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

Maanak Gupta and Ravi Sandhu
Institute for Cyber Security (ICS),
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC),
Department of Computer Science, University of Texas at San Antonio
Email: gmaanakg@yahoo.com, ravi.sandhu@utsa.edu

ABSTRACT

Internet of Things has become a predominant phenomenon in every sphere of smart life. Connected Cars and Vehicular Internet of Things, which involves communication and data exchange between vehicles, traffic infrastructure or other entities are pivotal to realize the vision of smart city and intelligent transportation. Vehicular Cloud offers a promising architecture wherein storage and processing capabilities of smart objects are utilized to provide on-the-fly fog platform. Researchers have demonstrated vulnerabilities in this emerging vehicular IoT ecosystem, where data has been stolen from critical sensors and smart vehicles controlled remotely. Security and privacy is important in Internet of Vehicles (IoV) where access to electronic control units, applications and data in connected cars should only be authorized to legitimate users, sensors or vehicles. In this paper, we propose an authorization framework to secure this dynamic system where interactions among entities is not pre-defined. We provide an extended access control oriented (E-ACO) architecture relevant to IoV and discuss the need of vehicular clouds in this time and location sensitive environment. We outline approaches to different access control models which can be enforced at various layers of E-ACO architecture and in the authorization framework. Finally, we discuss use cases to illustrate access control requirements in our vision of cloud assisted connected cars and vehicular IoT, and discuss possible research directions.

CCS CONCEPTS

• **Security and privacy → Security requirements**; **Access control**; **Authorization**;

KEYWORDS

Access Control; Internet of Things; Vehicular Internet of Things; Connected Cars; Vehicular Cloud; Internet of Vehicles; Big Data; Attributes Based; Trust; Fog Computing; Cloud Computing

ACM Reference Format:
Maanak Gupta and Ravi Sandhu. 2018. Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things. In *Proceedings of 23rd ACM Symposium on Access Control Models and Technologies (SACMAT'18).* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3205977.3205994

1 INTRODUCTION

Internet of Things (IoT) is the new era of technology which envisions to make human lives smarter. The concept has attracted wide applications and services in variety of domains including health-care, homes, industry, transportation, power grids etc. The magnitude of this technology is illustrated by the number of devices which are estimated to be more than 20 billion by year 2020 [32]. The prime asset delivered by such massive interconnection and networking of smart devices is Big Data, which is analyzed to gather insights and deliver valuable information.

IoT requires the use of multiple technologies including identification (naming and addressing), sensing (sensor devices, RFID tags etc.), communication technologies (Bluetooth, WiFi etc.), computation technologies involving hardware or software platforms like Cloud, multiple IoT services [35] and the applications which provide functionalities to the end user [9, 13, 36]. Several IoT architectures have been demonstrated to incorporate physical objects, object abstraction (virtual objects), middleware or service, application and business layers with variations in architecture stack and nomenclature [9, 13]. Cloud computing is also an important domain in today's world which offers boundless applications and resources (storage and compute) to multiple users. Therefore, the merger of IoT and cloud is arguably indispensable to harness the full potential of IoT smart objects which have limited storage, processing and communication capabilities. The literature has recognized this desirable integration using terms such as cloud-assisted, cloud-enabled, and cloud-centric IoT [8, 16, 18, 20, 21, 25, 50].

Smart cities and intelligent transportation has been a vision of future society. IoT plays an important role to make transportation smarter by introducing connected cars and vehicular communication. Vehicular IoT involves interaction and V2X data/messages exchange between several entities including vehicle to vehicle (V2V), vehicle to road infrastructure (V2I), vehicle to human (V2H), intra-vehicle, and vehicle to cloud (V2C). Vehicular Ad-hoc Networks (VANETs) provide necessary connectivity which is extended with use of smarter devices and cloud or fog infrastructures. Several sensors in and around connected car 'talk' to each other for smarter decisions and convenient transportation experience to user. Our vision of vehicular IoT harness computation and storage capabilities of cloud and the concept of virtual objects (e.g. AWS shadows [14]).

Security and privacy have been a serious concern and challenge for the adoption of IoT. The gravity of these issues is magnified

SACMAT'18, June 13–15, 2018, Indianapolis, IN, USA
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5666-4/18/06…$15.00
https://doi.org/10.1145/3205977.3205994

when we think about implications in vehicular IoT and the emerging concept of autonomous cars. This ecosystem has connected cars as its most important, and also most vulnerable, entity. With over 100 millions lines of code, more than 100 electronic control units (ECUs) and broad attack surface opened by features such as onboard diagnostics, driver assistance systems and airbags, it becomes a challenge to protect this smart entity. Further, the communication among smart objects (vehicle to vehicle, vehicle to infrastructure etc.), mobility, and dynamic network topology makes it even harder to secure the system. Some of the potential risks in vehicular IoT involves untrustworthy or fake messages from smart objects, data privacy, critical ECU hacking and control, spoofing connected vehicle sensor, and injecting malicious software. The US Department of Transportation (USDOT) and National Highway Traffic Safety Administration (NHTSA) have focused on vehicular security and have released important cyber-security guidelines in this regard [52, 53]. USDOT's strategic plan also outlines the direction and goals of Intelligent Transportation System (ITS) Program [15].

Access control is an important mechanism to prevent unauthorized access to resources in any system. This paper focuses on access control and authorization requirements in Vehicular Internet of Things and Connected Cars, which we also refer to collectively as the Internet of Vehicles (IoV). We envisage cloud and virtual objects as an important component of cloud-assisted vehicular IoT. We propose an extended access control oriented architecture (E-ACO) for IoV, which is an extension to the recently proposed ACO architecture for IoT [10]. The prime difference between these architectures is the introduction of clustered objects, which are objects with multiple sensors, and possible interaction between sensors in same clustered object or between different object's sensors. Clustered objects are particularly relevant in case of connected cars, traffic lights or other smart devices which have multiple sensors and ECUs mounted on them. Our authorization framework illustrates different interaction and data exchange scenarios in vehicular IoT and proposes access control models at various E-ACO layers including physical, virtual objects, cloud layer and applications. We further discuss different cloud or fog based architectures in IoV, and the concept of vehicular cloud and its relevance. Comprehensive use cases and research directions are also elaborated to illustrate the need for an authorization framework in vehicular IoT ecosystem.

The paper is organized as follows. Section 2 discusses important technologies and concepts relevant to vehicular IoT including connected cars, vehicular clouds, virtual objects, IoV security and privacy concerns, and ACO architecture. Section 3 elaborates IoV characteristics, various cloud or fog architectures, and our proposed extended access control oriented (E-ACO) architecture. Authorization framework with different IoV entities interactions and some access control approaches, is discussed in Section 4. Real world use cases reflecting access control requirements in single and multiple cloud systems are discussed in Section 5, followed by some proposed research agenda in Section 6 and conclusion in Section 7.

2 RELEVANT BACKGROUND

Vehicular IoT is a novel domain where networking and communication among cars, traffic infrastructure, pedestrians, homes or ultimately anything is proposed. This emerging concept involves several new and established technologies which needs to be discussed to understand IoV systems and our authorization framework. This section reviews IoV building blocks which we believe are fundamentally required and are the basis of our work.

2.1 Connected Cars

The prime goal of IoV is inter-connectivity among smart entities in which vehicles are most important. As stated [4] by Wikipedia , "A Connected car (or Connected Vehicle (CV)) is a car equipped with internet access and usually also with the wireless area network. This allows the car to share internet access with other devices both inside as well as outside the vehicle". Gartner predicts a quarter billion connected cars by year 2020 [31] which will form a significant portion of the overall connected devices. The communication among vehicles and infrastructure, driving assistance and autonomous driving, automatic braking and emergency calling, weather and accident warnings, parking areas, E-toll, and predictive maintenance, are among the most desired and available features in today's connected cars. These cars have more than 100 ECUs and 100 millions lines of code in support of such functionality. CVs have controller area network (CAN) bus, FlexRay, Ethernet and other protocols which are used for ECU communication within the car. Messages are broadcasted to all ECUs attached to bus. Multiple buses are connected via a gateway, usually a TCU (Telematics Control Unit), which also provides interface to external environment. These vehicles generate, exchange and process huge amounts of data and are often referred to as 'smartphones on wheels' [63]. Some of the most hackable and exposed attack surfaces in a connected car include airbag ECU, Bluetooth, TPMS, and remote key [22]. As vehicles with a broad attack surface get connected to the internet, they get exposed to remote malicious activities. Cyber attacks can be orchestrated from in-vehicle network, from a user inside the car using a smartphone, from external entities in proximity, or even through cloud.

