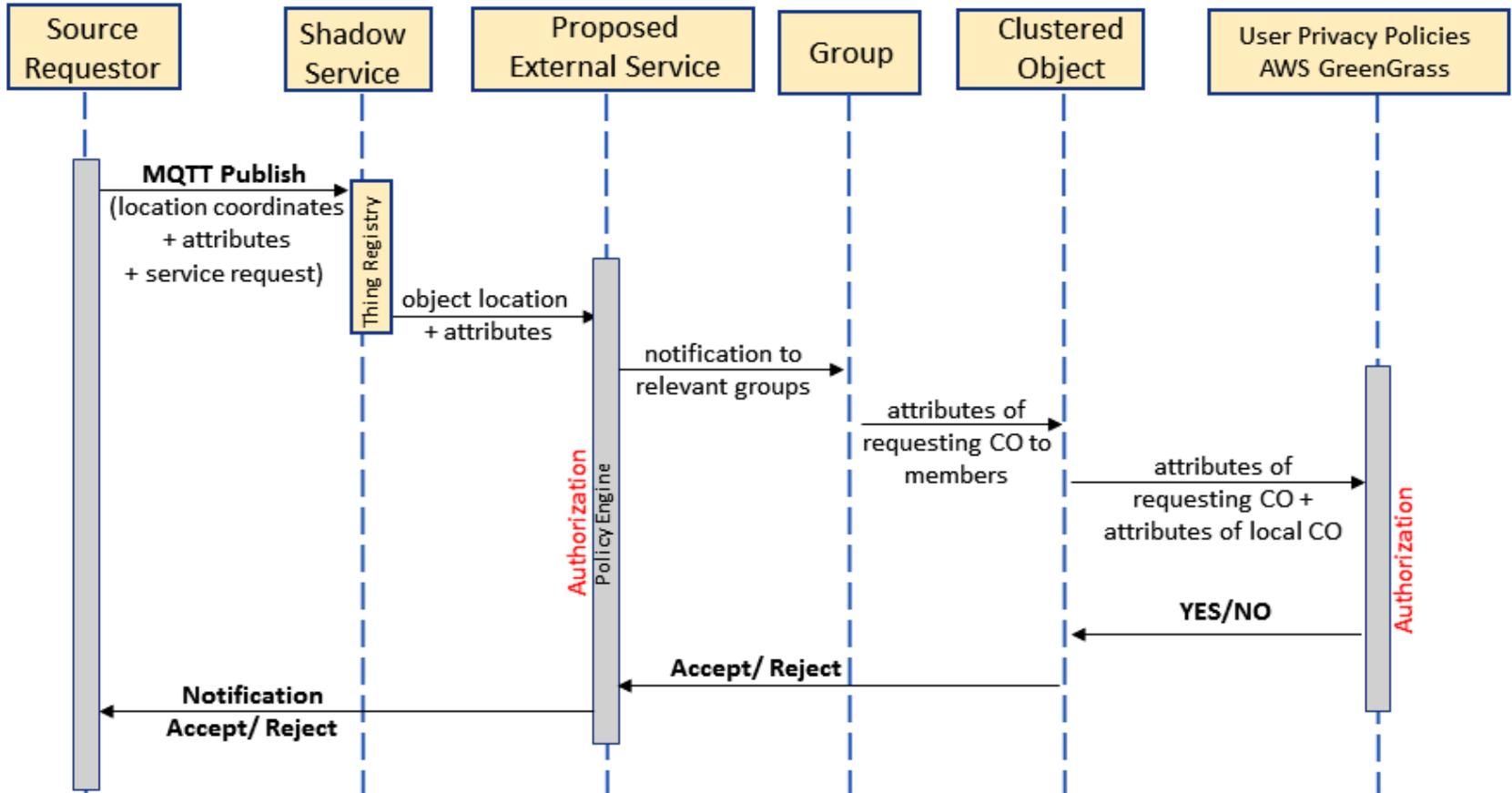




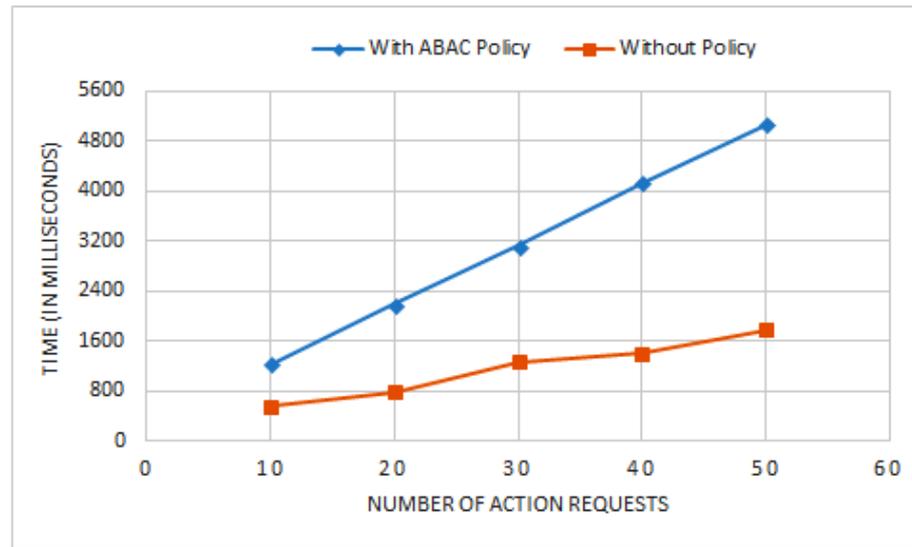
```

('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']
  
```

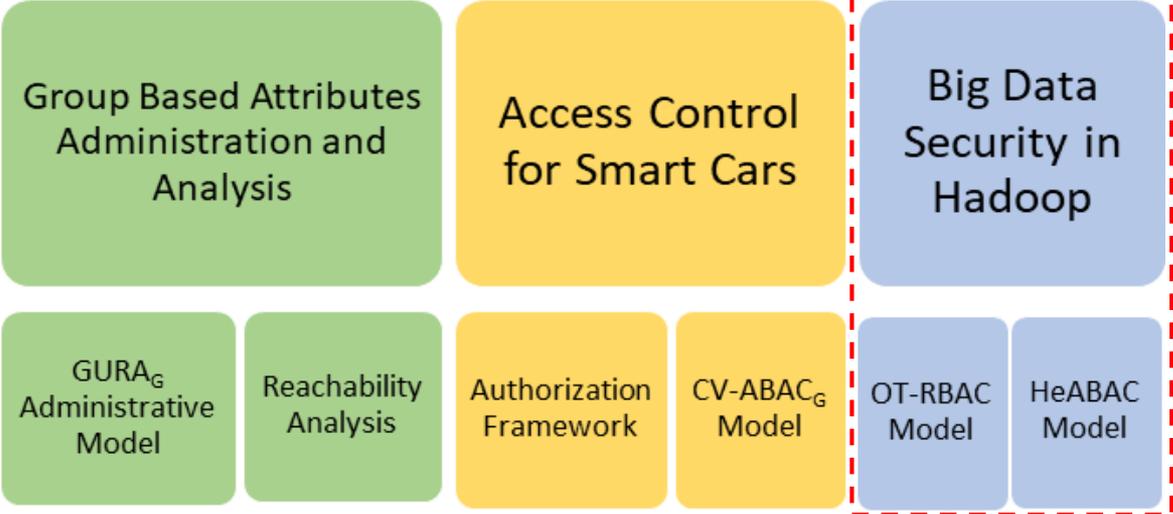




Number of Requests	Policy Enforcer Execution Time (in ms)	Cars Notified		
		nth Request	With ABAC Policy	Without Policy
10	0.0501	41st	2	5
20	0.1011	42nd	3	5
30	0.1264	43rd	5	5
40	0.1630	44th	3	5
50	0.1999	45th	2	5
		46th	3	5

