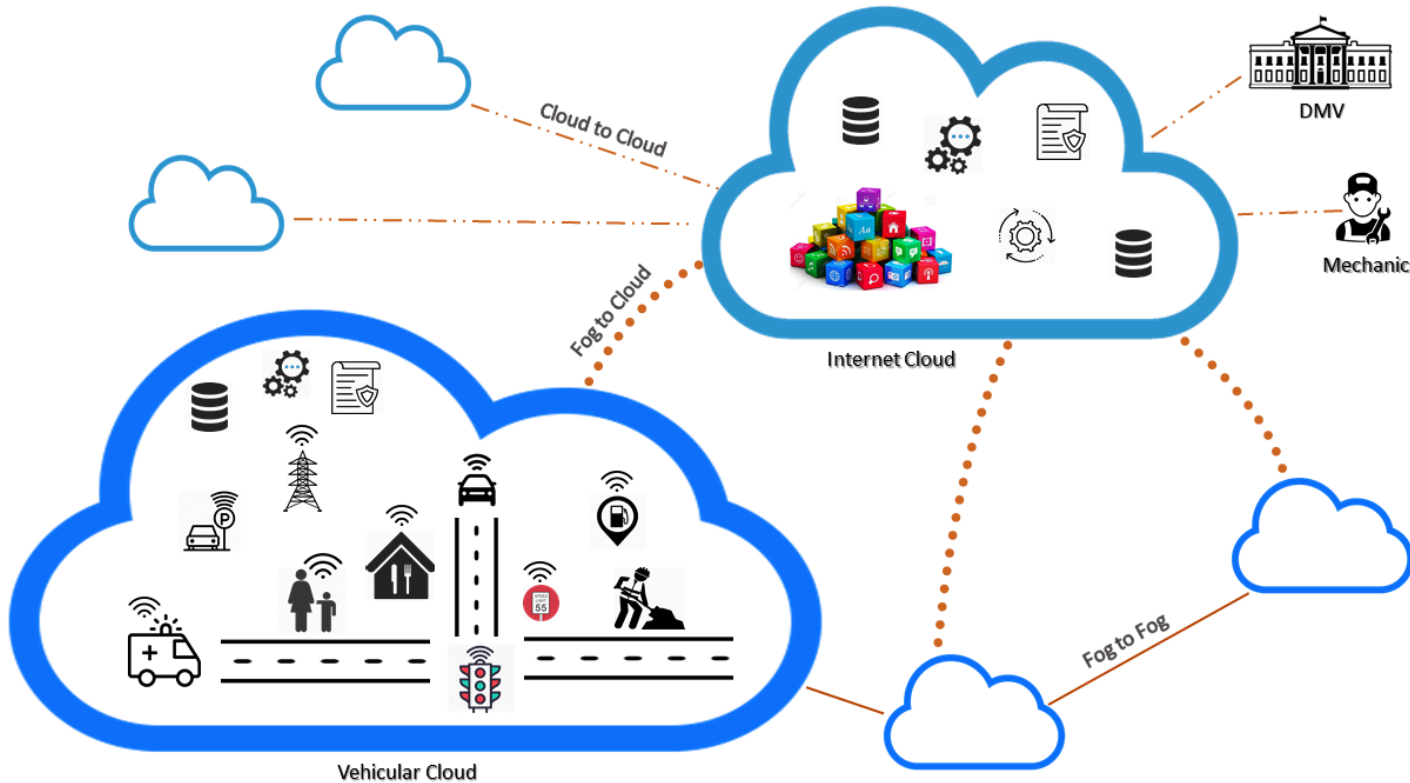


Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things

Maanak Gupta and Ravi Sandhu

Institute for Cyber Security,
Center for Security and Privacy Enhanced Cloud Computing,
Department of Computer Science
University of Texas at San Antonio

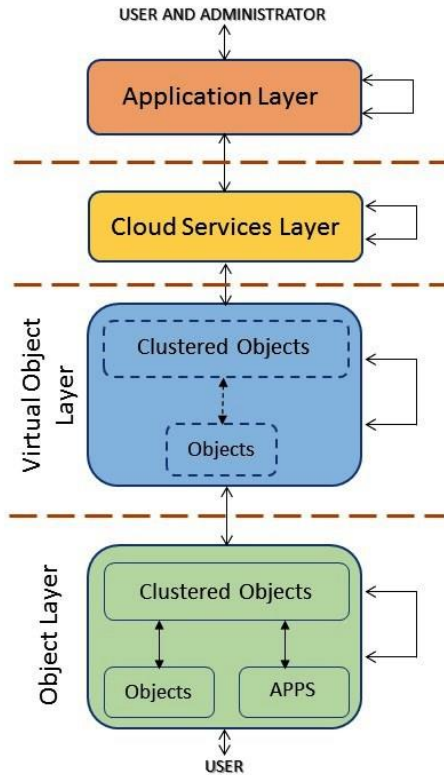
**23rd ACM Symposium on Access Control Models and Technologies
(SACMAT 2018)
Indianapolis, IN, USA, June 13-15, 2018**



