A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications

This paper was downloaded from TechRxiv (<https://www.techrxiv.org>).

LICENSE

CC BY 4.0

SUBMISSION DATE / POSTED DATE

23-12-2021 / 28-12-2021

CITATION

Salek, M Sabbir; Khan, Sakib Mahmud; rahman, Mizanur; Deng, Hsien-wen; islam, Mhafuzul; Khan, Zadid; et al. (2021): A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.17429510.v1>

DOI

[10.36227/techrxiv.17429510.v1](https://doi.org/10.36227/techrxiv.17429510.v1)

A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications

M Sabbir Salek, Sakib Mahmud Khan, *Member, IEEE*, Mizanur Rahman, *Member, IEEE*, Hsien-Wen Deng, Mhafuzul Islam, Zadid Khan, Mahsur Chowdhury, *Senior Member, IEEE*, and Mitch Shue

Abstract— In an internet-of-things (IoT) environment, cloud computing is emerging as a technologically feasible and economically viable solution for supporting real-time and non-real-time connected vehicle (CV) applications due to its unlimited storage, enormous computing capabilities, and cost advantage, i.e., cloud computing costs less than owning such systems. However, maintaining cybersecurity is a major challenge in cloud-supported CV applications as it requires CVs and various transportation or non-transportation services to exchange data with the cloud via multiple wired and wireless communication networks, such as long-term evolution (LTE) and Wi-Fi. In this paper, we review the cybersecurity requirements of cloud-supported CV applications, such as confidentiality, integrity, availability, authentication, accountability, and privacy. Our review also identifies the associated cybersecurity challenges that might impact cloud-supported CV applications and corresponding solutions to these challenges. In addition, we present future research opportunities to prevent and mitigate cybersecurity issues in cloud computing for CV-related applications.

Index Terms—Cloud computing, Cybersecurity, Connected vehicle, Internet of Things.

I. INTRODUCTION

A. Background and Motivation

THE advancement of intelligent transportation systems (ITS) is facilitating the development of connected vehicles (CVs) along with the infrastructure to support CV applications. CVs, which can be either human-driven or automated, communicate among themselves and/or with external transportation infrastructure and digital infrastructure to navigate efficiently through roadway traffic. CVs run many online and offline applications and produce a vast amount of data every second, which need to be stored, protected, and processed for further use as needed. The storage requirement of this vast amount of data, along with the requirements of distributed and extensive computational resources to process the data for various CV or transportation-related applications,

accelerated the introduction and usage of cloud computing for CV applications [1]–[6].

Cybersecurity is of utmost importance for cloud-supported CV applications, as security failures can break down the cloud-supported transportation system of an entire area by exposing sensitive information, increasing road users' vulnerabilities, and even causing fatal crashes. These effects can be amplified in a cloud internet-of-things (IoT) environment, where any breach of cybersecurity happening in cloud-supported CV applications can affect other IoT applications and vice versa because of similar resource sharing in an IoT environment [7], [8]. The Cloud IoT environments are emerging as lucrative targets for threat actors seeking to exploit the lack of end users' understanding of the cloud cybersecurity model. According to the 2020 Trustwave Global Security Report, the cyberattacks on cloud services nearly doubled in 2019 [9]. Among the most targeted domains for cyberattacks, cloud environments are third, following corporate and internal networks. For example, in 2016, a botnet called Mirai performed a large-scale network Denial of Service (DoS) attack and brought down several well-protected cloud services [10].

Apart from the traditional cloud infrastructure, cloud computing for supporting CV applications require sophisticated cybersecurity and privacy protection mechanisms. Cyber attackers can take advantage of cloud-enabled system loopholes and perform cyberattacks as they experience the same privileges as legitimate users. Therefore, to ensure the cybersecurity of cloud-supported applications, requirements such as confidentiality, integrity, availability, authentication, accountability, and privacy must be met along with the expected computing and storage characteristics, i.e., efficiency and flexibility of data storage and usage [7]. Although many traditional cybersecurity mechanisms are available today, they are not enough to address the cybersecurity challenges in cloud-supported CV applications [11], [12]. Cloud-supported CV applications can be compromised due to the cybersecurity issues associated with the vehicular network and the cloud.

Manuscript received April 09, 2021; revised December 23, 2021.

M. Salek, S.M. Khan, M. Islam, Z. Khan, and M. Chowdhury are with the Glenn Department of Civil Engineering, Clemson University, Clemson, SC 29634, USA (e-mail: msalek@clemson.edu, sakibk@clemson.edu, mdmhafi@clemson.edu, and mdzadik@clemson.edu).

M. Rahman is with Department of Civil, Construction and Environmental Engineering, University of Alabama, Tuscaloosa (email: mizan.rahman@ua.edu).

H. Deng, and M. Shue are with the School of Computing, Clemson University, Clemson, SC 29634, USA (e-mail: hsienwd@clemson.edu, and mshue@clemson.edu).

TABLE I
COMPARISON OF EXISTING SURVEY LITERATURE TO OUR PAPER

Survey Source	Cloud Architecture	Cybersecurity Requirements	Cybersecurity Challenges	Research Gaps in Existing Solutions to Address the Cybersecurity Challenges	Future Research Directions to Address the Cybersecurity Challenges	Mapping among Cybersecurity Requirements, Challenges, Existing Solutions and Future Research Directions
Masood et al. [12]	P	P	P	P	PP	PP
Goumidi et al. [16]	P	P	P	NP	PP	NP
Sheikh et al. [17]	P	P	P	NP	P	PP
Sharma and Kaur [18]	P	PP	P	NP	NP	NP
Whaiduzzaman [19]	P	P	P	PP	NP	NP
Yan et al. [20]	NP	PP	P	NP	PP	NP
Our paper	P	P	P	P	P	P

P = Present; PP = Partially Present; NP = Not Present

TABLE II
COMPARISON OF THE CYBERSECURITY CHALLENGES PRESENTED IN THE EXISTING SURVEY LITERATURE TO OUR PAPER

Survey Source	Cybersecurity Challenges								
	Authenticat ion	Establishing Trust	Location Validation	Secure Communication	Secure Data	Secure Heterogeneous Networks and Nodes	Scalability of Cybersecurity Solutions	Privacy	Other
Goumidi et al. [16]	P	NP	P	P	NP	P	P	P	
Sheikh et al. [17]	P	NP	P	P	P	NP	NP	NP	
Sharma and Kaur [18]	P	NP	P	P	P	NP	NP	P	User access interface
Whaiduzzaman et al. [19]	P	NP	P	P	P	P	NP	P	
Yan et al. [20]	P	P	P	NP	NP	P	P	P	
Mekki et al. [21]	P	P	P	NP	NP	NP	P	P	Security cost (bandwidth, QoS)
Our paper	P	P	P	P	P	P	P	P	

P = Present; NP = Not Present

There are many cybersecurity issues in cloud-supported CV applications, such as unregistered and malicious nodes, that can jeopardize the trustworthiness between the users in cloud-supported CV applications [13]–[15]. Moreover, ensuring the cybersecurity of a CV application becomes one of the major concerns due to the use of the wireless network, which allows other CV applications to use common resources, such as a shared communication bandwidth. Hence, CV applications and CV application developers need to have comprehensive and continuous accountability of their activities. This accountability along with the existing cybersecurity solutions will help to

ensure the cybersecurity of the overall system. Therefore, in this paper, we present a comprehensive review of existing literature on the security aspect of cloud-supported CV applications.

B. Contribution

Few papers in the literature comprehensively studied the security aspect of cloud computing for CV applications [12], [16]–[21]. Although the cybersecurity challenges are discussed in the literature, in this paper, we focus on the integrated cloud cybersecurity discussion for CV applications by mapping among the security requirements, challenges, existing

solutions, and future research directions based on the current knowledge gap. Table I presents a comparison of the existing surveys that comprehensively studied the security aspect of cloud computing for CV applications. Table II presents a list of the survey papers we reviewed and the cybersecurity challenges they discussed. As observed from Table II, most of the cybersecurity challenges presented in the other surveys are also directly covered in our paper as well. In addition, we study the challenges in detail with reference to their corresponding existing solutions, current knowledge gaps, and potential future research directions. Among the challenges that we do not directly list as high-level cybersecurity challenges (based on the other surveys listed in Table II) are (i) User access interface [18], which we discuss as “Scalability of Cybersecurity Solutions” in Subsection G of Section IV, and (v) Security cost (bandwidth, quality of service or QoS, etc.) [21], which we discuss as an issue that can be solved using 5G’s high bandwidth and low latency in “5G for Secure and Faster Communication” in Subsection D of Section V.

The primary contributions of our paper are as follows:

- Identification of the cybersecurity requirements, challenges, and future research directions to address the current knowledge gap while considering the holistic and integrated cloud-based environment to operate multiple CV applications in an IoT environment supported by any communication technology and associated protocols
- Discussion on potential future research directions based on emerging technologies and how they can serve as enablers of a secure cloud IoT environment for supporting CV applications

The rest of the paper is organized as follows: Section II discusses various components of cloud computing for CVs with their functions; Sections III and IV discuss in detail these cybersecurity requirements and existing cybersecurity challenges with solutions that have been discussed in the existing literature, respectively; future research directions for cloud computing for CV applications are discussed in Section V, followed by the conclusions in Section VI.

II. ARCHITECTURE OF CLOUD-SUPPORTED CV APPLICATIONS

In this section, we discuss the architectural components and their corresponding functions required in a cloud-supported CV application to present their cybersecurity requirements and challenges. In general, a cloud computing environment for supporting CV applications can be formed in three ways depending on the CV application type, the amount of data to process and store, and the required geometric area coverage by the CV application: (1) using only a group of CVs where the CVs communicate with each other using vehicle-to-vehicle (V2V) communication and share their physical resources such as computational and storage resources (tier 1), (2) using roadside or edge infrastructures (i.e., roadside units or RSUs) where CVs communicate with the RSUs using vehicle-to-infrastructure (V2I) communication and RSUs are connected to local servers (tier 2), or (3) using backend clouds or clouds that reside in the internet domain, such as commercial clouds (tier 3) [22]. The tier 2 formation is often referred to as Edge computing [23], [24]. A cloud formed using a group of CVs

(tier 1) or including RSUs (tier 2) can better assist small-scale and localized transportation applications, whereas backend or commercial clouds (tier 3) are capable of handling large-scale transportation applications and thus hold significant potential to serve large-scale CV applications [3].