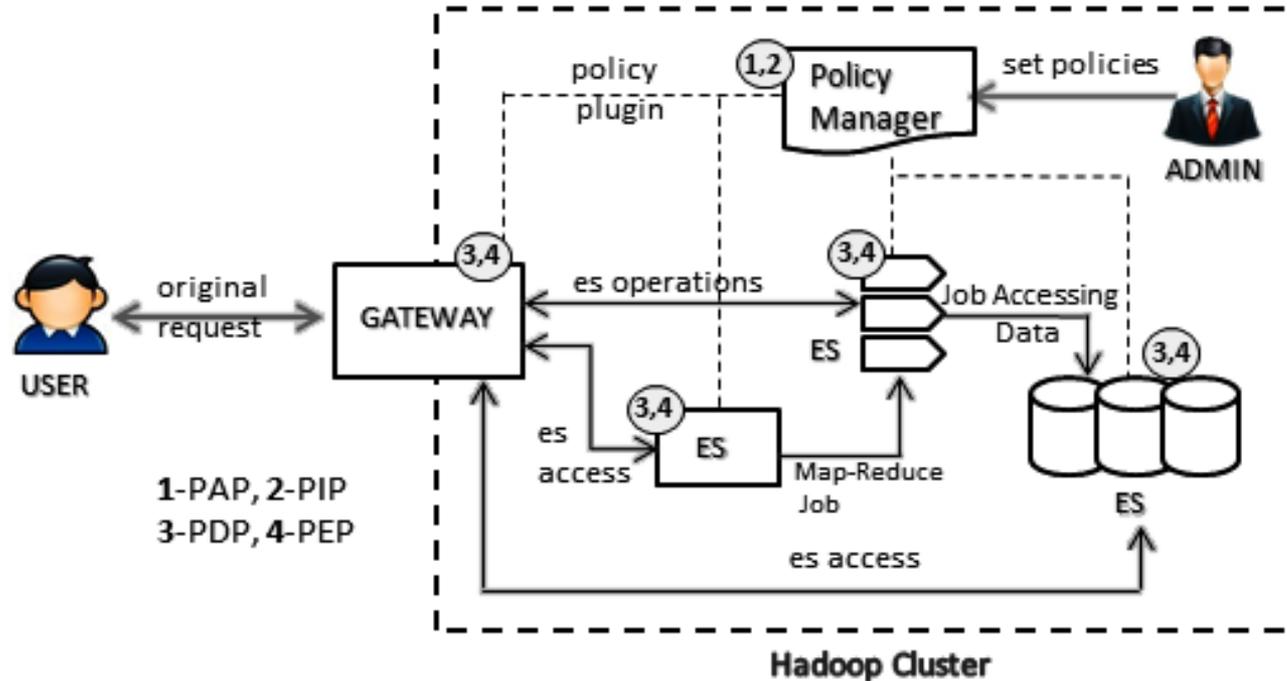


Secure Cloud Assisted Smart Cars and Big Data:
Access Control Models and Implementation



Big Data Security in Hadoop

1. **Maanak Gupta**, Farhan Patwa and Ravi Sandhu, “An Attribute-Based Access Control Model for Secure Big Data Processing in Hadoop Ecosystem.” In Proceedings of the 3rd ACM Workshop on Attribute-Based Access Control (ABAC), March 19-21, 2018, Tempe, Arizona, pages 13-24.
2. **Maanak Gupta**, Farhan Patwa and Ravi Sandhu, “Object-Tagged RBAC Model for the Hadoop Ecosystem.” In Proceedings of the 31st Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec), Philadelphia, Pennsylvania, July 19-21, 2017, pages 63-81.
3. **Maanak Gupta**, Farhan Patwa, James Benson and Ravi Sandhu, “Multi-Layer Authorization Framework for a Representative Hadoop Ecosystem Deployment.” In Proceedings of the 22nd ACM Symposium on Access Control Models and Technologies (SACMAT), Indianapolis, Indiana, June 21-23, 2017, pages 183-190.