2.2 Vehicular Clouds

Vehicular Ad-hoc Networks (VANETs) have been proposed in the literature to support vehicle to vehicle and vehicle to infrastructure communication to enable advanced services to the drivers. The network nodes in VANETs (cars, infrastructure etc.) have storage, computation and communication modules to provide such services. However, most of these on-board resources are usually under-utilized with the set of applications offered, and can be utilized for additional services to stakeholders [27, 56]. The concept of vehicular cloud (VC) has been proposed which blends the two separate ideas of VANETs and Cloud computing. Cloud computing provides the idea of boundless storage, compute or network resources in the form of IaaS, PaaS and SaaS, which are extended to the inter-networked cars and infrastructure provided by VANETs. Vehicular Cloud [27, 33, 34, 56] utilizes coordinated on-board resources of cars and infrastructure to offer the capabilities of 'cloud on the fly' to users that need them.

The vision of IoV requires cooperation among entities for smooth and efficient traffic flow with information and entertainment (infotainment) to driver. All such applications have local relevance which need time and location sensitive computation of information avoiding the latency and bandwidth problems when the information is loaded and processed in central cloud. Therefore, the surrounding vehicles can form autonomous clouds to solve driver's locally relevant queries about traffic ahead or parking nearby. Several architectures have been proposed for the formation of vehicular clouds like stationary VC, VC linked with a fixed infrastructure or dynamic VC, where each has different formation scenarios [45, 71].

The key features to distinguish conventional cloud and VC are mobility, agility and autonomy of vehicles, which are computation and storage nodes in vehicular cloud. In VCs, one vehicle is selected as the broker by surrounding vehicles which mediates resource sharing among vehicles in and around specific geographic boundary (for example in 2 miles radius). The broker asks permission for cloud formation from relevant authorities and also sends request to neighbouring vehicles to share resources. Once approved by authorities (DMV or transportation agency), these vehicles pool their resources to form a virtual environment which is shared by all VC users. Further, large scale federation of VCs can be established in case of emergency situations like earthquake, providing temporary infrastructure when conventional cloud is unreachable.

We believe vehicular IoT will involve single or multiple cloud/fog instances supporting different service models – SaaS, PaaS and IaaS. These instances can cover wide geographic area using central cloud, fog instances within 1-2 miles radius or even fog instances at each connected car level based on different use cases. These architectures can be public, private (for example by a car manufacturer) or hybrid and involve single internet clouds, vehicular clouds, fog instances or any combination of them as discussed further in Section 3.

2.3 Virtual Objects

The cyber-physical ecosystem of vehicular IoT has heterogenous objects with different operating conditions, communication technology, and functionalities. Further, the issues related to object connectivity, scalability, object and service discovery, security and privacy, quality management, and identification are challenges in any IoT system [55]. To counter these issues the concept of virtual objects is introduced in several IoT architectures [60, 70]. Amazon AWS IoT [17] also incorporates virtual objects as device shadows where in case a physical device is not connected, its cyber counterpart (i.e. shadow) will have the last received state or desired future state information. Therefore, whenever the physical device gets connected to its virtual entity, it gets updated to the state of its cyber object and also mitigates the problem of sporadic object connectivity. Microsoft Azure [7] has device twins which are JSON documents maintained in Azure IoT hub for each device connected and stores device state information. Different association scenarios exist between physical and virtual objects: single virtual object for one physical object irrespective of the number of services and functionalities provided by physical object; whereas for object with multiple services, it is possible to have many virtual objects for each service of same physical object. Similarly, other configurations such as many physical to one virtual or many physical to many virtual mappings are also possible depending on different use-case requirements. The creation and location of virtual objects is primarily proposed in the cloud and their communication uses RESTful technologies [55]. Since high latency and low bandwidth issues will exist in virtual objects creation, for real time applications like vehicular IoT, we envision to keep the virtual objects near to the physical objects, i.e at the fog level or in vehicular cloud (VC).

2.4 Security and Privacy Concerns

Most security vulnerabilities like trojan horse, buffer overflow exploits, malware, ransomware, and privilege escalation can be exploited on connected vehicles and other IoV entities. Connected vehicle with more than 100 ECUs, with broad attack surface interacting both in-vehicle systems and a wide range of external networks including WiFi, cellular networks, and internet to data exchange between service garages, toll roads, gas stations, and several automotive and aftermarket applications [22], present a big challenge for security. Recently Tesla Model X was hacked [66] with many other incidents of attacks noticed in past. Security is vital in IoV and CVs where attacks (like disabling brakes) can even lead to loss of life. Several studies and reports [2, 5, 58, 59, 69] have been published to illustrate potential risks and attacks which can be orchestrated on smart entities in IoV. Some examples of cyber attacks in connected cars and IoV as discussed in [24, 26, 30, 44, 62] include: user impersonation to exchange fake basic safety messages (BSM) or false information about an accident, stealing personal data or credit card information, controlling critical sensors of connected vehicle, gaining knowledge of vehicle and driver movement, spoofing CV's sensors, coordinated attacks on infrastructure, unauthorized over-the air firmware updates, and infecting a CV with ransomware. CAN bus used for internal ECU communication must also be secured to prevent unauthorized gain of data and manipulation of software on ECU and sensor systems. An unauthorized party that gains access to the bus can block legitimate messages and transmit illegitimate ones. On board equipments (OBEs) integrate with the CAN bus to provide information such as vehicle speed and brake system status to participating entities. This bring us back full circle to needing to protect the internal components of a vehicle in order to maintain confidence that V2V, V2I and V2X messages are legitimate. Securing IoV and connected vehicles will require protecting control systems (on-board diagnostic (OBD) port, CAN bus etc.), protecting infotainment systems, securing smartphone applications, securing infrastructure, securing over-the air updates, and securing hardware from manual tampering. Security mechanisms become hard to implement considering intrinsic IoV characteristics like dynamic topology, mobile limitation, and large scale network.

US Department of Transportation initiated the ITS (Intelligent Transportation Systems) program to enable communication among vehicles and other smart infrastructures while ensuring security and privacy of the stake-holders. The BSMs exchanged among entities must not include personally identifiable information and must be broadcasted in limited geographic area [67]. Dedicated short range communications (DSRC) is used to exchange information across entities which is used by several safety and other applications to generate alerts for drivers. Therefore, the confidentiality and integrity of such messages is imperative so that drivers can trust their source and information in them. Security Credential Management System (SCMS) [68] has been proposed to ensure trust and message security using public key infrastructure (PKI) approach where certificate generated by certificate authority (CA) is attached with the BSM to ensure trust between talking entities. European

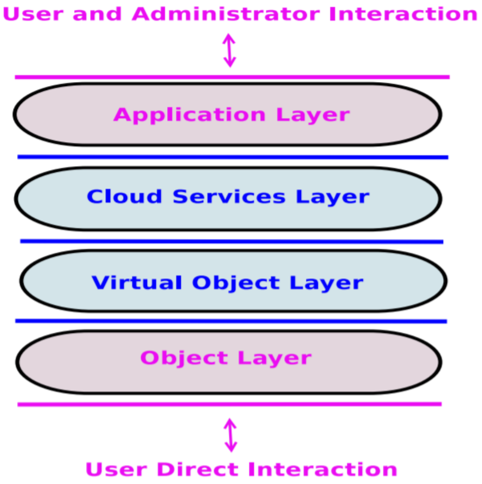


Figure 1: ACO Architecture [10]

Union Agency for Network and Information Security (ENISA) has also released a study in year 2017 [28] which enlists critical assets in smart cars, threats, potential risks, and proposed good practices mainly segmented into three categories, policy and standards, organizational measures, and security functions, to ensure security of smart cars against cyber threats. European Commission has set up Cooperative Intelligent Transport Systems (C-ITS) Deployment Platform to foster cooperative, connected and automated vehicles, and has released security frameworks [65] and certificate policy [64] documents. National Institute for Standards and Technology (NIST) also proposed a framework [54] for cyber-physical systems (CPS) which address conceptualization, realization and assurance of CPS including security and interoperability.

2.5 ACO Architecture

In general, all proposed IoT architectures [9, 13, 20, 36, 55] have three layers: object, middleware (with multiple sub-layers) and application layer. Recently, Alsehri and Sandhu proposed an IoT architecture, referred as access control oriented architecture (ACO) [10], taking into consideration the access control requirements in IoT and incorporation of models at various layers. As shown in Figure 1, ACO architecture has four layers – object, virtual object, cloud services and application – with user and administrators interacting at object and application layers. Since, our proposed extended ACO architecture for vehicular IoT (discussed in Section 3) adds to/refines generic IoT based ACO architecture, we will outline ACO architecture layers below.