To show the interactions among CVs, cloud, and various transportation and other infrastructures, we present a general architecture for cloud-supported CV applications in Fig. 1. CVs represent mobile nodes and can communicate directly to the cloud through various wireless networks, such as long-term evolution (LTE), 5G, and Wi-Fi, or indirectly through Roadside Data Infrastructure (RDI), such as RSUs, Traffic Control Infrastructure (TCI), such as connected roadway traffic signals, or other CVs to send Basic Safety Messages (BSMs). According to the SAE J2735 standard [25], CVs broadcast BSMs 10 times per second, which include information, such as the CVs’ location, heading, speed, and other states information. On the infrastructure side, TCI communicates with the cloud by sending its own traffic control information, such as the Signal Phase and Timing (SPaT) messages, and Traffic Management Centers (TMCs) share traffic and roadway information recorded by Traffic Management Infrastructures (TMIs). Other services, such as weather services, news services, and social media, can also be connected with the cloud. Inside the cloud, a message broker is deployed to help data producers and consumers exchange data. A message broker acts as a topic-based intermediary message routing program that operates in a publish/subscription pattern to exchange data between the CV application-related data producers and subscribed consumers of the data. Fig. 1 also presents the cybersecurity requirements and relevant challenges faced in such cloud-supported CV applications that will be discussed in detail in Sections III and IV.

Leading global cloud service providers offer commercial cloud services that can be utilized in cloud-supported CV applications. For example, Amazon Web Services (AWS) offers an IoT solution architecture for CV applications [26]; Google established a cloud platform that can support CV applications in a cloud IoT environment [27]; and Microsoft Azure offers high-performance computing services that can support CV applications[28]. The commercial cloud services can dynamically scale resources up/down depending on the demand or the number of CVs connected to the cloud at a particular time. Any cloud-supported CV applications that use CV-generated data include three types of cloud services: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Developers can utilize IaaS to set up low-level requirements of an application, such as data storage, virtual machines (VMs), and operating systems. Beyond infrastructure, PaaS provides flexible and scalable services, such as database management and computing services for developers to build their applications. Applications are implemented on the SaaS for users, where developers implement real-time or non-real-time applications according to target user requirements. Many commercial cloud service

Fig. 1. Architecture for cloud-supported CV applications and corresponding cybersecurity challenges.

providers now offer server-based as well as serverless computing services. In a server-based architecture, application developers are responsible for setting up and managing the server instances, whereas, in a serverless architecture, this role is taken care of by cloud service providers. Server-based architectures include all three types of services, i.e., IaaS, PaaS, and SaaS. On the other hand, in serverless architectures, IaaS is managed by the cloud service providers. Serverless cloud architecture, which includes PaaS and SaaS, can help to cost-effectively implement real-time CV applications [29], [30].

III. CYBERSECURITY REQUIREMENTS FOR CLOUD-SUPPORTED CV APPLICATIONS

In this section, we discuss the cybersecurity requirements of cloud computing for supporting CV applications, how these requirements can be compromised and how existing technologies could protect the cybersecurity requirements against corresponding threats or attacks. As shown in Fig. 1, the cybersecurity requirements of cloud-supported CV applications can be categorized as follows [19], [20]: 1) confidentiality, 2) integrity, 3) availability, 4) authentication, 5) accountability, and 6) privacy. These cybersecurity requirements could be

violated by various cyberattacks on data, such as data breaches and data loss [31], [32], or cyberattacks on the internal network used by the cloud or the network used by the external entities to communicate with the cloud [22].

A. Confidentiality

Confidentiality of sensitive information related to 1) CVs, such as vehicle identity (ID) authentication information, which is exchanged between the cloud and the CVs or stored in the cloud for further processing, and 2) VMs that process CV data, such as the location of VMs, is required to ensure the cybersecurity of cloud-supported CV applications. Confidentiality means controlled and authorized access to sensitive information while preventing those data from being accessed by unauthorized users or attackers. Different types of cybersecurity threats on CV data (e.g., data breach using VM Escape attack where VMs intrude the host system [33], VM location information breach using mapping of the cloud's internal infrastructure [34]) or network (e.g., eavesdropping, account or service hijacking, spoofing, and Sybil attack) can compromise confidentiality. To ensure the confidentiality of information for the cloud service users, access control models and data encryption schemes are essential. In a cloud-supported CV application, distributed and scalable access control schemes

are required. Various attribute-based access control models have been presented in the literature (e.g., ciphertext-policy attribute-based encryption [35], secure billing protocol over attribute-based encryption [36]) for preserving confidential information in cloud-supported CV applications. Along with an appropriate access control model, asymmetric or public-key cryptography is necessary for information exchange in cloud-supported CV applications [37]–[40].

B. Integrity

In cloud-supported CV applications, integrity refers to the integrity of CV data exchanged with or stored in the cloud or the integrity of the executable scripts in the cloud. CV data integrity refers to accurate, trustworthy, and reliable data related to CVs (e.g., vehicle ID, speed, and location information) which needs to be maintained over the entire data life cycle, i.e., all the stages that data go through from data creation to data deletion. In a CV environment, tampered or modified CV data can be hazardous as they can be responsible for many unacceptable and often unsafe outcomes of CV applications. For example, in a CV data modification attack, an attacker can modify the data about the surrounding environment that is being transferred from the cloud to a CV. Due to the inaccurate information about the surrounding environment (i.e., location and speed of the surrounding vehicles), a CV route guidance application can recommend an unsafe path along a route leading to a fatal or severe injury crash. Similarly, modification attacks on codes or scripts related to a CV application running in the cloud can compromise safety, especially in a cloud IoT environment where multiple IoT applications share the same countermeasure resources, including the defense scripts. The integrity requirement can be compromised by various other types of cybersecurity threats, such as data loss during data exchange, processing, and storing in the cloud [41], or cyberattacks, such as identity spoofing, repudiation, information disclosure, and Sybil attack. Unsecured cloud service/storage could compromise data integrity as they can be tampered intentionally, such as the deletion of stored data, or even unintentionally, such as users being unaware of data storage crashes. Integrity-preserving schemes, such as data- or batch-verification schemes, have been presented in the literature to preserve the integrity of data in a cloud-supported CV application [42]–[45].

C. Availability

Availability refers to the ability of authorized CVs to access and use services from the cloud whenever needed. In a CV environment, many real-time applications have a stringent requirement of an uninterrupted flow of data to and from the CVs. Therefore, ensuring timely access to cloud resources and services is mandatory for the deployment of cloud-supported CV applications. Availability can be compromised due to the loss of required data caused by cyberattacks. Various types of network attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), malware attack, blackhole attack, replay attack, and jamming attack, can compromise the availability of cloud resources [17], [46]. For example, in a DoS attack, an attacker can flood the communication channel or

consume the cloud computing resources with fake service requests so that CV application-related service requests or CV data requests from legitimate users are denied due to capacity overloads, such as communication bandwidth overload and resource overload. To protect the communication channel and make data available for legitimate CVs, trust- or cryptography-based techniques can be deployed [17].

D. Authentication

In cloud-supported CV applications, authentication refers to the process of verifying the identity of CVs communicating with the cloud and/or other CVs. Without a proper authentication method, illegitimate entities can gain access to sensitive information, which can compromise other cybersecurity requirements, such as confidentiality, integrity, and availability. Attacks, such as identity spoofing, information disclosure, brute force, and Sybil attacks can compromise authentication. The existence of mobility nodes, i.e., CVs, makes authentication challenging in a cloud-supported CV application as it constitutes dynamic nature in the network communication topology. In Section IV, we present various existing methods for secured authentication in cloud-supported CV applications, such as geographic location-based authentication [20], biometric and elliptic curve cryptography (ECC)-based authentication [47], and batch-verification schemes [42].

E. Accountability

In the context of cloud cybersecurity, accountability means keeping track of all data processors in the cloud and their corresponding data processing actions [48]–[50]. All information related to CVs, such as identity, authentication, location, and motion, must be tracked inside the cloud as these data can be randomly duplicated, transferred, and used across the cloud, which could compromise the accountability requirements. Thus, all processing of the CV data in the cloud must be continuously audited based on cybersecurity analysis, and appropriate cybersecurity mechanisms should be deployed to ensure accountability requirements are met [12], [51]. Various accountable privacy-preserving attribute-based schemes have been presented in [52]–[54] that can be adopted to fulfill the accountability requirement in cloud-supported CV applications.

F. Privacy

Private data related to cloud-supported CV applications can be classified into two categories: (i) personally identifiable information, such as CV owner information (e.g., name and phone number) and vehicle information; and (ii) sensitive information, such as CV authentication and CV location information [48]. CVs, especially connected and automated vehicles (CAVs), depend on various in-vehicle sensors to operate that produce a huge amount of data every second. Common in-vehicle sensors include Global Positioning System or GPS (collect location data for navigation), Radio Detection and Ranging or RADAR (measure distance and speed of the surrounding objects), camera (collect video data for object

detection and classification), and Light Detection and Ranging or LiDAR (generating a 3D map of the surrounding area) [55]–[57]. Location data collected by GPS or video data captured by the camera are of key privacy concerns. The US Fair Information Practices (FIP) defines the basis of the data protection and privacy laws, which includes: (i) data collection limitation, (ii) purpose specification, (iii) purpose use limitation, (iv) individual participation, and (v) visibility and transparency [58]. The ISO/IEC 27018 is among the first industry standards that defines cloud privacy in 2014 [59]. This standard provides the guidelines for the protection of personally identifiable information through six principles: consent, transparency, communication, portability/data retention, compliance, and confidentiality [48]. Microsoft Azure and AWS are examples of two cloud service providers who follow the ISO/IEC standard to comply with privacy requirements [60], [61].

IV. CYBERSECURITY CHALLENGES, SOLUTIONS AND GAPS BASED ON EXISTING STUDIES FOR CLOUD-SUPPORTED CV APPLICATIONS

We discuss the challenges, existing solutions and gaps related to the cybersecurity of cloud-supported CV applications in this section. As summarized in Table II, our list of challenges is the most comprehensive one compared to all of the six reviewed papers. In addition, Figure 1 broadly categorized the challenges into three primary groups: CVs, cloud, and communication, which map with the categories adopted by the US Department of Transportation (USDOT) [62].

We discuss the cybersecurity challenges related to cloud-supported CV applications in this section. For each challenge, we present a comprehensive literature review of the existing solution techniques. Table III presents findings from the following subsections, i.e., Subsections A to H.