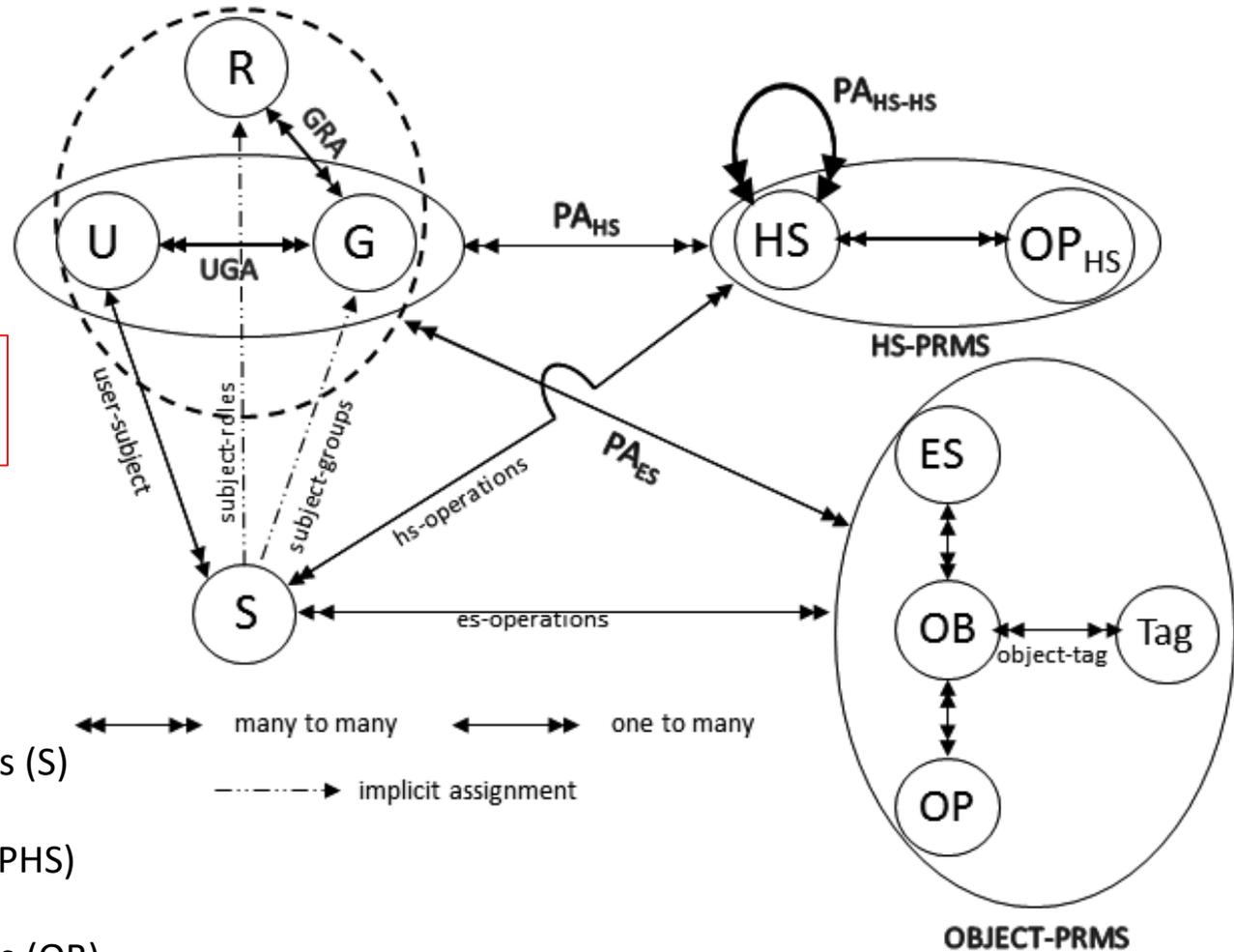
Policy Manager : Apache Ranger, Apache Sentry