- **Object Layer:** The bottom layer of ACO architecture comprises physical smart devices like sensors, RFIDs, beacons, and ECUs, which are responsible for data sensing and accumulation, and for sending data to upper layers. These devices can communicate with other devices using different communication technologies including Bluetooth, WiFi, Zigbee, LAN and LTE. Physical devices communicate with their cyber counterparts (virtual objects) using protocols like HTTP, MQTT, DDS or CoAP [9]. Users can also directly access physical objects at this layer.

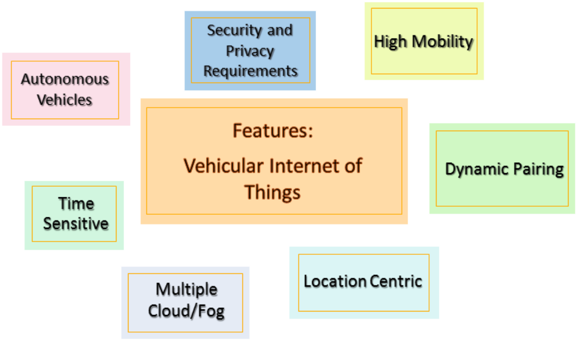


Figure 2: IoV Distinguishing Characteristics

- **Virtual Object Layer:** As discussed, virtual objects represent the digital counterpart of physical objects which maintain the status of physical objects even when they are not connected. ACO architecture recommends virtual object layer as a part of middleware to support communication between heterogenous objects and overcome IoT challenges of scalability or locality.
- **Cloud Services Layer:** With the number of IoT devices proliferating, the storage and computation of data will be done in cloud, where different applications can harness it to make valued decisions. Single or multiple cloud scenarios can exist to support federation or trusted collaboration between them. Some important IoT cloud platforms include Amazon AWS [14], Microsoft Azure IoT Hub [7], and Google Cloud IoT Core [6].
- **Application Layer:** The applications offered by IoT systems to end users are situated in this layer, which leverage the services and functionalities of the lower cloud services layer. Users and administrators can remotely send commands and instructions to smart devices at bottom layer using these applications, but such interaction has to pass via other two ACO middleware layers (cloud services and virtual object). Administrators can also define access control policies for various IoT resources using this layer.

3 CLOUD ASSISTED VEHICULAR INTERNET OF THINGS

The vision of smart city and intelligent transportation encompasses connected cars and vehicular IoT as an important component. The eventual goal of IoV is the integration of vehicles, infrastructure, smart things, homes or ultimately any thing to promote efficient transportation, accidental safety, fuel efficiency etc. and for pleasant travel experience to the driver. The technology involves communication between vehicles (V2V), vehicle to human (V2H), vehicle to cloud (V2C), vehicle to infrastructure (V2I) etc. to exchange vehicle telematics [12, 29] and gather information about surroundings to offer services to the users. Safety applications in IoV require basic safety messages (BSM) to be exchanged among smart entities, which contain information about vehicle position, heading, speed, etc, related to vehicle state and predicted path [1]. Such interaction can happen using dedicated short-range communications (DSRC) technology (similar to WiFi, secure and reliable) which allows rapid communications (up to 10 times per second) between elements of IoV network required for end user applications.

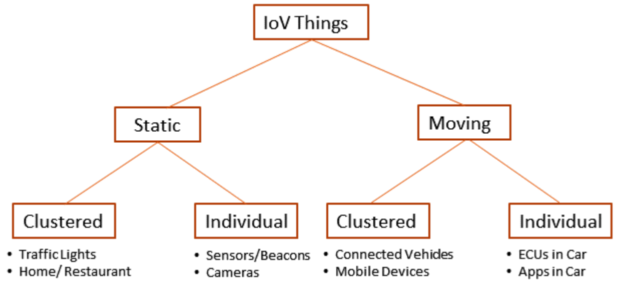


Figure 3: Smart Object Types in IoV

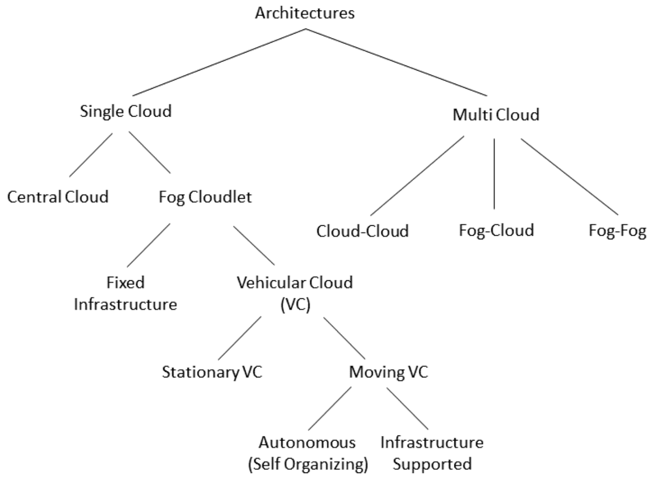


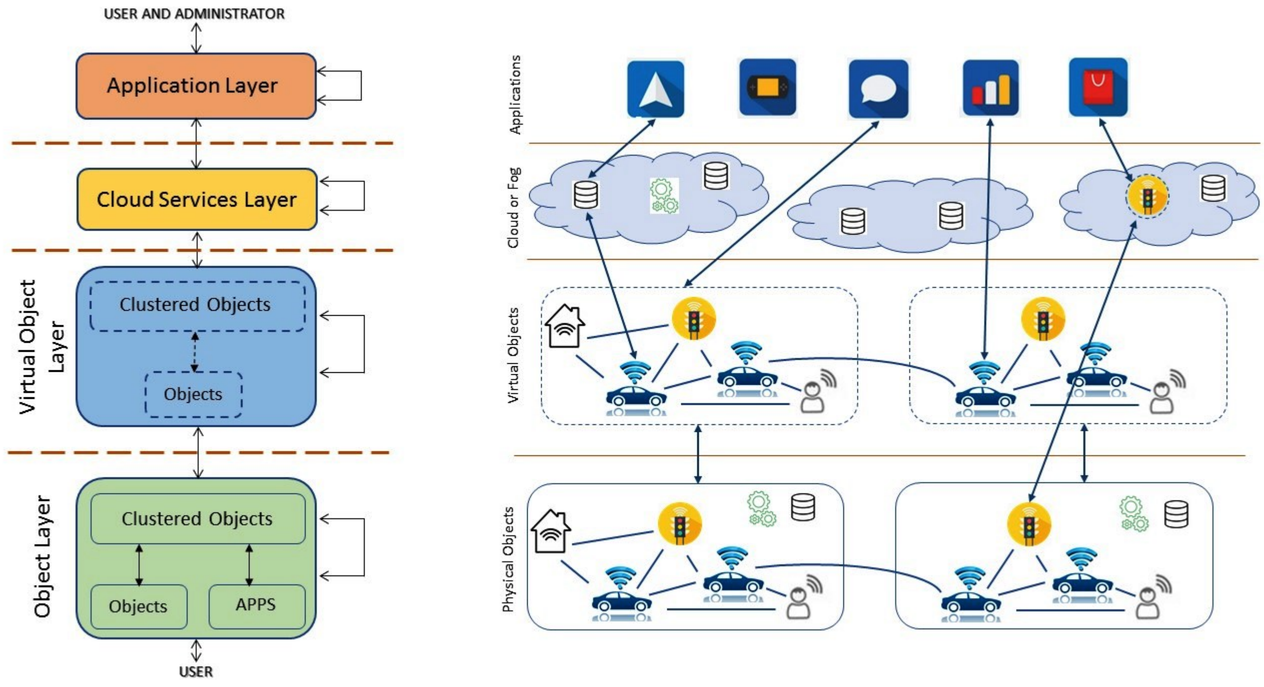
Figure 4: Different Cloud and Fog Architectures in IoV

3.1 Characteristics and Cloud Architectures

Vehicular IoT inherits intrinsic IoT characteristics of data sharing, communication and accumulation in cloud. However, dynamic topology structures, dynamic communication, mobility, network scale, and non-uniform nodes distribution (shown in Figure 2) are some features that distinguish it from other IoT domains, resulting in new security and privacy challenges. Further, several applications in IoV domain are very time and location sensitive; for example, BSM information about traffic congestion from a neighbouring vehicle or a traffic light, or about ice on bridge or an accident report to a nearby hospital etc. makes IoV ecosystem very dynamic. Internet of Vehicles involve different kinds of objects (as shown in Figure 3) based on their mobility, functionalities or processing capabilities. Some smart objects are static in nature; for example, beacons outside a restaurant, or sensor on a smart traffic light whereas moving objects include connected cars, pedestrian with mobile phones, etc. Further, some of these are individual objects with single sensor performing only one function whereas some are clustered objects having multiple sensors associated with them. A connected car has several ECUs and sensors on it, and hence is referred as a clustered object whereas a single ECU in a car generally performs one function and is an individual object. Such characterization is necessary as it drives our access control framework and models. Several applications of connected cars and vehicular IoT are envisioned for smart city intelligent transportation initiative, including the following.