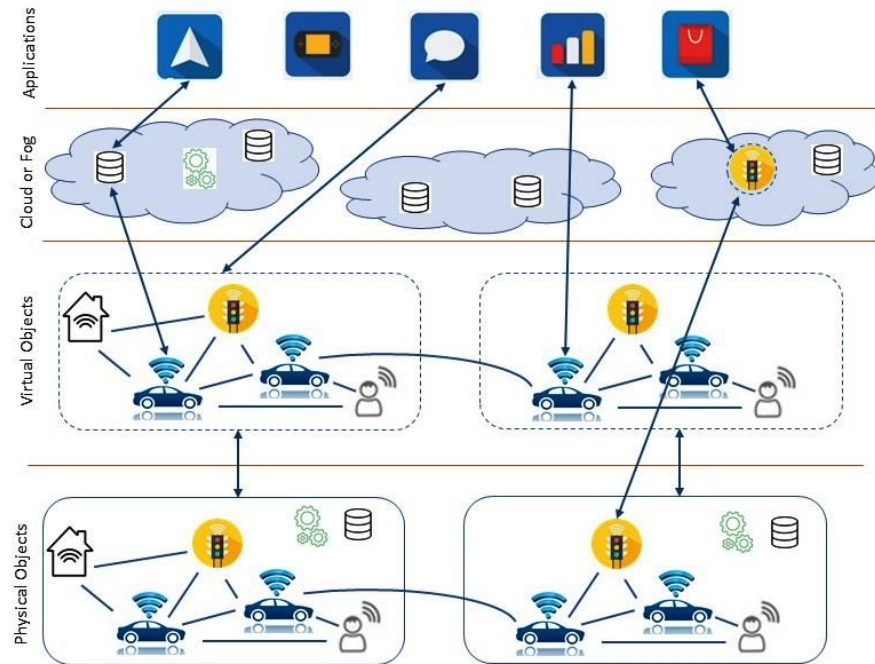
- On-Board Application and Sensors
 - Tesla and Jeep X
- Over the Air updates
- V2X fake messages
- In-vehicle ECU communication
- Personal Data
- Third Party devices
- User Privacy Preferences
- Spoofing, Ransomware, Injection...
- Loss of Information in Cloud

- On-Board Application and Sensors
 - Tesla and Jeep X
- 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

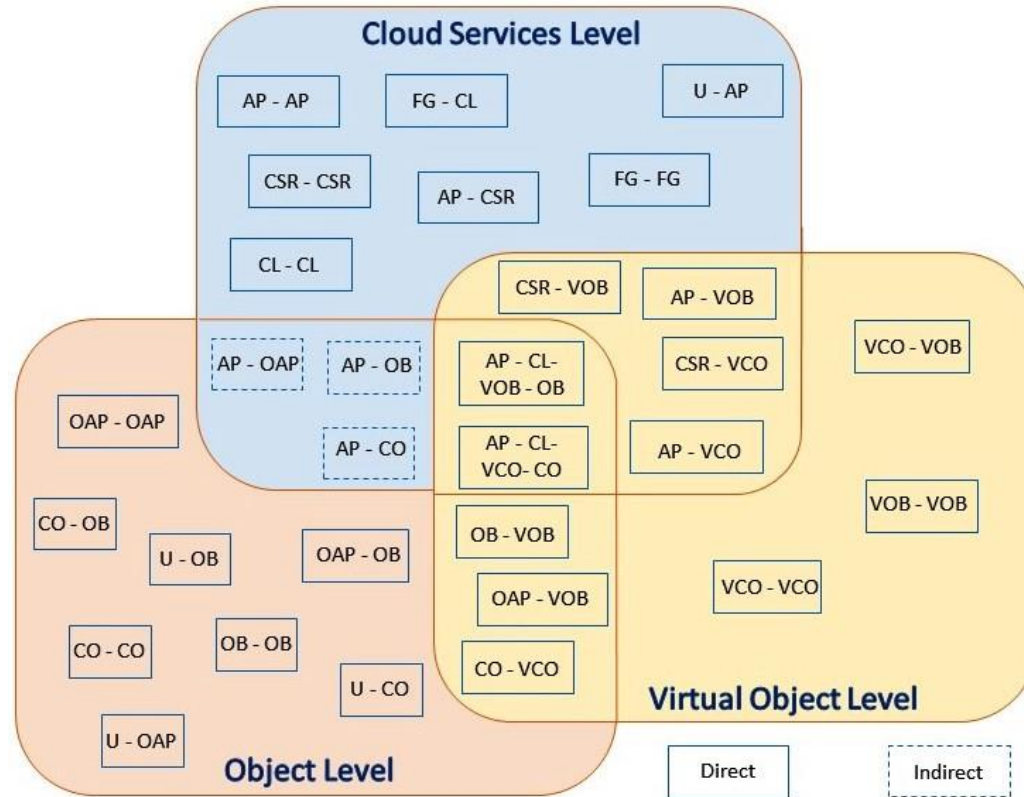
- Software Reliance
- Broad Attack Surface
- Untrusted Entities



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?

- External Interface
- In-Vehicle Interaction
- Whom to TRUST? How establish TRUST?
- Cross Cloud Sharing
- Data in Cloud