Gateway : Apache Knox

Ecosystem Service (ES) : Apache Hive, HDFS, Apache Storm, Apache Kafka, YARN

Hadoop Ecosystem Access Control Model

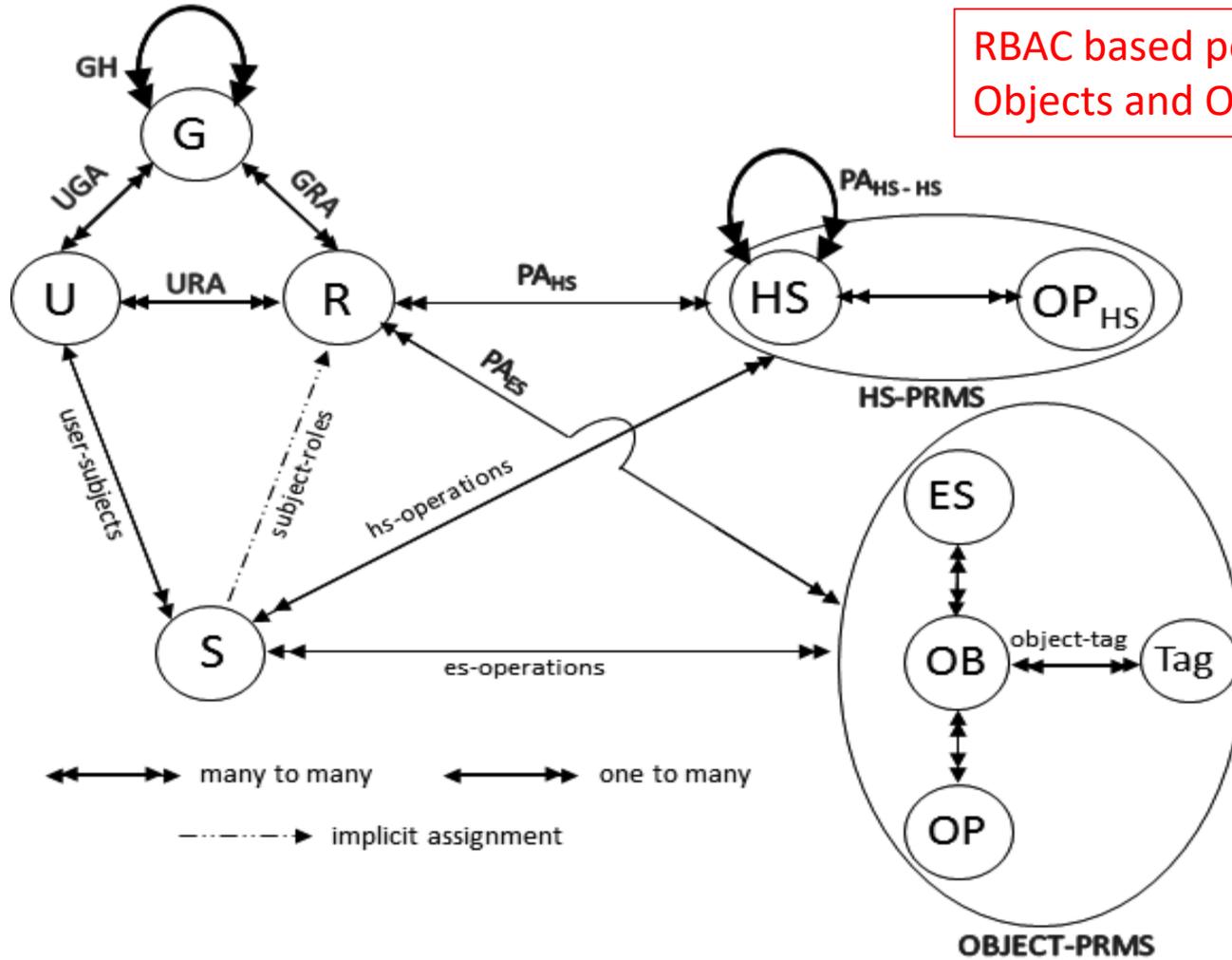
ACLs based permissions on
Objects and Object-Tags