- **Safety and Assistance:** With machine to machine (M2M) communication among vehicles and infrastructure, these applications provide real-time information about other vehicles and traffic to control speed, in-lane position control or road work warning from signboards. Further, in inclement weather, in non-ideal driving conditions, or blind spots, even pedestrian with mobile phones can exchange safety messages with incoming vehicle such as while crossing roads.
- **Diagnostic and Maintenance:** Remote diagnostic and predictive maintenance of vehicles through manufacturer or authorized mechanic will save time and money. Vehicle sensor data can be send to cloud for processing to predict vehicle mechanical issues. Over the air (OTA) updates can also be issued by manufacturer for fixing car firmware which will obviate the need to go to mechanic. Fleet management applications provide real-time telematics, driver fatigue detection and package tracking.
- **Information and Entertainment:** Driving based insurance models have been introduced which will assess the driver behaviour to determine insurance premiums. Real-time parking information can be shared between parking garages and vehicles. Restaurant and gas stations can send offers to nearby vehicle's dashboard. Car-pooling, connected driving [47], web-browsing, music etc. are some additional IoV applications.

We believe cloud platforms like Amazon AWS, Microsoft Azure etc. will play an important role to fully harness the potential and applications of IoV. Further, the use of edge or fog computing [19] is imperative to resolve the issues of high latency, low bandwidth and communication delays pertinent to using central cloud, which are very critical in time and location sensitive IoV applications [3]. Figure 4 shows various single and multi cloud scenarios viable in IoV. Single cloud architectures may involve only one central cloud which manages user applications, virtual objects and data generated from smart entities in a wide geographic area, such as a city. This architecture is not feasible because of latency and other issues mentioned above. Fog or edge computing is essential, and we believe IoV can either use vehicular cloud (i.e the resources offered by smart vehicles and infrastructure on road) or a fixed infrastructure setup along the road where compute and storage clusters are dedicated for small areas. It is also possible to use fog structure for each connected vehicle, and sensors in the vehicle have virtual objects in the fog which can be used to enable intra-vehicle communication. Vehicular cloud (VC) can be stationary where the vehicles are standing in a mall parking lot and offering their resources for an incentive (like a free parking) or moving VC where vehicles while moving may form cloud using broker [33, 34, 45, 56, 71] and can leave or join the cloud if in specified geographic range. Further, these moving VCs can be supported by fixed infrastructure (example, a traffic light on the roadside acting as a broker) or moving vehicles in autonomous manner can form a VC. In multi-cloud IoV architectures, we envision to have either multiple clouds, cloud-fog or multiple fogs setup. However, we believe single central cloud and multiple fog architectures are a good fit to cover most connected car and IoV applications, as discussed later in our extended ACO architecture.



a) Extended ACO Architecture for Connected Car and IoV

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

Figure 5: Extended ACO Architecture for Connected Cars and Vehicular IoT

3.2 Extended ACO Architecture

Connected Cars and Vehicular IoT ecosystem has several heterogenous devices (individual or clustered) and in-built car applications which cooperate to provide services to the end users. Some devices are independent (camera on street, beacons on restaurant) whereas some belong to a larger clustered object (ECU or sensor in a connected car). Hence, we propose to incorporate this distinction into previously defined access control oriented architecture (ACO) [10] to address IoV ecosystem access control requirements. An important reason to incorporate clustered objects is to reflect cross-vehicle and intra-vehicle communication. The fact that two connected cars can exchange basic safety messages (BSM) with each other reflects clustered object communication. Such concept is not defined in ACO architecture which is proposed for generic IoT systems. Besides objects, these clustered objects may have applications running in them; for example, a car may have a navigation application installed in it, or a safety warning application, which may interact with sensors on a smart sign-board to warn the driver via car dashboard or seat vibration or buzzer. It should be noted that these sensors or applications may access sensors in car they belong to or possibly sensors on other cars also.

Figure 5 shows our proposed extended ACO (E-ACO) architecture along with the corresponding vehicular IoT components at different E-ACO layers in Figure 5 (b). E-ACO architecture has four layers similar to ACO: Object layer, Virtual Object layer, Cloud services and Application layer, where the communication can happen within a layer (shown as self loop in Figure 5 (a)) and the adjacent layers above and below. We will now discuss layers in more detail:

Object Layer: The object layer introduces clustered objects which have multiple individual sensors or smart objects. The clustered objects may also have several built-in applications (like tire-pressure monitoring) installed within them. These applications can communicate with ECUs and sensors in same car (or neighbouring car) to get data and update information to the drivers. Some of these applications accumulate data and send it to the cloud infrastructure for further analysis; for example diagnostic applications installed by the manufacturer which will collect data from critical engine sensors and send to the cloud for processing and offering customers with OTA maintenance services. The in-vehicle communication for applications, ECUs and sensors is supported by different networking technologies including Controller Area Network (CAN), Local Interconnect Network (LIN), Ethernet, Media Oriented Systems Transport (MOST) etc. Communication can occur between objects (and clustered objects) in the object layer and also with the layers above (virtual object) and below it (user). Communication across objects (within the object layer) among different vehicles or clustered objects is feasible via technologies like dedicated short-range communications (DSRC), Bluetooth, WiFi, and LTE. An example interaction in object layer is BMW connect application in phone which reads address from phone and send to the car navigation system, or V2V BSM exchange using DSRC.

It should be noted that instead of introducing clustered objects as a separate layer in E-ACO, we have added them to the same object layer of ACO architecture, which reflects the binding between objects, applications and the clustered object to which they belong. We believe the relationship between objects and clustered objects is important, for example, a lane departure sensor in car will have some attributes (like vehicle id) it inherits from the car and such binding is shown by putting them in same layer. These clustered objects and cars also have applications associated with them which offer services to drivers inside. For example, a rear vision system is an application in cars to get rear-view, which gets data from rear-camera (an object) to provide dashboard view to the driver. Other applications include tire-pressure monitoring system which talks to sensor installed in tire, cabin monitoring system, info-tainment systems etc. are in-built in connected cars and can communicate with sensors or other applications in system. These applications in object layer of E-ACO is add-on to the object layer in ACO architecture and reflects its importance in IoV ecosystem which is very dependent on in-built applications supported by smart cars.

Virtual Object Layer: Communication of sensors, vehicles and other smart entities may also involve virtual objects or cyber entities to eliminate connectivity, heterogeneity and locality issues. The most important smart entity in IoV, a smart car, is usually in motion and passing through areas with low or no internet connectivity all times. In such scenario, it is imperative to create a cyber entity of smart car (and its sensors) in the cloud so that the last state and desired state information of car (and sensors) can be sent to the virtual entity when car is not connected. Once the physical object gets back internet connectivity, the virtual entity will push information/state to its physical counter part. For example, if a problem is diagnosed in powertrain control ECU of a car and a command needs to be sent by mechanic to ECU to control air-fuel ratio. In case a car has internet connectivity, message can be sent directly to ECU, but if no connectivity message should be sent to virtual entity of the ECU which will push message to physical ECU when car gets connectivity and syncs virtual and physical entity. We envision the virtual object layer in E-ACO architecture will have one or many cyber entity (virtual object or device shadow) for both clustered and individual objects. Physical objects can communicate with their cyber counterpart using HTTP, MQTT, AMQP or CoAP protocols. When sensors s_1 and s_2 across different vehicles or clustered objects communicate with each other, the sequence of communication via virtual object layer should follow starting s_1 to vs_1 (virtual entity of s_1), vs_1 to vs_2 and vs_2 to physical sensor s_2. Similar communication can be envisioned for in-built car applications which can indirectly exchange information from physical sensors through their cyber counterparts created in cloud, vehicular cloud or fog architecture. It is possible to create a fog cloudlet for each vehicle where cyber entities will reside and support the indirect communication within physical sensors and ECUs inside car. Our E-ACO architecture does not support cyber-entity for in-car applications supported by IoV and will not create virtual objects for such applications [1].