A. Authentication of High Mobility Nodes

1) Challenges:

One of the challenges in securing a cloud-supported CV application is effective authentication in the presence of CVs that represent mobility with high and varying speeds. The security requirements related to this challenge are authentication and integrity. Authentication refers to the verification of the CVs' identities. CVs can authenticate themselves with the cloud using several methods, such as vehicle identification numbers (VINs), pseudonyms, security tokens, software tokens, passwords, and signatures [20]. However, the challenge is the authentication process due to the high mobility of CVs in the physical world. Usually, CVs enter and leave the transmission range of access points in a short time interval. Authentication of event-based messages (such as alerts and warnings) is associated with a location context, but with the continuous change in the network topology, it is difficult to authenticate the messages of an individual CV [19]. Authentication also depends on reliable wireless communication because it requires message exchanges between the cloud and the CVs. Unreliable wireless communication increases the probability of packet loss; as a result, the exchange

of authentication tokens, such as passwords and signatures might be lost [14]. The authentication process with security tokens needs to incorporate the cases of dynamic network topology into their system [20]. Due to the inability of traditional authentication methods, many attacks could be carried out against the cloud, such as Sybil and impersonation attacks. Identity consistency for each CV, where the same authentication credential is used to connect to multiple cloud services by different providers, is a challenge that could compromise the authentication process for CVs [63]. Messages from unauthenticated CVs can compromise the integrity of the overall cloud-supported CV application.

2) Existing Studies Addressing the Challenge and Current Gap:

Many studies have looked at solving the problem of the authentication of CVs in the cloud. In recent studies, the most popular approach for authentication of CVs in the cloud is multi-factor authentication, which utilizes the strength of different schemes, such as multiple cryptography-based authentication schemes to create a more robust and secure authentication system. For example, in [63], the authors present an integrated authentication framework using a single-server 3-factor authentication protocol and a non-interactive identity-based key establishment protocol. In [47], the authors present a biometric and ECC-assisted authentication framework for cloud computing for CVs to enhance efficiency in terms of communication and computation overhead. The method presented in [47] is able to reduce at least 42% of the computational cost to complete the cryptographic operations compared to other existing methods. Another study focuses more on message confirmation in the cloud using batch verification in the roadside edges [42]. The authors, using their developed verification method, calculate the execution time, which depends on the completion of the total required number of cryptographic operations to complete the verification. The average verification time of the developed method in [42] is 0.176 milliseconds (ms), while it varies between 1.783 ms and 30.516 ms for the existing baseline verification methods. In [20], the authors present a geographic location-based security mechanism that ensures secure authentication of CVs for V2V communication. The encryption key of the sender CV messages are geographic location keys, and the receiving CV cannot decrypt the messages if it is not within a specific geographic region. This method can be adapted for cloud-supported CV applications, where a CV cannot decrypt a message from the cloud unless it is physically within a specific geographic region. The decryption region can be dynamically changed, which makes the authentication more secure and robust. Using Artificial Intelligence (AI), the dynamically changing topology can be predicted to improve authentication algorithms, which needs to be studied in the future. The existing gaps in literature also include authentication process investigations in a real-world mobility environment with considerable CV penetration utilizing fast, secure, and reliable communication, such as 5G. Furthermore, an efficient authentication process in a virtual, software-based digital infrastructure environment needs to be investigated.

B. Establishing Trust Relationships with a High Number of CVs

1) Challenges:

Establishing trust relationships with CVs is an essential part of cloud security. The security requirements related to this challenge are confidentiality and accountability. A CV can be authenticated by the cloud as a legitimate vehicle, but cloud usage may be restricted based upon the trust relationship with the CV. Different CVs communicate with the cloud for different applications, and the cloud needs to establish a trust relationship with different CVs in real-time to initiate the service [20]. However, establishing trust with a large number of CVs in real-time poses a cybersecurity challenge. A related case is multi-hop routing, where the CVs communicate with the cloud through various agents (i.e., other CVs, roadside edges) due to network topology or application requirements. In this scenario, the cloud needs to establish trust with all the intermediate agents, such as RSUs, service providers, network channels, and secret key generators, in real-time, which adds to the computational burden of the trust establishment service [19]. The cloud needs to maintain confidentiality of CV application services by evaluating the trust on CVs and be accountable for access to different services.

2) Existing Studies Addressing the Challenge and Current Gap:

One way to establish cloud-CV trust is to use trusted middle-agents, such as the servers operated by the Department of Motor Vehicles (DMV), who have access to the CV information and can verify the CV information for the cloud [20]. In general, the use of infrastructure as a middle agent to establish the trust between CVs and the cloud is an effective strategy since the infrastructure is capable of handling trust relationships with a large number of connected agents within its domain. Another effective strategy is the distributed agent-based trust establishment technique, in which the cloud can establish a trust relationship with a leader CV elected to represent a group of CVs, in which all other CVs in that group communicate with the cloud through the leader CV [20], [64]. Other CVs can broadcast protest packets (i.e., warning message sets indicating that the information communicated by the leader CV seemed incorrect to the protesting CVs) against the leader CV if they deem the leader CV to be malicious. The cloud then examines the leader and protester CVs and re-evaluates the legitimacy of the leader CV [20], [64]. To develop better trust models for cloud-supported CV applications, edge computing can be used. In [65], the authors introduce a decoy technology (DT) and user behavior profiling (UBP) to solve trust issues in cloud servers using edge computing architecture. The edge computing-based UBP system ensures the trust relationship with the CVs in the cloud, as an intruder can be detected based on its behavior profile [65]. The authors in [65] evaluate the combination of DT (where a decoy file having scrambled content is shared with the intruder) with UBP for scenarios with up to 50 vehicles and found that the combination of both DT and UBP is more effective (minimum attack detection accuracy of 83%) in a majority of the events compared to the system which uses DT and UBP separately (minimum attack detection accuracy of 76.9%). Blockchain has also proven to be a useful technology

for ensuring trust in cloud-supported CV applications. In [66], the authors present a system called Trust Bit, which provides trust for each broadcasted data packet by CVs in all networks. The Trust Bit is a bit in the data packet sent by CVs, where the bit represents a trusted unique ID given to each CV, which the other CVs can use to gather background information about CVs in the network, thus representing the trustworthiness of vehicle actions (i.e., legal and illegal actions). In [67], biometrics are combined with blockchain technology to provide an ID-aware credit-based trust system for secure CV data sharing. The protocol presented in [67] assigns crypto data to each CV. Then, a consensus competition determines a winner CV based on the highest credit record and rewards the winner CV with an extra credit associated with its biometric ID. The winner CV then takes the lead in the communication network. Even though blockchain has been proved to be very effective in establishing trust for a high number of moving nodes in an IoT environment, seamless integration of blockchain and virtual or cloud-based transportation infrastructure (referred to as the 'Infrastructure as Code' in Section V) for cloud-based CV applications is yet to be developed. The research gaps we have identified are improving blockchain-based trust establishment systems and using Infrastructure as Code to enhance and support the trust establishment systems.

C. CV Location Validation

1) Challenges:

The security requirements related to the challenge of CV location validation are confidentiality, integrity, and authentication. The CVs broadcast BSMs every one-tenth of a second [25], which is used by the cloud to provide several services to the CVs. Most, if not all, of the services provided by the cloud depend on the accurate localization of a CV [20]. One approach for accurate and secure localization of CVs is having multiple sources of location validation data. However, cyberattacks on the GPS signal, such as jamming and spoofing, can easily compromise the location data that the CVs generate. In jamming, the GPS signal from the satellite is obstructed, so the receiver in the CV is not able to receive the signals, and the position information cannot be generated. On the other hand, a spoofing attack, in which the original signal is replaced by a fake signal which results in incorrect position information of a CV, is the most sophisticated type of attack [19], [68]. By manipulating the GPS signal, one can generate turn-by-turn spoofed data so that a CV is guided to a wrong destination [69]. For this turn-by-turn attack, an attacker manipulates the GPS signal, and an insignificant shift (in terms of distance) of the current location of a CV occurs [69]. Although a GPS signal can be cross-validated continuously using multiple GPS receiver antennas, all the antennas can be locked into the spoofed signal using multiple phase-locked spoofers during a sophisticated coordinated spoofing attack [70]. Eventually, it could compromise the reliability of cloud services for supporting CV applications. The integrity of the location data will be compromised along with the leakage of sensitive information. Moreover, the authentication of the CV also needs to be reevaluated once an attack has been detected.

2) Existing Studies Addressing the Challenge and Current Gap:

The cloud needs to deploy active or passive location validation techniques for CV locations. In terms of active validation, the cloud can access data from roadside sensors along with the BSM data from roadside devices to validate the precise location of each of the CVs [20]. The cloud can also leverage the sensor data from the in-vehicle sensors, such as camera, RADAR, and LiDAR, to locate other CVs accurately. Passive validation includes using statistical and filtering techniques to correct wrong or missing location data using previous location data and data from other CVs [20]. The cloud has been used in previous studies for CV localization and monitoring. For example, in [71], the authors develop a time of arrival (ToA) based localization algorithm that runs in the cloud. The algorithm leverages the neighboring CVs to implement more accurate localization. Using direct V2V communication, one CV can be tracked using another neighboring one, which means that if a neighboring CV can determine its own position accurately using GPS, then it can act as the reference point for calculating the location of other CVs around it. This method can be used at geographic locations with weak GPS signals and for CV location validation during jamming or spoofing attacks. In [72], Dasgupta et al. presented a prediction-based location validation strategy, i.e., a spoofing attack detection, using a long short-term memory (LSTM) model. The authors use an LSTM model to predict the distance traveled between two consecutive locations to validate the location of a vehicle using in-vehicle sensors data. Blockchain-based strategies have also been proved to be effective for ensuring the cybersecurity of information, such as data owner's location, which is used in supply chain management of transporting goods [73]. From low to medium loads (i.e., 100 to 360 mobility nodes), the authors in [73] found that the efficiency of blockchain in terms of latency was less than a second, and communication throughput was higher than 99%. In [74], blockchain is used to prevent location tracking or remote hijacking by attackers. In this study, the authors present a Lightweight Scalable Blockchain (LSB), which is a decentralized system that creates clusters of nodes managed by the cloud. The LSB has the capability to adjust its throughput utilizing a distributed throughput management (DTM) method so that the additional load on the network does not affect the network efficiency. In [75], the authors present a Cross-layer Location Verification Enhancement (CLVE) system, in which a validated entity, such as CV and roadside infrastructure, is used to verify the location of the CVs. The location validation is achieved through different networking layers, such as the physical layer, network layer, and application layer. On the physical layer, the location validation occurs directly through sensors, such as RADAR. For CVs outside the sensor range, the network layer can be used for location validation. If a CV receives a message with location information of remote CVs, the CV can confirm them by randomly challenging the positions using other CVs on bi-directional roadway traffic (i.e., roadway traffic in the same direction and the oncoming roadway traffic) using multi-hop routing. On the application layer, a CV can collect the location information of another CV from all other entities and perform information fusion to determine the correct CV location. Based on a simulation analysis, the range of

standard error for CLEV-based position estimate is 0.12-0.25, while it is 0.18-0.37 for a virtual grid-based method [75]. With increasing CV penetration in the real world, the requirement of real-time, secure, and efficient data transfer to process location data from a plethora of CVs within a short period of time will become a challenge. Thus, in the future, 5G's fast and secure communication will be effective in solving this challenge [76]. We have also identified some research gaps, such as crowdsourcing and data fusion, to enhance the algorithms for detecting and preventing CV location spoofing and using machine learning and predictive analytics to improve the CV location validation process.