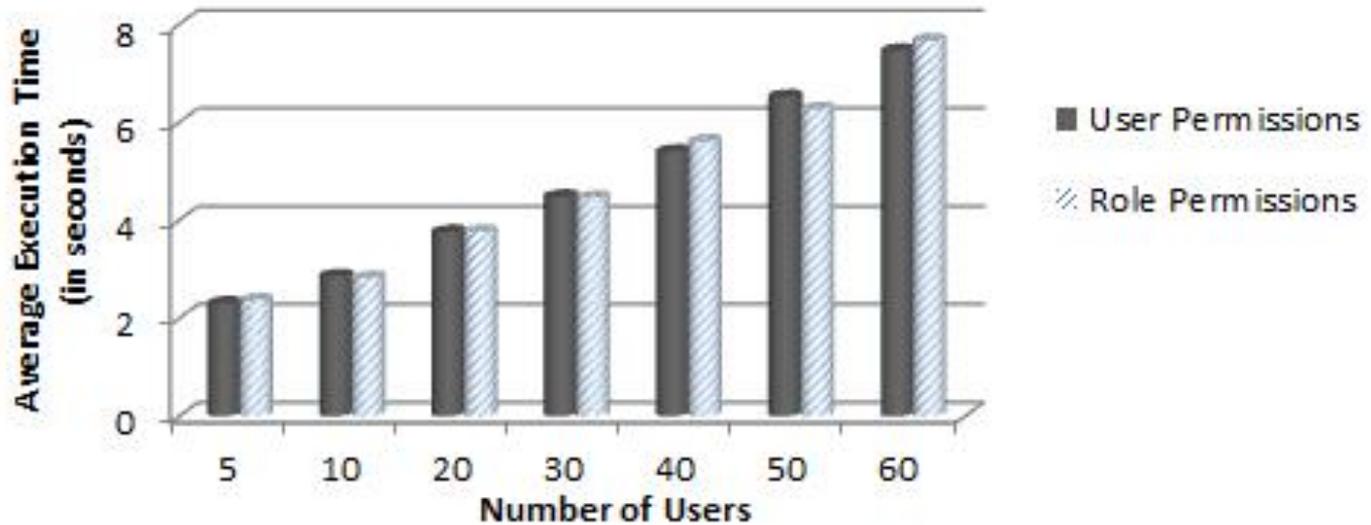
Users (U), Groups (G) , Subjects (S)
Hadoop Services (HS)
Hadoop Service Operations (OPHS)
Objects (OB), Operations (OP)
Ecosystem Service (ES), Objects (OB)
Operations (OP), Tag