Cloud Services and Application Layer: Since most user IoV applications are cloud supported (i.e. use cloud infrastructure and services), we explain them together to provide a better understanding of these two mutually dependent E-ACO layers. Cloud layer provides storage and processing whereas application layer provides application interface to users to control and interact with object layer components as discussed in ACO architecture [10]. Over the air (OTA) updates for firmware and other software components in the cars are through the cloud service layer where only authorized users are allowed to issue OTA. User and applications can access the data pushed into the cloud by smart infrastructures for offering value added services to customers. Our proposed architecture assumes to have both central cloud and fog (instantiated by vehicular cloud) component in IoV ecosystem but are collectively represented as cloud services. An important use for cloud layer in IoV and connected cars involves defining security policies for authorized vehicular communication, which we understand is missing in literature. Further, we assume that virtual entities of various objects can be created in both central cloud and fog depending on the use-cases and the scope of applications which are accessing the objects. For example, an accidental safety application will have limited geographic scope and hence will access virtual objects created in fog (to overcome latency issues); whereas, a health-monitoring application may access body sensors via virtual objects created in central cloud. Cloud services and applications can access information and data from virtual objects using MQTT or other relevant protocols. It should be noted that most IoV architectures and use-cases we studied [24, 34, 47] don't have virtual object layer and include only object, cloud services and application layer. Communication between cars, sensors and applications in object layer do not involve virtual objects and is done using lower layer protocols like DSRC, WAVE, Bluetooth or WiFi. Sensors can directly send data to cloud storage for processing without involving virtual objects, which is then used by applications. However, connectivity issues in moving cars and communication heterogeneity among entities supports the need for virtual layer, as discussed earlier in this section.

Figure 5 (b) shows an instance of IoV with physical objects (car, traffic light) along with cyber counterparts in virtual objects layer, and other E-ACO layers. It can be seen that physical objects communicate with virtual objects, and applications are accessing data through cloud which is pushed by virtual entity of an object. Storage and processing icons at object layer symbolizes road-side infrastructures which can help to store data from vehicles and filter before pushing data to cloud. Virtual objects are created at both fog and central cloud to satisfy different application needs.

4 AUTHORIZATION FRAMEWORK FOR INTERNET OF VEHICLES

The dynamic and distributed nature of vehicular IoT brings in challenges to secure the ecosystem. Broad attack surface and numerous external interfaces along with the intrinsic characteristics of IoV makes it hard to ensure security and privacy of the components and data inside. Access controls are important to restrict unauthorized access to data, sensors, applications, infrastructure and other resources in connected cars and IoV. Applications like MobEyes [51] and CarSpeak [49] allow vehicles (or sensors) to access not only its own sensors but also neighbouring vehicle sensors to get data and information. The exchange of BSM messages among vehicles and smart entities, and their use must be trusted and checked. Further, in-vehicle communication along buses between ECUs and applications should be secured. Such exchange must be authorized to ensure confidentiality and integrity of vehicle's and user's personal data, and to prevent remote (or physical) control of connected smart

[1] Note that Amazon AWS IoT does allow applications to have a thing shadow [14] but comprehensive IoV use-cases to support the functionality are still missing in literature.

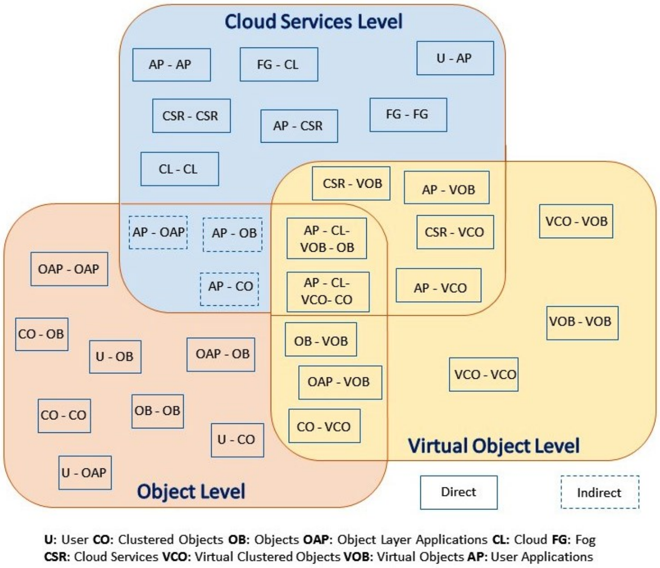


Figure 6: Different Interactions in IoV Ecosystem

entities. In this section, we define an access control framework that reflects authorization needs at various layers of extended ACO architecture discussed earlier. We also discuss some access control models and authorization approaches relevant for IoV ecosystem.

4.1 Authorization Framework

Several interaction scenarios exist in Internet of Vehicles which makes it hard to comprehend different access control decision and enforcement points, together with other security requirements. Based on the extended ACO architecture, we have put together various vehicular IoT communications into three categories: Object Level, Virtual Object Level and Cloud Services Level as shown in Figure 6. Since most user applications are cloud based which use services and resources in cloud, we have bundled the interaction of IoV entities with cloud and applications together. As discussed in the E-ACO architecture, each layer components interact with themselves (components in same layer) and the components in layers immediately above and below it. Two types of interactions exist in E-ACO, direct and indirect, marked with solid and dashed boxes shown in figure. Communication between adjacent and same layer is direct communication whereas indirect includes interaction beyond adjacent layers i.e. two or more layers above or down in E-ACO. For example, interaction between clustered object and objects inside the clustered object is direct, as they belong to the same object layer whereas interaction between an application in application layer and object will be indirect as applications will interact with object via its virtual entity created in cloud. It is possible to have interactions overlapping in two categories, e.g., cloud service (CSR) and virtual object (VOB) interaction is part of both cloud services and virtual object category. Following are the authorization framework categories and some IoV communication scenarios:

- **Object Level:** This category covers object layer interaction within itself and with adjacent layers (virtual objects and users) in E-ACO architecture. Some interaction types (shown in Figure 6) include between clustered objects (CO-CO), between clustered object and object (CO-OB) for example smartphone and car USB port, between user and sensors (U-OB), between sensor and any application running inside car (OB-OAP), and between ECUs (OB-OB). Access control models to authorize each of these interactions and resulting data exchange are required. BSM exchanges between connected cars using DSRC is an example communication that needs entity authorization to ensure integrity of message, which must be addressed by appropriate access control methods.
- **Virtual Object Level:** This includes communication of virtual entities with real objects, with cloud services or with user applications. Some examples include, between virtual objects (VCO-VCO, VOB-VOB), between application and virtual objects (AP-VOB), cloud services and virtual objects (CSR-VOC, CSR-VOB) etc. Most of these communications are through publish-subscribe protocols like MQTT, DDS or through HTTP, CoAP. Recently, Alsehri and Sandhu [11] presented access control models for VOB-VOB interaction in topic based communication using CapBAC (Capability based access control), ACLs and ABAC.
- **Cloud Services Level:** Cloud provides necessary storage, processing and services to unleash true IoT potential. Further, most applications are also cloud based with their software and hardware components supported in cloud. Therefore, this category includes both application and cloud interactions with IoV entities and virtual objects. The layer also considers multi-cloud or fog-cloud interactions which are important in distributed IoV. Some interactions in this category (shown in Figure 6) include: between user application and cloud services (AP-CSR), multi-cloud or fog interaction (CL-CL, FG-CL), indirect interaction between application and objects (AP-OB), cloud services (CSR-CSR) etc.

In-vehicle network allows interaction among sensors and applications inside the car, which also needs protection. Such communication can fit into above categories depending if entities involved are physical, virtual or applications. CAN bus and other intra-vehicle communication can be protected by assigning ACLs and capabilities to ECUs to prevent spoofing and other attacks. TCUs or Gateways have been used to separate critical ECUs from non-important subnetworks and also act as a common external interface to connected car. Access control models should be developed for various interactions in each category to control communication and data exchange. Note that our authorization framework does not include physical tampering and OBD port connectivity which is excluded from discussion. In next subsection, we will discuss some access control approaches relevant to fit in the IoV authorization framework.

4.2 Access Control Approaches

Researchers have investigated authorization requirements in IoT systems and proposed several access control models and implementations [23, 42, 43, 48, 57, 61, 72]. Recently, an access control model for virtual objects was proposed [11] using ACLs, CapABAC and ABAC. AWS access control model for IoT is discussed [17] which uses policies to control physical, virtual, cloud services and other communications in a publish subscribe exchange protocol.