D. Securing CV Communication Network

1) Challenges:

The security requirements related to CV network security are confidentiality, integrity, and availability. One of the major concerns of cybersecurity in a cloud-supported CV application is securing the communication network between the mobile edges (i.e., CVs), roadside edges (i.e., RSUs), and the cloud. Network security is a major challenge in cloud computing for CVs due to the various communication methods used by different CVs at the same time. In a cloud-supported CV application, each communication channel may have its own protocol stack and layers which need to be secured. Network security has several vulnerabilities, such as DoS, DDoS, jamming, spoofing, malware injection, communication network traffic tampering, eavesdropping, and man-in-the-middle attacks. For example, in the DoS attack, an attacker CV can start flooding the communication channel, which is being used by other CVs to communicate with the cloud. As a result, the cloud service to other CVs may be interrupted. A man-in-the-middle attack can be caused by intermediate nodes that are forwarding messages from CVs to the cloud and vice versa. The traditional security for communication channels is cryptographic algorithms. The most important part of the cryptographic algorithm is the key management system in cloud computing for supporting CV applications. Creating an efficient Vehicular Public Key Infrastructure (VPKI) is essential for secure communication [77]. In this case, one of the major challenges is the continuous generation of key pairs (i.e., private and public keys) while CVs move from one location to another quickly. CVs change association quickly from one communication access point to another, which breaks down existing communication channels and creates new channels frequently, and new key pairs need to be generated for cryptographic algorithms, which is challenging. Overall, communication network presents the problem of availability since the network always needs to be available for data exchange and security. Moreover, a compromised network endangers confidentiality and integrity requirements since a malicious attacker can gain access to any service.

2) Existing Studies Addressing the Challenge and Current Gap:

Securing the communication channel between CVs and the cloud is an important aspect of cloud cybersecurity. The most common cybersecurity technique is to use cryptographic algorithms to generate a continuous stream of private/public

key pairs for the dynamically changing vehicular environment. In [78], the authors present a novel key management protocol for securing cloud-supported CV applications. The scheme presented in [78] uses the ECC. The certification authority (CA) generates an individual unique key pair for each registered CV, which is securely stored at the CA repository using key wrapping constructors/hash functions. The CA uses a global revocation approach based on the Public Key Infrastructure Certificate Revocation List (PKI CRL) to delete keys and certificates of malicious vehicles. The authors in [78] compared the computation time to evaluate the security system's performance, and the analysis shows the group key computation time is 14 ms for keys of 512 bits, whereas it can be up to 160 ms while using any existing base model. Machine learning methods have been used to monitor the raw network data stream and detect intrusions within the network. In [79], the authors construct a convolutional neural network (CNN) model to analyze the network traffic data. In [80], the authors present a firewall scheme that they refer to as the Enhanced Intrusion Detection and Classification (EIDC) system to ensure the cybersecurity of the cloud computing environment. EIDC takes the received traffic packets as input, combines both past data with associated decisions with the current decision to estimate the final attack category classification. Blockchain has also been used to secure the communication channel between CVs and the cloud [81]. In [82], the authors combine blockchain and software-defined networking (SDN) to increase the security of the network between CVs. Using a simulation analysis, the authors in [82] show that, with over 5% malicious node, the blockchain-based detection gives 5% to 15% more accuracy than the traditional method with individual effort-based detection. In the near future, quantum computers will help further secure the CV communication/network with quantum cryptographic solutions, which future research needs to address. Other research gaps and future research directions include developing and deploying the new generation faster communication technologies (5G and beyond) and using SDN and NFV to virtualize the network and improve network security by enhancing the control over the network.

E. Securing CV Data in the Cloud

1) Challenges:

Security breach in cloud-supported CV data compromises multiple security requirements of CV applications, including confidentiality, authentication, and integrity. In cloud-supported CV applications, the CVs work as mobile nodes containing mobility attributes and position information collected from On-Board Units (OBUs) [19]. As mobile nodes, CVs share their data in a public space inside the cloud that is used by various applications. For data in the cloud, it is necessary to prevent data leakage to avoid compromising CV data confidentiality. [83]. Using the leaked information, the authentication process can be further compromised once attackers use the leaked sensitive information to have access to the cloud. Many CV applications supported by cloud computing would require developments using outsourced commercial cloud services, such as AWS, Microsoft Azure, Google Cloud, and IBM Cloud. Either a small leakage or an improper usage of CV data stored in the cloud could result in catastrophic

aftermath in the cloud-supported applications which would affect all the entities, such as CVs, dependent on those applications. Therefore, it is important to protect users' data integrity and storage correctness [84].

2) Existing Studies Addressing the Challenge and Current Gap:

Generally, encryption is used to ensure data confidentiality, integrity, and authentication. Before transmitting messages to a public cloud, CVs can utilize Rivest–Shamir–Adleman (RSA) based encryption with cryptography and signatures to prevent access by an unauthorized user [83]. This approach may fail without any verification in a malicious server. Su et al. offer a verifiable Multi-Key Searchable Encryption (MKSE) to secure the encrypted data efficiently [85]. To detect and prevent data leakage in the cloud, Lü et al. present non-interference for the cloud that allows concurrent and sequential access to the cloud to coexist [86]. Ma et al. on the other hand, developed an anti-leakage Block-level (i.e., part of a file) Client-side Deduplication (BC-Dedu) scheme for ownership management with a dynamic data storage strategy to enhance its performance (up to 57.4% computation time saving) compared to the total file-level deduplication [87]. For protecting data integrity, Li et al. present a low client cost auditing scheme for provable data integrity (PDI) in untrusted environments [88] which has 98 times lower cost than the state-of-the-art strategy (that does not consider the storage overhead of the verification metadata). Garg et al. provide an efficient approach for data integrity auditing [89]. Both [88] and [89] rely on bilinear pairing. Zhang et al. provide a security approach on storage correctness without using the PKI, which eliminates the complex certificate management. Their system uses the lattice basis delegation technique to update the private key without changing the key size [90]. Zhang et al. design an identity-based data outsourcing with public integrity verification (DOPIV), which is also a lattice-based approach that ensures post-quantum cybersecurity for cloud storage [91]. Instead of performing time-consuming tasks (such as bilinear pairing operations and modular exponentiations), this lattice-based cryptography performs fast addition and multiplication operations, which results in 154%-time savings while performing auditing tasks with 350 data blocks. While existing data encryption and data integrity auditing can help to secure CV data in the cloud, moving forward, how CV data security will be integrated into a cloud environment with virtual transportation infrastructure nodes, where the software will replace the physical transportation infrastructure operating in a multijurisdictional environment, needs to be studied. Having multiple entities, who are in control of the infrastructure node in their jurisdiction, broadens the attack surface, and future study is needed to investigate and identify appropriate technological measures to have a cybersecure transportation infrastructure as code system.

F. Securing Heterogenous Networks and Nodes

1) Challenges:

Both confidentiality and authentication can be compromised once the CV communication network and nodes are targeted and breached by attackers with malicious intents. In a cloud-supported CV application environment, CVs communicate with

each other and external infrastructure through V2V and V2I technologies, respectively. Heterogeneous networks such as the combinations of Cellular Vehicle-to-Everything (C-V2X), LTE, and 5G, can be utilized to achieve the required CV application coverage over a geographical area. In an Advanced Heterogeneous Vehicular Network (AHVN), CVs work as heterogeneous network nodes with multiple applications [92]. Typically, CVs use V2V communication to process safety-critical applications, such as collision avoidance, obstacle warning, and lane changing. Due to the dynamic, distributed, and heterogeneous nature of cloud-based CV applications, data confidentiality and authenticity can be compromised by cyberattacks. Therefore, a major cybersecurity issue for heterogeneous network nodes is to ensure a way for the nodes to protect information and trust entities with whom the information is conducted for any cloud-supported CV applications. CVs also need to prevent the risk of a jammed network channel [93]. The presence of different types of networks is accompanied by the presence of different types of nodes. From Fig. 1, we have already seen that the lower layer in the architecture for cloud-supported CV applications consists of different types of nodes, such as CVs, RDI, and TCI. Another challenge arises from different vehicle models/types of CVs, which will have different capabilities in terms of computing speed and storage. For example, different encryption and decryption algorithms will require different models/types of CVs to meet certain hardware requirements.

2) Existing Studies Addressing the Challenge and Current Gap:

To solve the cybersecurity issues related to heterogeneous networks and nodes, Mudengudi et al. present an approach to establish trust among CVs and infrastructures through an evidence-based theory which is called the Dempster Shafer Theory of Evidence (DST) [94]. Their trust framework is agent-based, as an agent is responsible for establishing trust between the cloud service providers and the users based on evidence. Hurl et al. present a method for CAV cooperative perception utilizing the TruPercept model [95]. In this model, the CAV perception observations are used for evaluating the cooperative trust among CAVs through V2V communication. Lei et al. present a blockchain-based dynamic key method to manage cybersecurity in group broadcast within a heterogeneous wireless communication environment [96], which saves almost half of the processing time compared to a centralized key management method, while transaction number (i.e., number of transactions collected by a security manager within a given transaction collection period) is less than 1500. Yang et al. also utilize the blockchain-based hierarchical trust networking to defend against DDoS over IoT devices and find that the latency of their model is much lower than the state-of-the-art model (which requires no permission) for a number of transactions varying from 1 (latency savings of 81%) to 2000 (latency savings of 93%) [97]. The current research gap includes the development of a virtualized network that will be agnostic of the heterogeneity of the CV communication medium. In network function virtualization or NFV, security functions are decoupled from physical infrastructure. In an NFV-enabled CV environment, to overcome cybersecurity challenges arising due to heterogeneous nodes (i.e., data encryption and decryption for

different vehicles), lightweight algorithms (i.e., algorithms that require modest memory usage for computation) should be developed so that all CVs can meet the computation requirements of respective applications.