Object-Tagged RBAC

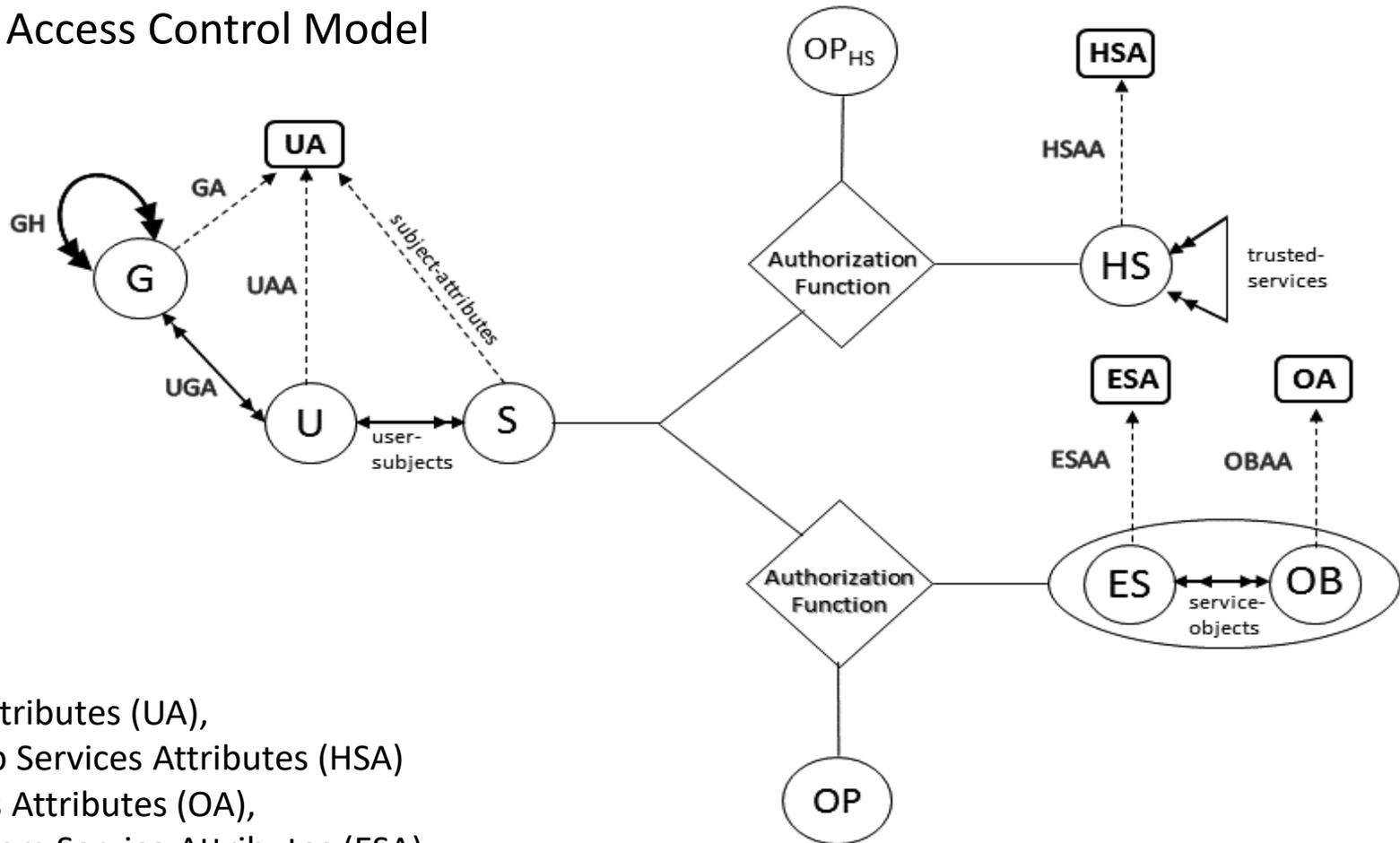
RBAC based permissions on Objects and Object-Tags



Comparing access request execution time



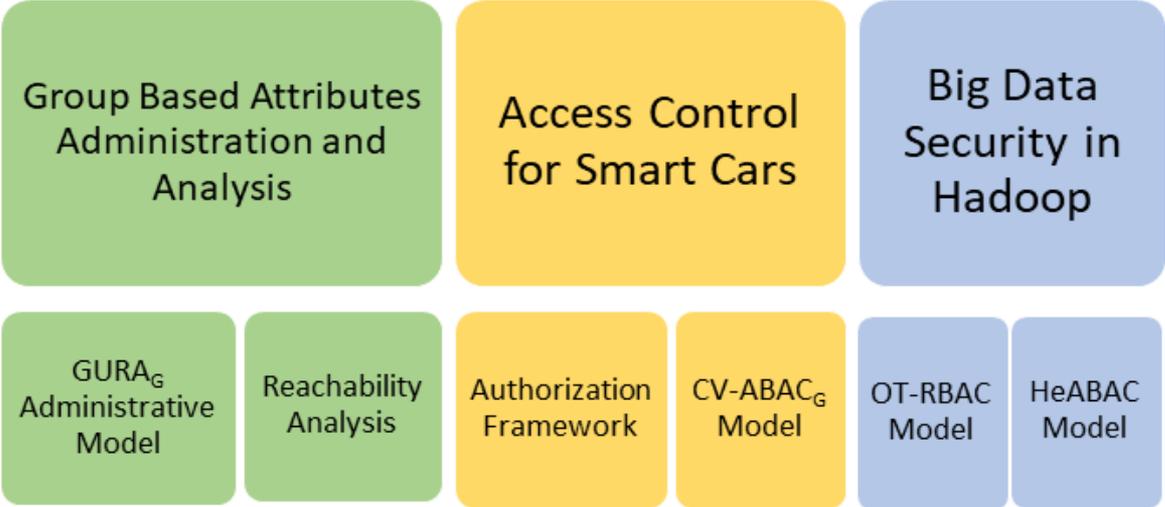
Hadoop Ecosystem Attribute-Based Access Control Model