We believe that IoV environment requires access control policy decision and enforcement at two levels: external communication

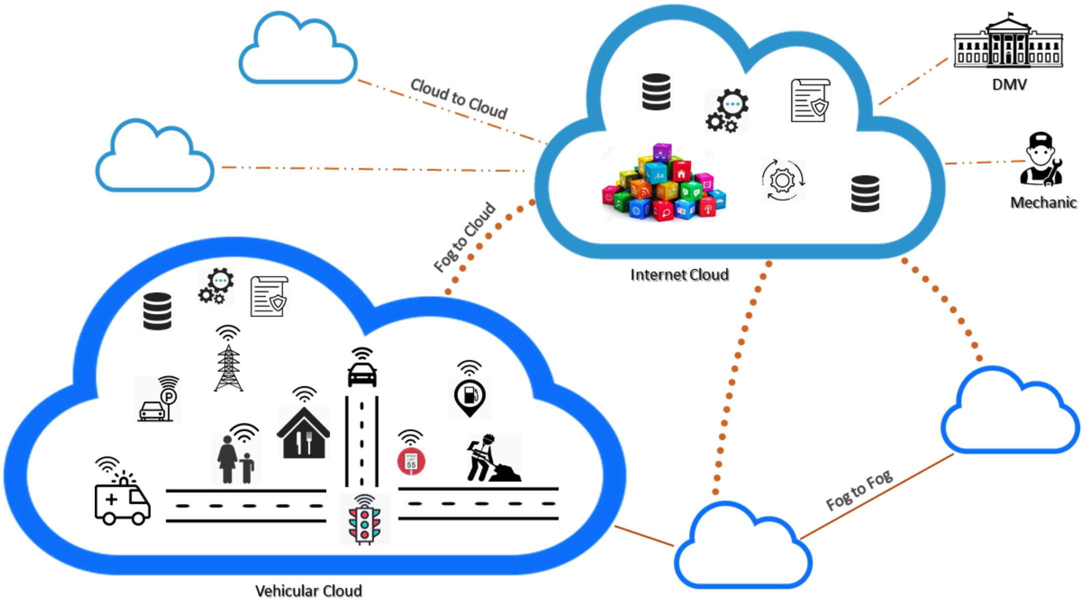


Figure 7: Connected Cars and Internet of Vehicles Ecosystem

and in-vehicle internal communication. Access control for external interface will secure authorized access to vehicle's data, sensors, ECUs and applications from external entities (like vehicle, traffic light, smartphones or user applications etc.) whereas internal mechanisms will secure ECUs and in-car applications communication and data exchange in a connected car supported by CAN bus, Bluetooth, WiFi etc. Securing external interface may not be enough to stop hackers, as they could impersonate a trusted device and bypass external access control. Also, in case if some ECUs with external interface are compromised, second level access control will protect critical systems in connected car. Vehicles discover new vehicles and infrastructure and start exchanging BSMs with them. Vehicular IoT mainly has two data exchange scenarios: static and dynamic, where static considers interaction due to long lasting relation for example, vehicle and owner or car manufacturer. Dynamic communication is temporary and occurs when entities are at certain place, or in geographic range with no prior relation between them. Also, static relation may share more private information which might not be the case in dynamic relation. These relations can help understand and develop access controls in IoV. Another approach may require multi-layered access control where the type of action required on an object determines the authority who can take access decision. For example, controlling an autonomous vehicle may require permissions from both owner and transportation authority, whereas reading data from vehicle may only need owner's consent.

We believe that clustered objects are important in access control decisions and can help to make preliminary decision. In case of vehicles, it is not only the vehicles which share BSMs, but also the sensors or applications in them which communicate. Therefore, first level check will ensure if two vehicles (as clustered objects) are allowed to talk, without considering their in-built sensors. If authorized at first level, next level access control will include sensors, applications and ECUs of the vehicles to make the final decision. Concept of trust can be introduced where only trusted entities can communicate. Trust can be established based on interaction, or relationships among two entities. For example, entities who have exchanged data earlier are more trusted; home and vehicle belonging to same owner are more trusted and can communicate. PKI based trust establishment in Security Credential and Management System (SCMS) [68] supported by USDOT is an important system to ensure BSM confidentiality and integrity in V2V communication. Further, attribute based [46] solutions can be added where IoV entities can inherit set of attributes from their geographic location, or from manufacturer. In such cases, attribute based policies can be used to determine sensors communication after trust is checked between their vehicles. Attributes which can be used in access decisions include geographic position, current speed, acceleration, deceleration, road surface temperature or other vehicle telemetry. Two level policy may be required: one at cloud level (to control V2V, V2I like communication) and another at fog or vehicular cloud level (to control intra-vehicle ECU's, applications or sensors interaction). Both single and multi-cloud scenarios can exist in which vehicles in same or across clouds can interact, which will also require access controls. Administrative models [11, 41] are also needed to support administration of IoV operational access control models.

5 USE CASES

In this section, we will discuss some use-cases in relevance to our authorization framework, incorporating the extended ACO architecture (shown in Figure 5), various IoV communication exchange scenarios (shown in Figure 6), using cloud and fog architectures, and entities of vehicular IoT ecosystem as shown in Figure 7. We have classified our use-cases into single cloud and multi cloud systems to reflect local or global scope of entity communications and user IoV applications, however, all applications in single cloud can be extended to multi-cloud and vice versa. Our prime objective is to describe how interactions and data exchange takes place in distributed and dynamic vehicular IoT ecosystem and various access control decision, enforcement points requirements.

Most applications in vehicular IoT are time and location sensitive, which require real time processing of information gathered from smart vehicles, sensors, ECUs and other smart objects present in a limited geographic area. To resolve issues related to latency and bandwidth pertinent to using central cloud, we believe vehicular cloud (VC) will play an important role, where the storage and computation present in smart vehicles or road side infrastructures (smart traffic lights, sign boards etc.) can be used to support IoV applications. Hence, our single cloud applications are supported by fog or cloudlet instance in the form of a VC where physical objects will have their cyber counterpart (virtual objects). It is also possible to have a fog instance for each connected car and any communication within the car is supported through it. Other scenarios may need to have multiple virtual objects for a single physical object where some objects are in VC and some in central internet cloud, required for more persistent state or for non-time sensitive applications or where the interacting IoV entities are not present in the range of same vehicular cloud. Such use-cases are discussed in multi cloud or fog-cloud architecture scenarios.

5.1 Single Cloud System

Single cloud applications include entities in limited geographic area communicating and exchanging information. A pedestrian crossing a road sends an alert message to an approaching car, or remote parking capability in BMW 7 series assists driver to park car using touch screen key are some examples of short-range communication. It is also possible to have a nearby restaurant or a gas station sending offers to connected vehicles on their dashboard, or in case of cruise mode cars, speed sign board automatically reduces the speed of car when a message is exchanged between them. Each IoV entity (clustered object, sensors, ECU's) in physical layer will have a cyber entity (one-to-one) created in virtual object layer, which is part of vehicular cloud or cloudlet or fog. MQTT and other IoT topic or content based publish subscribe model where publishers (sensors, applications) can publish to certain topics which are subscribed by other sensors or applications, and message broker passes relevant messages to desired subscribers whenever a publisher publishes on these topics. Besides cross entity interactions, in-vehicle communication also occurs, where sensors, ECUs and applications in a connected car exchange messages or interact with a smart device of a passenger sitting inside the car. In-vehicle communication is supported by fog architecture for each car where virtual entities can be created for each ECU, sensor or device. Further, in case of CAN bus communication critical ECUs are separated using gateway which also provides external interface to connected car. This ensures authentication and authorization to over-the-air (OTA) updates and enforces access control policies for in-vehicle communication.

Access control points are needed at physical, virtual object and cloud services layer, where the interaction and data exchange between legitimate and authorized entities is only allowed. At object layer V2V, V2I and other V2X communications using DSRC, WiFi etc. between clustered objects need access controls to ensure BSM confidentiality and prevent malicious activity. Direct access of user using a remote key to unlock a car or through a smart-phone application also needs authorization. It is also possible to store credit card information on vehicle storage or with a cyber entity of the vehicle, which can ease payment process on a toll road, or in a parking garage. In such cases, only authorized applications can access credit card information, which if leaked to nefarious actors can have huge financial implications. Within object layer, access controls are also needed to ensure authorized communication among sensors or applications and clustered devices, for example in case smart-phone accessing info-tainment systems or plug-in device into car needs security. Access controls are needed when physical objects communicate to their virtual entities in the cloud. For example, an airbag ECU or sensor in the car should only be able to contact its corresponding virtual entity to update its state or push messages via topics. Our concept of IoV ecosystem incorporates virtual objects (for every physical object) which will be important for message and information exchange among heterogenous objects. Virtual entity will be also created for smart devices inside the car that can issue commands to connected vehicle. Therefore, access control is required at virtual object layer also which will control interaction between cyber entities. In-built applications in cars also access on-board sensors for example, tire-pressure monitoring, lane-departure warning system etc., which must be authorized to legitimate applications only. Communication between ECUs also needs authorization using gateway or TCUs. Attribute based access controls can provide fine grained policies and use contextual information to secure data exchange and communication for both physical and virtual object layer. Hence, to secure critical ECUs first level access control restricts external interface and then in-vehicle access control provides second level check.