G. Scalability of Cybersecurity Solutions

1) Challenges:

The cloud scalability challenge affects cybersecurity requirements related to accountability, availability, authentication, and integrity. The cloud should be able to process and generate security authentication keys for CV traffics that can vary from a small number of CVs to a large number of CVs in order to ensure cybersecurity in a cloud-supported CV application environment. Due to the mobility of the CVs, the corresponding CV network topology changes frequently. The scalability of cloud computing for CVs is a challenging issue due to these moving nodes and a frequently changing network [98], [99]. To be widely deployed, cloud-supported CV applications should be able to handle an unstable and scalable network of CVs.

2) Existing Studies Addressing the Challenge and Current Gap:

Generally, establishing a cluster network can address the scalability challenge [100]. Recently, more and more studies related to cloud computing security for supporting CV applications have considered the ability of the cloud to scale when needed. Noroozi et al. implemented a dynamic and scalable VPKE on Google Cloud Platform (GCP) that proved to be cost-effective with a large amount of traffic and achieve a five-fold improvement, due to the dynamic scalability characteristics, in processing delay compared to the existing method [101]. Lim et al. present a scalable and secure strategy for delivering keys to individual nodes in VANET [102]. Mansour et al. introduce an Asymmetric Lightweight Multicast Scalable (ALMS) group key management protocol that can enhance the scalability of VANET, which potentially could overcome key distribution limitations of symmetric key management protocols (such as the centralized protocol to secure multicast communication) [103]. Wang et al. focus on the roadside infrastructure (i.e., RSUs) to develop a blockchain-assisted trustworthiness scalable computation system for V2I authentication and improved cybersecurity in VANET [104]. The existing research gap entails having scalable cybersecurity solutions for the virtual transportation infrastructure nodes (discussed in Subsection A of Section V). Also, future studies need to incorporate network virtualization techniques to make the security solutions for cloud-supported CV applications more scalable.

H. Data Privacy in the Cloud

1) Challenges:

Privacy can be compromised because of unprotected CV user data, which are susceptible to unauthorized usage [105]–[107]. There are three key issues related to the lack of proper user access control: (i) illegitimate data handling (IDH), (ii) illegitimate data dissemination (IDD), and (iii) unauthorized secondary usage (USU) [48]. IDH occurs when the

unauthorized user performs illegal actions on the data, such as copying and modification. IDD refers to unauthorized users who disseminate data to unauthorized third parties. USU occurs when secondary usage of data by another cloud service provider occurs. After receiving data from the CVs, dynamic algorithms in the cloud need to run to transfer and store data so that outside users do not know the data location in the cloud [48]. Dynamic algorithms are responsible for the replication of data, which ensures that services are always available in case of any single point of failure [48]. However, this dynamic process can make it difficult to keep track of all copies of data and all the actions taken on each copy of the data. It becomes difficult to ensure the removal of all the copies of the data if the data owner requests the removal of their data from the cloud.

Ensuring privacy compliance depends on the following considerations: (i) privacy policies related to user preferences and (ii) enforcement mechanisms to establish privacy policies [48]. As a user (e.g., CV owner), it is difficult to be aware of all the relevant complex privacy policies and what actions will be taken in the cloud on the corresponding private data, and how it will be shared in the cloud. In addition, the enforcement process of privacy policies, such as how the dynamic nature of the cloud will be controlled and how user access can be controlled, is not comprehensive yet. There is no trivial solution for privacy policies in the context of cloud-supported CV applications, and it poses challenges to data privacy in the cloud. Currently, there are two types of policies for private data protection: (i) data owner policies [108]–[111]; and (ii) legal policies [108], [111]–[113]. However, CV users may not be aware of all the policies, and cloud users may be responsible for unusual usage of data, such as secondary usage of data.

2) Existing Studies Addressing the Challenge and Current Gap:

In [114], the authors developed a privacy-preserving authentication using RSU signature verification. The advantage of this approach is the message overhead is low. However, the key limitation is that it depends on the RSUs for verification. In another study [115], the authors developed an approach for ensuring privacy using asymmetric cryptography. This approach is related to PKI-oriented security solutions, and it depends on the PKI certificated issuance. The privacy using ID-based cryptography removes the need for ID-based cryptography and introduces the problem of pseudonym issuance [116]–[118]. In [119], [120], the authors proposed an approach for ensuring privacy using symmetric cryptography that is computationally efficient. However, a receiver is required to know the secret key. In another study [121], a group of researchers ensures privacy using group signature schemes. Although it uses the need for pseudonym change, the limitation of this study is pseudonym resolution and revocation. In [122], a privacy scheme using access control and trust using geolocation was presented. However, this approach provides only access control of the private messages, and management schemes are unknown. In [123], the authors used encryption and decryption outsourcing mechanisms and developed an access control framework based on fog-to-cloud architecture. This approach ensures message confidentiality, access control, and vehicle authentication. However, it is difficult to maintain authentication credentials because of the dynamic nature of

vehicles, and fog nodes are semi-trusted and may not follow appropriate access control. Another study [124] presents an authentication scheme for vehicular communication in a multi-cloud environment. The authors in [124] evaluated the computational and communication latency, and they found that the latency for their authentication scheme is satisfactory for applications related to connected vehicles. In [125], the authors presented a cloud-enabled privacy-preserving truth discovery (PPTD) framework to protect moving users' personal information from their smartphone through crowdsensing, such as readings of compass, accelerometer, and gyroscope, to identify the indoor floor plan. The PPTD framework uses a homomorphic cryptosystem, which uses encrypted data for the application without directly decrypting it, for guaranteeing data privacy. They evaluated the cloud-based PPTD framework's processing time for the indoor floor plan identification application using data from moving smartphone users. The authors in [125] found that, for each smartphone user, the total processing time is only 0.039s, which was satisfactory for the cloud-based indoor floor identification application.

In [126], the authors develop an obfuscation technique that utilizes a middleware data obfuscator integrated into the cloud infrastructure to ensure privacy protection and prevent IDH, IDD, and USU issues. In [127], the authors introduce a middleware for deploying certifiable and auditable applications to process data in the cloud, which can prevent IDH, IDD, and USU issues through high-level enforcement resilience. In [128], the authors develop a data flow tracking model to keep track of data across system users. Some studies focus on dynamic models for distributed data tracking to track each host [129]–[131]. Also, data monitoring and auditing techniques are developed for data tracking, which ensures who is processing the data and what actions are taking place on data in the cloud [132], [133]. Instead of data monitoring and auditing techniques, some techniques enable data usage control requirements, which is referred to as retention obligation enforcement, for keeping track of data usage [128], [129]. Data segmentation, obfuscation, and encryption techniques have been developed for ensuring the confidentiality of data following data owner policies as well as legal policies [126], [134]–[136]. In addition to this data level policy compliance, some enforcement mechanisms have been developed to enforce policies at application and hardware levels to support data protection [108]–[110]. Beyond these existing privacy-protecting solutions, further studies are needed on the development of privacy solutions related to IDH, IDD, and USU, considering the dynamic interaction between CVs and cloud to make real-world cloud-supported CV applications a reality.

TABLE III
COMPROMISED REQUIREMENTS, EXISTING SOLUTIONS, AND FUTURE RESEARCH DIRECTIONS RELATED TO CYBERSECURITY CHALLENGES IN CLOUD-SUPPORTED CV APPLICATIONS

Cybersecurity Challenges of Cloud-Supported CV Applications (See Section IV for details)	Compromised Cybersecurity Requirements (See Section III for details)	Existing Cybersecurity Solutions (See Section IV for details)	Future Research Directions for Addressing Current Knowledge Gap (See Section V for details)
Related to Cloud			
Securing CV data in the cloud	<ul style="list-style-type: none"> Confidentiality Integrity Authentication 	<ul style="list-style-type: none"> Multi-Key Searchable Encryption (MKSE) [85] Block-level Client-side Deduplication (BC-Dedu) [87] Bilinear pairing-based data integrity auditing [88], [89] Data Outsourcing with Public Integrity Verification (DOPIV) [91] 	Leverage the Infrastructure as Code to provide CV data security solutions
Scalability of cloud security solutions	<ul style="list-style-type: none"> Accountability Availability Authentication Integrity 	<ul style="list-style-type: none"> Commercial cloud-based Vehicular Public Key Infrastructure (VPKI) [101] Asymmetric lightweight centralized group key management [103] Blockchain assisted trustworthiness [104] 	Implement the network virtualization techniques along with Infrastructure as Code to make the cybersecurity solutions for cloud-supported CV applications more scalable
Data privacy in the cloud	Privacy	<ul style="list-style-type: none"> Authentication using RSU signature verification [114] Privacy-preserving schemes using cryptography [115]-[120] Group signature scheme [121] Access control and trust using geolocation [122] Fog-to-cloud data sharing architecture with outsourced encryption and decryption mechanisms [123] Conditional privacy protection authentication scheme [124] Privacy-Preserving Truth Discovery (PPTD) framework [125] Integrating middleware data obfuscator [126] Integrating middleware for deploying certifiable and auditable applications [127] Data tracking, monitoring, and auditing [128]-[133] Data retention obligation [128], [129] Data segmentation and encryption [134]-[136] Privacy policy enforcement mechanisms [109]-[111] 	Develop privacy solutions related to illegitimate data handling (IDH), illegitimate data dissemination (IDD), and unauthorized secondary usage (USU) considering the dynamic interaction between CVs and cloud, and utilizing the blockchain-AI, and secure quantum machine learning and cryptographic techniques
Related to Communication			
Securing CV communication network	<ul style="list-style-type: none"> Confidentiality Integrity Availability 	<ul style="list-style-type: none"> Elliptical Curve Cryptography (ECC) [78] Public Key Infrastructure Certificate Revocation List (PKI CRL) [78] Machine learning [79], [80] Blockchain [81], [82] Software-Defined Networking (SDN) [82] 	Develop Infrastructure as Code to secure network, and quantum machine methods to create unbreakable cryptographic solutions to secure the communication
Securing heterogenous networks and nodes (i.e., CVs)	<ul style="list-style-type: none"> Confidentiality Authentication 	<ul style="list-style-type: none"> Establishing trust between CVs and infrastructure [94] Blockchain-based dynamic key method [96] Blockchain-based hierarchical trust networking [97] 	Develop lightweight security solutions inside a virtualized network that will be agnostic of the heterogeneity of the CV communication medium
Related to Connected Vehicles (CVs)			
Authentication of CVs (i.e., high mobility nodes)	<ul style="list-style-type: none"> Integrity Authentication 	<ul style="list-style-type: none"> Geographic location-based authentication [2] Multi-factor authentication [63] Biometric and Elliptic Curve Cryptography (ECC)-based authentication [47] Batch verification [42] 	Develop Infrastructure as Code to manage authenticity of CVs enabled with 5G communication
CV location Validation	<ul style="list-style-type: none"> Confidentiality Integrity Authentication 	<ul style="list-style-type: none"> Roadside sensor-based active validation [20] Statistical and filtering methods for correction [20] Crowdsourcing [71] Prediction-based location validation using neural network [72] Lightweight Scalable Blockchain (LSB) [74] Cross-layer Location Verification Enhancement (CLVE) [75] 	Leverage 5G's faster communication to transfer data into the cloud to validate the location information
Establishing trust relationships with a high number of CVs	<ul style="list-style-type: none"> Confidentiality Accountability 	<ul style="list-style-type: none"> Trusted middle agent [20] Distributed agent-based trust establishment [20], [64] Edge computing-based User Behavior Profiling (UBP) [65] Blockchain-based Trust Bit [66] Blockchain combined with biometrics [67] 	Ensure trust with the integration of Infrastructure as Code and Blockchain, and develop methods for suitable and seamless integrations