User Attributes (UA),
Hadoop Services Attributes (HSA)
Objects Attributes (OA),
Ecosystem Service Attributes (ESA)

1. Authorization_{access}(s:S, es:ES) \equiv diagnostic \in effective_{department}(s) \wedge technician \in effective_{role}(s) \wedge serviceType(es) = HIVE \wedge createdBy(es) = admin1.
2. Authorization_{select}(s:S, es:ES, ob:OB) \equiv Authorization_{access}(s:S, es:ES) = True \wedge diagnostic \in effective_{department}(s) \wedge effective_{role}(s) \in readerType(ob) \wedge tableType(ob) = sensor-data \wedge car(ob) = FVR1234.
3. Authorization_{access}(s:S, hs:HS) \equiv diagnostic \in effective_{department}(s) \wedge technician \in effective_{role}(s) \wedge serviceType(hs) = DataNode \wedge createdBy(hs) = admin2

Secure Cloud Assisted Smart Cars and Big Data: Access Control Models and Implementation



- ❑ Foundational aspects of groups based ABAC
 - ❑ Administrative Model
 - ❑ Reachability Analysis
- ❑ Access Control Solutions for Smart Cars
 - ❖ Authorization Framework
 - ❖ Dynamic Groups and ABAC
- ❑ Access Control Solutions for Big Data in Hadoop
 - ❖ Family of Models – HeAC, OT-RBAC and HeABAC
- ❑ **Some Future Work Directions**
 - ❖ Trust Based Cloud and Smart Cars Solutions
 - ❖ Location preserving approaches
 - ❖ Data Ingestion Security and privacy concerns
 - ❖ Cloudlet supported Intelligent Transportation

Journal Paper

- **Maanak Gupta** and Ravi Sandhu, “Reachability Analysis for Role-Based Administration of Group and User Attributes.” To be submitted to IEEE Trans. on Dependable and Secure Computing.

Conference Papers

- **Maanak Gupta**, James Benson, Farhan Patwa, and Ravi Sandhu, “Dynamic Groups and Attribute Based Access Control for Next Generation Smart Cars.” (To Appear) In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY), Dallas, Mar 25-27, 2019.
- **Maanak Gupta** and Ravi Sandhu, “Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things.” In Proceedings of the 23rd ACM Symposium on Access Control Models and Technologies (SACMAT), Indianapolis, Indiana, June 13-15, 2018, pages 193-204.
- **Maanak Gupta**, Farhan Patwa and Ravi Sandhu, “An Attribute-Based Access Control Model for Secure Big Data Processing in Hadoop Ecosystem.” In Proceedings of the 3rd ACM Workshop on Attribute-Based Access Control (ABAC), March 19-21, 2018, Tempe, Arizona, pages 13-24.
- **Maanak Gupta**, Farhan Patwa and Ravi Sandhu, “Object-Tagged RBAC Model for the Hadoop Ecosystem.” In Proceedings of the 31st Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec), Philadelphia, Pennsylvania, July 19-21, 2017, pages 63-81.
- **Maanak Gupta**, Farhan Patwa, James Benson and Ravi Sandhu, “Multi-Layer Authorization Framework for a Representative Hadoop Ecosystem Deployment.” In Proceedings of the 22nd ACM Symposium on Access Control Models and Technologies (SACMAT), Indianapolis, Indiana, June 21-23, 2017, pages 183-190.
- **Maanak Gupta** and Ravi Sandhu, “The GURAG Administrative Model for User and Group Attribute Assignment.” In Proceedings of the 10th International Conference on Network and System Security (NSS), Taipei, Taiwan, September 28-30, 2016, pages 318-332.