Connected cars generate lot of data and are referred as 'datacenters on wheels'. Applications use this data to provide real time information regarding traffic, road safety, weather, or road maintenance. Applications can also diagnose issues of vehicles and offer predictive and precautionary advices to the drivers on road. Such actions through mechanics or users via cloud must be authorized. Further, access controls are required for applications and virtual objects communication, in case any application wants to send a command to a sensor in car. Data generated can be sent to cloud servers for storage and processing. As most of these applications are relevant to geography they can harness the vehicular cloud and use its storage and processing capabilities. Data security is important in the cloud. Proper access controls are required to allow only relevant entities to access and process the data in multi-tenant data lake. Applications and cloud services must be authorized to ensure privacy of user data. The most common platform to analyze big data is Hadoop where several access control models have been proposed including [37–40]. This data can be used by applications inside vehicles or user applications at E-ACO application layer.

5.2 Multiple Cloud System

Some IoV applications and use-cases require multiple cloud instances to offer services in vast geographic area or non-time sensitive conditions. For example, assume a vehicle manufacturer has a private cloud where it gathers all data generated from its vehicles, performs analysis for potential problems and offers over the air (OTA) solutions like firmware or software updates. This data can sometimes also reflect problems in the vehicle which needs immediate attention and hence to be sent to a mechanic nearby. Now, the mechanic has its own private cloud and cannot access the vehicle's data which is stored in original equipment manufacturer (OEMs) cloud. In such a scenario, trust has to be established among two clouds so that vehicle's data can be shared between mechanic's cloud and manufacturer's cloud, with the approval of vehicle owner. If a mechanic needs to send messages to sensors in vehicle, cross cloud communication must take place between vehicular cloud (where virtual object of sensor in the car is created) and application in mechanic cloud, which also needs access controls and trust.

Applications like CarSpeak [49] gather data from different sensors not only in the same car but across different cars which may or may not be in the same vehicular cloud. In such cases, the application will access the virtual entity across different vehicular clouds also, which may require trust across different cloud infrastructures. It is also possible to have two vehicular clouds or a vehicular cloud and central cloud exchanging information. For example, suppose a vehicle is approaching the driver's home, and it needs to send a message to the thermostat to turn on the air conditioner. It is possible that the home is in a different cloud, and hence will have its cyber entity in other cloud. In such a scenario cross cloud communication will take place where the application from vehicle will communicate with the virtual object corresponding to the thermostat in the home in other cloud. Since, in this case the home and vehicle belongs to the same owner, we can create a level of trust between them across clouds and use it to make faster access decision without using policy based controls. In another example, suppose department of motor vehicle (DMV) or local police issues a notice about a stolen car or some nefarious elements in city, a vehicle dashboard will start displaying alert messages. These applications will be running in DMV cloud or cloud owned by police department, which will send messages to the cars running in the city, which also requires multi cloud access scenarios. In such cases, DMV can also have dedicated infrastructure installed around the city or highway which will receive messages over cloud and will then pass to nearby vehicles or relevant sensors (through cyber objects or WiFi communication) within a geographic area.

Hence, access controls across single and multiple cloud architectures are needed to ensure secure interaction among physical, virtual objects and applications in Internet of Vehicles ecosystem.

6 PROPOSED SECURITY FOCUSED RESEARCH AGENDA

The main objective of authorization framework and extended ACO architecture for IoV is to understand security requirements and present some security focused research directions. In this section, we will highlight some research problems as discussed below:

- **External Interaction:** The exposure of smart entities to external actors and internet opens doors for remote attacks and data theft. Connected Cars and personal devices have private data which need user-centric privacy policies where user can accept or reject the disclosure. Further, the need to control data in critical ECUs and issuing command to actuate an action must be secured by authorized entity. Trusted entities should be allowed to share more as compared to someone randomly on the road sending messages. An important question here is: How to establish trust between objects? V2X BSM messages must be encrypted and entities must be properly authenticated before performing operation. The dynamic and short-lived interaction in IoV makes it hard to prevent or detect attacks from compromised entities.
- **In-Vehicle Interaction:** The broadcast CAN communication bus and other protocols inside car are used to support ECUs and application communication using gateway. This gateway provides firewall functionality and isolates critical sensors from other applications installed in the vehicle and also provides a secure external interface. Authentication is required to prevent spoofing of ECU along with isolation of critical sensors. Data inside ECUs should be protected and over-the-air firmware updates must be secured. US GAO [30] have stated how short range communication to vehicle's Bluetooth unit can allow attackers to gain access to vehicle, also needs security. Physical tampering and direct OBD port access to ECU must be restricted.
- **Cross-Cloud Interaction and Sharing:** The cloud assisted vision of vehicular IoT supports multiple cloud or fog infrastructures. To ensure secure cross cloud or fog interactions, trust must be established between two providers which can determine the level of sharing and data exchange. IoT specific cross cloud access controls and relevant security models are still at infancy stage and need more focused attention.
- **Data in Cloud:** User and vehicle data gathered in cloud must be secured from malicious users and be shared, processed based on user and cloud provider defined privacy policies. Further cloud applications and virtual entities must be securely communicating. Also the issues related to moving vehicular cloud (VC) and its security needs require further research. The problems like virtual machine transfer when a participating vehicle leaves VC or VC formation are still not discussed broadly in literature.

7 SUMMARY

This paper provides an authorization framework for cloud assisted connected cars and vehicular IoT. It provides security requirements and discusses several access control decision and enforcements points necessary in the dynamic ecosystem of IoV. The paper first outlines some background study for relevant concepts including connected cars, virtual objects, vehicular cloud and ACO architecture. We proposed an extended ACO (E-ACO) architecture which introduces the novel concept of clustered objects (cars, infrastructure, home), which have several individual smart objects, sensors and applications. We envision IoV to have both fog and cloud instances where fog can be static or dynamically built using vehicle infrastructure or fixed roadside units. Different communication and data exchange scenarios have been discussed followed by access control approaches in E-ACO layers. Real-world use-cases with single and multi-cloud scenarios and access control requirements reflect the need and use of authorization framework for vehicular IoT. We envision to develop access control models for different communication and data exchange needs in cloud assisted connected cars and IoV based on the proposed research agenda.

ACKNOWLEDGMENTS

This work is partially supported by NSF CREST Grant HRD-1736209, NSF grants CNS-1111925, CNS-1423481, CNS-1538418 and DoD ARL Grant W911NF-15-1-0518.

REFERENCES

[1] 2014. *Connected Vehicles and Your Privacy.* https://www.its.dot.gov/factsheets/pdf/Privacy$_f$actsheet.pdf

[2] 2015. Building Autonomous and Connected Vehicle Systems with the Vortex IoT Data Sharing Platform. *Prismtech* (2015).

[3] 2016. *Convergence Of Secure Vehicular Ad-Hoc Network And Cloud In Internet Of Things.* http://mahbubulalam.com/convergence-of-secure-vehicular-ad-hoc-network-and-cloud-in-iot/ [Online; Accessed: 2018-02-01].

[4] 2017. Connected Car. (2017). https://en.wikipedia.org/wiki/Connected$_c$ar

[5] 2017. Securing The Connected Vehicle. *Thales E-Security* (2017).

[6] 2018. *Cloud IoT Core.* https://cloud.google.com/iot-core/

[7] 2018. *Device Twins.* https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins [Online; Accessed: 2018-02-03].

[8] M. Aazam and et al. 2014. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In *Proc. of IBCAST.* 414–419.

[9] A. Al-Fuqaha and et al. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Comm. Surveys & Tutorials* (2015), 2347–2376.

[10] Asma Alshehri and Ravi Sandhu. 2016. Access control models for cloud-enabled internet of things: A proposed architecture and research agenda. In *Proc. of CIC.* IEEE, 530–538.

[11] Asma Alshehri and Ravi Sandhu. 2017. Access Control Models for Virtual Object Communication in Cloud-Enabled IoT. In *Proc. of IRI.* IEEE, 16–25.

[12] Mikio Aoyama. 2012. Computing for the Next-Generation Automobile. *IEEE Computer* 45, 6 (2012), 32–37.

[13] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The internet of things: A survey. *Computer networks* 54, 15 (2010), 2787–2805.

[14] Amazon AWS. 2017. *Thing Shadows for AWS IoT.* http://docs.aws.amazon.com/iot/latest/developerguide/iot-thing-shadows.html [Accessed: 2018-01-25].

[15] Jim Barbaresso and et al. 2014. USDOT's Intelligent Transportation Systems ITS Strategic Plan 2015- 2019. (2014).