V. FUTURE RESEARCH DIRECTIONS FOR CYBERSECURITY OF CLOUD-SUPPORTED CV APPLICATIONS

In this section, we present potential future research directions related to the cybersecurity of cloud-supported CV applications (also included in Table III) that can be pursued in the future.

A. *Infrastructure as Code*

In the future, the physical transportation infrastructure will be replaced with a cloud or virtual infrastructure that will be defined in code. This will enable managing and provisioning the infrastructure through software in an automated manner, rather than configuring the hardware manually. Also, there will be increasing instances where the hardware components will be replaced by software. Such Infrastructure as Code can solve the cybersecurity challenges related to authentication of mobile nodes with high and varying speeds, such as CVs, which will support trust relationships with a large number of CVs in a cloud-supported CV application environment. Virtual traffic light control is an example of Infrastructure as Code. In this system, no physical traffic light control is required, and the traffic signal phase and timing are determined by the incoming vehicles or cloud-based infrastructure. Being programmable, portable, and easily expandable, this Infrastructure as Code system will be able to mitigate the challenges related to the scalability of cloud-based cybersecurity solutions. Also, while a communication network is compromised due to a DoS attack, cloud-based virtual traffic signal servers can be migrated automatically to a different domain or server, and the service can be restored immediately. The infrastructure nodes will enhance the cloud-based depth-in-defense (DID) system. In DID, multiple security barriers in the forms of security software, such as firewalls and hardware, are placed to prevent the attackers from having access to their desired targets [137]. Having the programmable infrastructure nodes with added cybersecurity mechanisms will enhance the overall system's cybersecurity and will address the existing challenges of mobile node authentication and trust establishment for a high number of CVs, scalable security solutions, as well as securing CV communication and CV data. Furthermore, the security functions in the cloud will replace the hardware security modules (HSM) that exist to secure the hardware components through encryption and authentication. Thus, the physical hardware that provides security to the CVs (e.g., HSM) could be replaced by the infrastructure as code cybersecurity modules in the cloud.

B. *Integration of Blockchain with AI*

Blockchain is one of the evolving cybersecurity technologies which shows potential for ensuring the cybersecurity of cloud-supported applications. Blockchain technology works based on the identification of and trust between two transacting parties. Blockchain cybersecurity is based on peer-to-peer (P2P) network fundamentals [66], [67]. To establish trust between a high number of CVs, blockchain technology helps each CV to authenticate the arriving data. Blockchain can be used to trust the connected entities and permit access to a cloud entity. Blockchain technology-based security can be enhanced if integrated with AI, where AI will enable pattern recognition of the underlying data and establish a robust trusted system by

incorporating AI-based cyberattack detection and mitigation strategies. However, the process of integrating blockchain, AI, and IoT for a CV-like large network system is not yet implemented [138]–[140]. Though blockchain is being used to secure cloud interactions, much research needs to be done on the widespread implementation of the integration of AI and blockchain technology-enabled cybersecurity in the cloud-supported CV application environment. Thus, research in this direction will help the industry adopt blockchain-based cybersecurity solutions for establishing trust among the CVs and securing cloud architecture for supporting CV applications.

C. *Quantum Computing for Machine Learning*

Quantum computing in the cloud has the potential to revolutionize industries in a similar way as other emerging technologies, such as AI-enabled technologies. Quantum computers incorporate quantum phenomena into processing power to achieve better computing capability compared to classical computers. If users are allowed access to quantum computers via the internet, then it is known as quantum-as-a-service (QaaS) in the cloud. The cloud is getting reshaped by using the higher processing capabilities of quantum computers. Though existing quantum computers are not portable enough to support an operation inside a vehicle, cloud-supported quantum computers are gaining momentum, such as IBM quantum computers, which are accessible through the IBM cloud. To overcome cybersecurity challenges in cloud-supported CV applications, such as securing CV communication and ensuring privacy compliance, quantum computing-based machine learning, and cryptographic solutions will be effective. Using quantum computers, we will be able to process a vast amount of data to detect anomalies in high-volume and high-velocity data in a very short period which can be very useful for validating CV locations. Such processing capabilities will be able to detect cyberattacks and compute complex mitigation strategies quickly. For example, a cloud-supported hybrid-classical quantum system was used to detect an in-vehicle cyberattack in [141]. Recent developments on the quantum key distribution (QKD) aim to reduce the possibility of cyberattacks on the network, which might include the cloud as well. Quantum machine learning can supplement QKD in securing cloud computing for supporting CV applications as well as quantum computing. However, quantum computing also poses threats to the current cryptographic schemes incorporated in today's computer systems, as future attackers may be able to decipher encrypted information using quantum computers [142]. To make cloud-supported CV applications safe from threats posed by quantum computers, research on post-quantum cryptography [143] needs to be conducted.

D. *5G for Secure and Faster Communication*

5G is considered an enabler of IoT technologies. Smart cities rely on IoT to reduce traffic congestion, meet water distribution needs, increase cybersecurity, and even decrease pollution. Moreover, with 5G's low communication delay characteristic, it could potentially support cybersecurity solutions for cloud-supported CV applications, where fast communication is required between the CVs and the cloud. 5G offers two major

advantages over 4G and LTE networks: ultra-low latency and high data rate. CVs can connect instantly with the cloud through 5G and leverage the cloud services for in-vehicle cybersecurity. In the case of CAVs, which are equipped with various types of in-vehicle sensors, the high data rate will allow them to share the large amount of in-vehicle data generated from sensors. This data can be used for authentication and location validation of CVs, which will be helpful to secure cloud-supported CV applications by detecting and mitigating cyberattacks. A 5G network is inherently more secure than a 4G and LTE network due to several new additions in the standards (5G New Radio or 5G NR) such as anti-tracking and network slicing. However, 5G has its own cybersecurity vulnerabilities, some of which have been inherited from 4G, such as threats from cell-site simulators (also known as Stingrays), and some of which are unique issues, such as mass network failure due to shared infrastructure. Any failure in the underlying network between the CVs and the cloud potentially compromises cloud-supported CV applications, so more research is required on the cybersecurity of 5G.

E. Heterogeneous Wireless Networking

Heterogeneous wireless networking refers to the usage of different communication options, such as C-V2X, LTE, Wi-Fi, and 5G, while CVs are moving along a roadway. CVs need to leverage different communication options and perform efficient handovers between communication access points (AP) and base stations (BS) to maintain connectivity with the cloud. The network between the cloud and the CVs is susceptible to cyberattacks during horizontal handover – i.e., handoff between AP/BS using the same wireless communication technology, and vertical handover – i.e., handoff between AP/BS using different wireless communication technologies. Innovative key exchange protocols can be introduced to maintain faster data transmission while protecting the network during the handover process. A secure handover management process is crucial to ensure cloud cybersecurity since the cloud can be compromised through the underlying network connecting CVs with the cloud. SDN can be combined with the cloud to develop more robust and secure handover management systems for cloud-supported CV applications.

F. Network Function Virtualization

Whereas network security functions (e.g., intrusion detection systems (IDS) and firewalls) are deployed in proprietary hardware in legacy systems, virtualization of such security functions, which is referred to as network function virtualization (NFV), can provide a cost-effective solution to the cybersecurity of cloud-supported CV applications. Isolating the network security functions is one of the key features of NFV, which can decouple the dependency among cloud components, such as IaaS, PaaS, and SaaS, thus making the security barriers harder to penetrate by cyber attackers. NFV-based cybersecurity solutions can run on top of off-the-shelf hardware – e.g., industry-standard storage, servers, and switches. Compared to security functions running in proprietary hardware, virtualized cloud network security functions can provide same-level or even better performance [144]. Virtual

networks are also isolated from the underlying physical infrastructure. Thus, even if the physical infrastructure is compromised, virtual networks can continue their operation normally. The cloud cybersecurity architecture needs to be re-defined while the NFV is being integrated into the cloud IoT environment for cloud-supported CV applications. We can operate distributed and lightweight cybersecurity algorithms (with small memory usage requirements) using NFV in cloud-supported CV applications. Research on the integration of network visualization techniques with cloud-supported CV applications is needed to take full advantage of the NFV. NFV can help solve the cybersecurity challenges, such as securing the heterogeneous network of the CV nodes and scalability of cloud cybersecurity solutions for cloud-supported CV applications.

VI. CONCLUSION

This paper presents an in-depth review of the cybersecurity of cloud computing from the perspective of CV applications. Based on the review, we discuss the cybersecurity requirements of cloud-supported CV applications in terms of confidentiality, integrity, availability, authentication, accountability, and privacy. Moreover, existing cybersecurity techniques and technologies to meet these cybersecurity requirements and corresponding threats or cyberattacks related to cloud-supported CV applications are discussed. However, many cybersecurity challenges, which arise from CVs, need to be addressed, such as authentication, establishing trust relationships between CVs, and between the CVs and the cloud infrastructure, validating CV location, securing CV data and communication network, scalability of cybersecurity solutions, and data privacy. We identify these challenges for cloud-supported CV applications and discuss the corresponding existing cybersecurity solutions through a review of published studies. While existing and potential cybersecurity measures presented in this paper provide cyber-defenses, their respective efficiency is an important consideration for their real-world adoption related to various cloud-enabled CV applications based on their corresponding communication and computational latency requirements.

As technology advances rapidly, new possibilities emerge to protect cloud-supported CV applications. Potential future research opportunities are identified in this paper to prevent and mitigate the cybersecurity issues related to cloud-supported CV applications. Flexible and dynamic nature of infrastructure as code, the decentralized and immutable property of blockchain, high-speed computing capability of quantum computers, high bandwidth and low latency of 5G network, heterogeneous wireless networking, and cloud network virtualization have the potential to address existing and future cybersecurity challenges in cloud-supported CV applications. Our security challenges are classified to meet the six cybersecurity requirements of cloud-supported CV applications (shown in Figure 1). Although our cyberattack challenge categories are comprehensive, they may not be complete, especially with the evolving cyber-threats of the future. New cybersecurity challenges can emerge and pose new threats to cloud-supported CV applications as technology evolves, which are to be investigated in future studies. In the future, a cyberattack that

uses quantum computers could be a major threat to prevailing cyber defenses, including cloud-supported CV applications, for example. As cloud computing can provide technologically feasible and economically viable solutions for supporting CV applications, the proposed solutions can help develop new cybersecurity architectures and protocols for addressing evolving cybersecurity issues.

REFERENCES

- [1] A. Seal and A. Mukherjee, "Real Time Accident Prediction and Related Congestion Control Using Spark Streaming in an AWS EMR cluster," in *2019 SoutheastCon*, Apr. 2019, pp. 1–7. doi: 10.1109/SoutheastCon42311.2019.9020661.
- [2] A. Bhatnagar, V. Sharma, and G. Raj, "IoT based Car Pollution Detection Using AWS," in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Jun. 2018, pp. 306–311. doi: 10.1109/ICACCE.2018.8441730.
- [3] H.-W. Deng, M. Rahman, M. Chowdhury, M. S. Salek, and M. Shue, "Commercial Cloud Computing for Connected Vehicle Applications in Transportation Cyberphysical Systems: A Case Study," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 6–19, Spring 2021, doi: 10.1109/ITS.2020.3037314.
- [4] M. Amarasinghe, S. Kottegoda, A. L. Arachchi, S. Muramudalige, H. M. N. D. Bandara, and A. Azeez, "Cloud-based driver monitoring and vehicle diagnostic with OBD2 telematics," in *2015 Fifteenth International Conference on Advances in ICT for Emerging Regions (ICTer)*, Aug. 2015, pp. 243–249. doi: 10.1109/ICTER.2015.7377695.
- [5] A. Ghose, P. Biswas, C. Bhaumik, M. Sharma, A. Pal, and A. Jha, "Road condition monitoring and alert application: Using in-vehicle Smartphone as Internet-connected sensor," in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, Mar. 2012, pp. 489–491. doi: 10.1109/PerComW.2012.6197543.
- [6] Y. Du *et al.*, "A Distributed Message Delivery Infrastructure for Connected Vehicle Technology Applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 787–801, Mar. 2018, doi: 10.1109/TITS.2017.2701799.
- [7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.
- [8] B. Omoniwa, R. Hussain, M. A. Javed, S. H. Bouk, and S. A. Malik, "Fog/Edge Computing-Based IoT (FECIoT): Architecture, Applications, and Research Issues," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4118–4149, Jun. 2019, doi: 10.1109/JIOT.2018.2875544.
- [9] "2020 Trustwave Global Security Report," 2020. [Online]. Available: <https://trustwave.azureedge.net/media/16717/2020-trustwave-global-security-report.pdf?rnd=132319806410000000>
- [10] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.
- [11] S. Sharma and A. Kaul, "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud," *Vehicular Communications*, vol. 12, pp. 138–164, Apr. 2018, doi: 10.1016/j.vehcom.2018.04.005.
- [12] A. Masood, D. S. Lakew, and S. Cho, "Security and Privacy Challenges in Connected Vehicular Cloud Computing," *IEEE Communications Surveys Tutorials*, vol. 22, no. 4, pp. 2725–2764, Fourthquarter 2020, doi: 10.1109/COMST.2020.3012961.
- [13] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.
- [14] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, Apr. 2014, doi: 10.1016/j.vehcom.2014.05.001.
- [15] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.
- [16] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular Cloud Computing Security: A Survey," *Arab J Sci Eng*, vol. 45, no. 4, pp. 2473–2499, Apr. 2020, doi: 10.1007/s13369-019-04094-0.
- [17] M. S. Sheikh, J. Liang, and W. Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey," *Wireless Communications and Mobile Computing*, vol. 2020, Jan. 2020, doi: 10.1155/2020/5129620.
- [18] M. K. Sharma and A. Kaur, "A survey on Vehicular Cloud Computing and its security," in *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, Sep. 2015, pp. 67–71. doi: 10.1109/NGCT.2015.7375084.
- [19] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, Apr. 2014, doi: 10.1016/j.jnca.2013.08.004.
- [20] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 284–294, Mar. 2013, doi: 10.1109/TITS.2012.2211870.
- [21] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," *Vehicular Communications*, vol. 9, pp. 268–280, Jul. 2017, doi: 10.1016/j.vehcom.2016.11.009.
- [22] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular Cloud Networks: Architecture, Applications and Security Issues," in *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, Dec. 2015, pp. 571–576. doi: 10.1109/UCC.2015.101.
- [23] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, "Edge Computing for Autonomous Driving: Opportunities and Challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1697–1716, Aug. 2019, doi: 10.1109/JPROC.2019.2915983.
- [24] S. Raza, S. Wang, M. Ahmed, and M. R. Anwar, "A Survey on Vehicular Edge Computing: Architecture, Applications, Technical Issues, and Future Directions," *Wireless Communications and Mobile Computing*, vol. 2019, Feb. 2019, doi: 10.1155/2019/3159762.
- [25] "J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary™ - SAE International," Nov. 19, 2009. https://www.sae.org/standards/content/j2735_200911/ (accessed Mar. 20, 2021).
- [26] "Connected Vehicle Solution | Implementations | AWS Solutions," *Amazon Web Services, Inc.* <https://aws.amazon.com/solutions/implementations/aws-connected-vehicle-solution/> (accessed Jun. 26, 2020).
- [27] "Designing a Connected Vehicle Platform on Cloud IoT Core | Solutions," *Google Cloud*. <https://cloud.google.com/solutions/designing-connected-vehicle-platform> (accessed Jun. 26, 2020).
- [28] "Azure High-Performance Computing for Automotive | Microsoft Azure." <https://azure.microsoft.com/en-us/solutions/high-performance-computing/automotive/> (accessed Jun. 26, 2020).
- [29] P. F. Pérez-Arteaga, C. C. Castellanos, H. Castro, D. Correal, L. A. Guzmán, and Y. Denneulin, "Cost Comparison of Lambda Architecture Implementations for Transportation Analytics using Public Cloud Software as a Service," in *Proceedings of the 13th International Conference on Software Technologies*, Porto, Portugal, 2018, pp. 855–862. doi: 10.5220/0006869308550862.
- [30] I. Baldini *et al.*, "Serverless Computing: Current Trends and Open Problems," in *Research Advances in Cloud Computing*, S. Chaudhary, G. Somani, and R. Buyya, Eds. Singapore: Springer Singapore, 2017, pp. 1–20. doi: 10.1007/978-981-10-5026-8_1.
- [31] Top Threats Working Group and others, "The notorious nine: cloud computing top threats in 2013." 2013. Accessed: Apr. 04, 2021. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