[16] S. Bhatt, F. Patwa, and R. Sandhu. 2017. An Access Control Framework for Cloud-Enabled Wearable Internet of Things. In *Proc. of CIC.* IEEE, 328–338.

[17] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. 2017. Access Control Model for AWS Internet of Things. In *Proc. of NSS.* Springer, 721–736.

[18] A. R. Biswas and R. Giaffreda. 2014. IoT and cloud convergence: Opportunities and challenges. In *Proc. of WF-IoT.* IEEE, 375–376.

[19] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. 2012. Fog computing and its role in the internet of things. In *Proc. of MCC Workshop.* ACM, 13–16.

[20] A. Botta, W. de Donato, V. Persico, and A. PescapÃľ. 2014. On the Integration of Cloud Computing and Internet of Things. In *Proc. of FiCLOUD.* IEEE, 23–30.

[21] Alessio Botta and et al. 2016. Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems* (2016), 684 – 700.

[22] David Brown et al. 2015. Automotive Security Best Practice. *Intel Security* (2015).

[23] V. G. Cerf. 2015. Access Control and the Internet of Things. *IEEE Internet Computing* 19, 5 (Sept 2015), 96–c3.

[24] J. Contreras, S. Zeadally, and J. A. Guerrero-Ibanez. 2017. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet of Things J.* (2017), 1–9.

[25] M. DÃŋaz and et al. 2016. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *J. of Network and Computer Applications* (2016), 99 – 117.

[26] A. Elmaghraby and M. Losavio. 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. *J. of advanced research* 5, 4 (2014), 491–497.

[27] Mohamed Eltoweissy and et al. 2010. Towards Autonomous Vehicular Clouds. In *Ad Hoc Networks.* Springer, 1–16.

[28] ENISA. 2017. *Cyber Security and Resilience of smart cars: Good practices and recommendations.* https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars [Online; Accessed: 2018-01-27].

[29] Y. Fangchun and et al. 2014. An overview of internet of vehicles. *China Communications* 11, 10 (2014), 1–15.

[30] US GAO. 2016, March. Vehicle Cybersecurity . *GAO-16-350* (2016, March). https://www.gao.gov/assets/680/676064.pdf

[31] Gartner. 2015. *Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities.*

[32] Gartner. 2017. *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.*

[33] M. Gerla. 2012. Vehicular cloud computing. In *Proc. of Med-Hoc-Net.* IEEE.

[34] M. Gerla, E. Lee, G. Pau, and U. Lee. 2014. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *Proc. of WF-IoT.* IEEE, 241–246.

[35] Matthew Gigli and Simon Koo. 2011. Internet of things: services and applications categorization. *Advances in Internet of Things* 1, 02 (2011), 27.

[36] J. Gubbi and et al. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems* 29, 7 (2013), 1645–1660.

[37] M. Gupta and et al. 2017. Multi-Layer Authorization Framework for a Representative Hadoop Ecosystem Deployment. In *Proc. of SACMAT.* ACM, 183–190.

[38] M. Gupta and et al. 2018. An Attribute-Based Access Control Model for Secure Big Data Processing in Hadoop Ecosystem. In *Proc. of ABAC'18.* ACM, 13–24.

[39] Maanak Gupta, Farhan Patwa, and Ravi Sandhu. 2017. Object-Tagged RBAC Model for the Hadoop Ecosystem. In *Proc. of DBSec.* Springer, 63–81.

[40] Maanak Gupta, Farhan Patwa, and Ravi Sandhu. 2017. POSTER: Access Control Model for the Hadoop Ecosystem. In *Proc. of SACMAT.* ACM, 125–127.

[41] Maanak Gupta and Ravi Sandhu. 2016. The GURA$_G$ Administrative Model for User and Group Attribute Assignment. In *Proc. of NSS.* Springer, 318–332.

[42] Sergio Gusmeroli, Salvatore Piccione, and Domenico Rotondi. 2013. A capability-based security approach to manage access control in the internet of things. *Mathematical and Computer Modelling* 58, 5 (2013), 1189–1205.

[43] J. Hernandez-Ramos and et al. 2013. Distributed capability-based access control for the internet of things. *J. of Internet Services and Info. Sec.* 3, 3/4 (2013), 1–16.

[44] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. 2004. The security and privacy of smart vehicles. *IEEE Security & Privacy* 2, 3 (2004), 49–55.

[45] Rasheed Hussain and et al. 2012. Rethinking vehicular communications: Merging VANET with cloud computing. In *Proc. of CloudCom.* IEEE, 606–609.

[46] Xin Jin, Ram Krishnan, and Ravi Sandhu. 2012. A unified attribute-based access control model covering DAC, MAC and RBAC. In *Proc. of DBSec.* Springer, 41–55.

[47] O. Kaiwartya and et al. 2016. Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access* 4 (2016), 5356–5373.

[48] Sun Kaiwen and Yin Lihua. 2014. Attribute-role-based hybrid access control in the internet of things. In *Proc. of APWeb.* Springer, 333–343.

[49] Swarun Kumar and et al. 2012. CarSpeak: A Content-centric Network for Autonomous Driving. *SIGCOMM Comput. Commun. Rev.* 42, 4 (Aug. 2012), 259–270.

[50] R. Lea and M. Blackstock. 2014. City Hub: A Cloud-Based IoT Platform for Smart Cities. In *Proc. of CloudCom.* IEEE, 799–804.

[51] U. Lee and et al. 2006. Mobeyes: smart mobs for urban monitoring with a vehicular sensor network. *IEEE Wireless Communications* (2006), 52–57.

[52] NHTSA. 2016. NHTSA and Vehicle CyberSecurity. *NHTSA Report* (2016).

[53] NHTSA. 2016, October. Cybersecurity Best Practices for Modern Vehicles. *NHTSA Report No. DOT HS 812 333* (2016, October).

[54] NIST. 2016. *Framework for Cyber-Physical Systems.* https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot [Online; Accessed: 2018-01-13].

[55] M. Nitti and et al. 2016. The virtual object as a major element of the internet of things: a survey. *IEEE Comm. Surveys & Tutorials* (2016), 1228–1240.

[56] Stephan Olariu and et al. 2011. Taking VANET to the clouds. *International Journal of Pervasive Computing and Communications* 7, 1 (2011), 7–21.

[57] Aafaf Ouaddah and et al. 2017. Access control in The Internet of Things: Big challenges and new opportunities. *Computer Networks* 112 (2017), 237–262.

[58] Christopher Poulen. 2014. Driving security: Cyber assurance for next-generation vehicles. *IBM Global Business Services* (2014).

[59] Brian Russell and et al. 2017. Observations and Recommendations on Connected Vehicle Security. *Cloud Security Alliance* (2017).

[60] Chayan Sarkar and et al. 2015. DIAT: A scalable distributed architecture for IoT. *IEEE Internet of Things journal* 2, 3 (2015), 230–239.

[61] Ludwig Seitz, Göran Selander, and Christian Gehrmann. 2013. Authorization framework for the internet-of-things. In *Proc. of WoWMoM.* IEEE, 1–6.

[62] Yunchuan Sun and et al. 2015. Security and Privacy in the Internet of Vehicles. In *Proc. of IIKI.* IEEE, 116–121.

[63] Toyota. 2011. *Toyota-to-launch-smartphone-on-wheels.* https://www.2wglobal.com/news-and-insights/articles/features/Toyota-to-launch-smartphone-on-wheels/ [Online; Accessed: 2018-02-03].

[64] European Union. 2017. *Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS).* https://ec.europa.eu/transport/sites/transport/files/c-its$_c$ertificate$_p$olicy$_r$elease$_1$.pdf

[65] European Union. 2017. *Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS).* https://ec.europa.eu/transport/sites/transport/files/c-its$_s$ecurity$_p$olicy$_r$elease$_1$.pdf

[66] USAToday. 2017. *Chinese group hacks a Tesla for the second year in a row.*

[67] USDOT. 2016. *Connected Vehicles and Your Privacy.* https://www.its.dot.gov/factsheets/pdf/Privacy$_f$actsheet.pdf

[68] USDOT. 2016. *Securty Credential Management System.* https://www.its.dot.gov/resources/scms.htm [Online; Accessed: 2018-01-13].

[69] Timo van Roermund. 2015. Secure Connected Cars for a Smarter World. *NXP Semiconductors* (2015).

[70] Evan Welbourne and et al. 2009. Building the internet of things using RFID: the RFID ecosystem experience. *IEEE Internet computing* 13, 3 (2009).

[71] Md Whaiduzzaman and et al. 2014. A survey on vehicular cloud computing. *Journal of Network and Computer Applications* 40 (2014), 325–344.

[72] Ning Ye and et al. 2014. An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics and Information Sciences* 8, 4 (2014), 1617–1624.