- [32] M. Kazim and S. Ying, "A survey on top security threats in cloud computing," *IJACSA*, vol. 6, no. 3, 2015, doi: 10.14569/IJACSA.2015.060316.
- [33] K. Kortchinsky, "Cloudburst." Jun. 02, 2009. Accessed: Apr. 04, 2021. [Online]. Available: <https://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf>
- [34] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, New York, NY, USA, Nov. 2009, pp. 199–212, doi: 10.1145/1653662.1653687.
- [35] Z. Guan, J. Li, Z. Zhang, and L. Zhu, "Conditional Ciphertext-Policy Attribute-Based Encryption Scheme in Vehicular Cloud Computing," *Mobile Information Systems*, vol. 2016, Nov. 2016, doi: 10.1155/2016/1493290.
- [36] L. Nkenyereye, Y. Park, and K. H. Rhee, "A secure billing protocol over attribute-based encryption in vehicular cloud computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, p. 196, Aug. 2016, doi: 10.1186/s13638-016-0687-0.
- [37] K. El Makkaoui, A. Beni-Hssane, and A. Ezzati, "Speedy Cloud-RSA homomorphic scheme for preserving data confidentiality in cloud computing," *J Ambient Intell Human Comput*, vol. 10, no. 12, pp. 4629–4640, Dec. 2019, doi: 10.1007/s12652-018-0844-x.
- [38] K. El Makkaoui, A. Beni-Hssane, A. Ezzati, and A. El-Ansari, "Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing," *Procedia Computer Science*, vol. 113, pp. 33–40, Jan. 2017, doi: 10.1016/j.procs.2017.08.282.
- [39] P. Li *et al.*, "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, Sep. 2017, doi: 10.1016/j.future.2017.02.006.
- [40] K. Benzekki, A. E. Fergougui, and A. Abdelbaki El Belrhiti El, "A Secure Cloud Computing Architecture Using Homomorphic Encryption," *IJACSA*, vol. 7, no. 2, pp. 293–298, 2016.
- [41] M. Armbrust *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
- [42] T. Limbasiya and D. Das, "Secure message confirmation scheme based on batch verification in vehicular cloud computing," *Physical Communication*, vol. 34, pp. 310–320, Jun. 2019, doi: 10.1016/j.phycom.2018.07.015.
- [43] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure Real-Time Traffic Data Aggregation With Batch Verification for Vehicular Cloud in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 807–817, Jan. 2020, doi: 10.1109/TVT.2019.2946935.
- [44] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," *Tsinghua Science and Technology*, vol. 21, no. 6, pp. 620–629, Dec. 2016, doi: 10.1109/TST.2016.7787005.
- [45] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. G. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Generation Computer Systems*, vol. 78, pp. 943–955, Jan. 2018, doi: 10.1016/j.future.2016.11.024.
- [46] I. A. Sumra, H. B. Hasbullah, and J. B. AbManan, "Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey," in *Vehicular Ad-hoc Networks for Smart Cities*, Singapore, 2015, pp. 51–61, doi: 10.1007/978-981-287-158-9_5.
- [47] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, "SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing," *International Journal of Communication Systems*, vol. n/a, no. n/a, p. e4103, Jul. 2019, doi: 10.1002/dac.4103.
- [48] A. Ghorbel, M. Ghorbel, and M. Jmaiel, "Privacy in cloud computing environments: a survey and research challenges," *J Supercomput*, vol. 73, no. 6, pp. 2763–2800, Jun. 2017, doi: 10.1007/s11227-016-1953-y.
- [49] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1–48, Aug. 2019, doi: 10.1016/j.cosrev.2019.05.002.
- [50] "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," *Cloud Security Alliance*, Jul. 26, 2017, <https://cloudsecurityalliance.org/artifacts/security-guidance-v4/> (accessed Apr. 05, 2021).
- [51] M. Aladwan, F. Awaysheh, J. Cabaleiro, T. Pena, H. Alabool, and M. Alazab, "Common Security Criteria for Vehicular Clouds and Internet of Vehicles Evaluation and Selection," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2019, pp. 814–820, doi: 10.1109/TrustCom/BigDataSE.2019.00118.
- [52] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds," *Journal of Parallel and Distributed Computing*, vol. 135, pp. 1–20, Jan. 2020, doi: 10.1016/j.jpdc.2019.08.014.
- [53] H. Cheng, C. Rong, M. Qian, and W. Wang, "Accountable Privacy-Preserving Mechanism for Cloud Computing Based on Identity-Based Encryption," *IEEE Access*, vol. 6, pp. 37869–37882, 2018, doi: 10.1109/ACCESS.2018.2851599.
- [54] J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, and D. Wang, "Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT," *IEEE Transactions on Cloud Computing*, pp. 1–1, 2020, doi: 10.1109/TCC.2020.2975184.
- [55] A. Sarker *et al.*, "A Review of Sensing and Communication, Human Factors, and Controller Aspects for Information-Aware Connected and Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 1, pp. 7–29, Jan. 2020, doi: 10.1109/TITS.2019.2892399.
- [56] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Self-driving and connected cars: Fooling sensors and tracking drivers," presented at the Black Hat Europe, 2015.
- [57] E. Guizzo, "How google's self-driving car works," *IEEE Spectrum Online*, 2011, <https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works> (accessed Apr. 05, 2021).
- [58] C. F. Libaque-Sáenz, S. F. Wong, Y. Chang, and E. R. Bravo, "The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps," *Information & Management*, p. 103284, Feb. 2020, doi: 10.1016/j.im.2020.103284.
- [59] P. De Hert, V. Papakonstantinou, and I. Kamara, "The New Cloud Computing ISO/IEC 27018 Standard Through the Lens of the EU Legislation on Data Protection," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2542125, Dec. 2014, doi: 10.2139/ssrn.2542125.
- [60] "ISO/IEC 27018:2019 Compliance - Amazon Web Services (AWS)," *Amazon Web Services, Inc.*, <https://aws.amazon.com/compliance/iso-27018-faqs/> (accessed Apr. 05, 2021).
- [61] L. Woehler, "Microsoft Azure: The first cloud computing platform to conform to ISO/IEC 27018, the only international set of privacy controls in the cloud," Feb. 16, 2015, <https://azure.microsoft.com/en-us/blog/azure-first-cloud-computing-platform-to-conform-to-isoiec-27018-only-international-set-of-privacy-controls-in-the-cloud/> (accessed Feb. 14, 2021).
- [62] USDOT, "How the U.S. Department of Transportation is Protecting the Connected Transportation System from Cyber Threats," <https://www.its.dot.gov/factsheets/cybersecurity.htm> (accessed Dec. 19, 2021).
- [63] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing," *IEEE Network*, vol. 32, no. 3, pp. 28–35, May 2018, doi: 10.1109/MNET.2018.1700347.
- [64] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, Jul. 2008, doi: 10.1016/j.comcom.2008.01.009.
- [65] M. Boussselham, N. Benamar, and A. Addaim, "A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System," in *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, Apr. 2019, pp. 1–4, doi: 10.1109/WITS.2019.8723723.
- [66] M. Singh and S. Kim, "Trust Bit: Reward-based intelligent vehicle commination using blockchain paper," in *2018 IEEE 4th World*

- Forum on Internet of Things (WF-IoT)*, Feb. 2018, pp. 62–67. doi: 10.1109/WF-IoT.2018.8355227.
- [67] B. Xu, T. Agbele, and R. Jiang, “Biometric Blockchain: A Secure Solution for Intelligent Vehicle Data Sharing,” in *Deep Biometrics*, R. Jiang, C.-T. Li, D. Crookes, W. Meng, and C. Rosenberger, Eds. Cham: Springer International Publishing, 2020, pp. 245–256. doi: 10.1007/978-3-030-32583-1_11.
- [68] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques,” *International Journal of Navigation and Observation*, vol. 2012, p. e127072, Jul. 2012, doi: 10.1155/2012/127072.
- [69] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, “A Practical GPS Location Spoofing Attack in Road Navigation Scenario,” in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, New York, NY, USA, Feb. 2017, pp. 85–90. doi: 10.1145/3032970.3032983.
- [70] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, and P. M. Kintner, “Assessing the spoofing threat: Development of a portable GPS civilian spoofer,” in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314–2325.
- [71] Y. Agarwal, K. Jain, and O. Karabasoglu, “Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks,” *International Journal of Transportation Science and Technology*, vol. 7, no. 1, pp. 60–73, Mar. 2018, doi: 10.1016/j.ijtst.2017.12.001.
- [72] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, “Prediction-based GNSS spoofing attack detection for autonomous vehicles,” presented at the Transportation Research Board 100th Annual Meeting, Transportation Research Board, Washington, DC, USA, 2021.
- [73] D. López and B. Farooq, “A multi-layered blockchain framework for smart mobility data-markets,” *Transportation Research Part C: Emerging Technologies*, vol. 111, pp. 588–615, Feb. 2020, doi: 10.1016/j.trc.2020.01.002.
- [74] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “BlockChain: A Distributed Solution to Automotive Security and Privacy,” *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, Dec. 2017, doi: 10.1109/MCOM.2017.1700879.
- [75] G. Yan, S. Olariu, and M. C. Weigle, “Cross-layer location verification enhancement in vehicular networks,” in *2010 IEEE Intelligent Vehicles Symposium*, Jun. 2010, pp. 95–100. doi: 10.1109/IVS.2010.5548057.
- [76] K. Lin, Y. Li, J. Deng, P. Pace, and G. Fortino, “Clustering-Learning-Based Long-Term Predictive Localization in 5G-Envisioned Internet of Connected Vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2020, doi: 10.1109/TITS.2020.2997472.
- [77] M. Khodaei and P. Papadimitratos, “The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,” *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63–69, Dec. 2015, doi: 10.1109/MVT.2015.2479367.
- [78] N. Hegde and S. S. Manvi, “A novel key management protocol for vehicular cloud security,” *TELKOMNIKA*, vol. 17, no. 2, 2019, doi: 10.12928/TELKOMNIKA.V17i2.9278.
- [79] E. K. Subramanian and L. Tamilselvan, “A focus on future cloud: machine learning-based cloud security,” *SOCAL*, vol. 13, no. 3, pp. 237–249, Sep. 2019, doi: 10.1007/s11761-019-00270-0.
- [80] Z. Chkirbene, A. Erbad, and R. Hamila, “A Combined Decision for Secure Cloud Computing Based on Machine Learning and Past Information,” in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2019, pp. 1–6. doi: 10.1109/WCNC.2019.8885566.
- [81] V. K. M. R. Koduri, S. Nandyala, and M. Manalikandy, “Secure Vehicular Communication Using Blockchain Technology,” SAE International, Warrendale, PA, SAE Technical Paper 2020-01-0722, Apr. 2020. doi: 10.4271/2020-01-0722.
- [82] L. Xie, Y. Ding, H. Yang, and X. Wang, “Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs,” *IEEE Access*, vol. 7, pp. 56656–56666, 2019, doi: 10.1109/ACCESS.2019.2913682.
- [83] R. V. Rao and K. Selvamani, “Data Security Challenges and Its Solutions in Cloud Computing,” *Procedia Computer Science*, vol. 48, pp. 204–209, 2015, doi: 10.1016/j.procs.2015.04.171.
- [84] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, Jan. 2012, doi: 10.1109/MIC.2012.14.
- [85] Y. Su, J. Wang, Y. Wang, and M. Miao, “Efficient Verifiable Multi-Key Searchable Encryption in Cloud Computing,” *IEEE Access*, vol. 7, pp. 141352–141362, 2019, doi: 10.1109/ACCESS.2019.2943971.
- [86] C. Lü, G. Qian, and T. Chen, “A Cloud Computing Security Model Based on Noninterference,” *Wuhan Univ. J. Nat. Sci.*, vol. 24, no. 3, pp. 194–200, Jun. 2019, doi: 10.1007/s11859-019-1385-7.
- [87] H. Ma, G.-H. Tian, and L.-C. Zhang, “Anti-Leakage Client-Side Deduplication with Ownership Management in Fog Computing,” *International Journal of Network Security*, p. 12, 2019, doi: 10.6633/IJNS.880.
- [88] A. Li, S. Tan, and Y. Jia, “A method for achieving provable data integrity in cloud computing,” *J Supercomput*, vol. 75, no. 1, pp. 92–108, Jan. 2019, doi: 10.1007/s11227-015-1598-2.
- [89] N. Garg, S. Bawa, and N. Kumar, “An efficient data integrity auditing protocol for cloud computing,” *Future Generation Computer Systems*, vol. 109, pp. 306–316, Aug. 2020, doi: 10.1016/j.future.2020.03.032.
- [90] X. Zhang, H. Wang, and C. Xu, “Identity-based key-exposure resilient cloud storage public auditing scheme from lattices,” *Information Sciences*, vol. 472, pp. 223–234, Jan. 2019, doi: 10.1016/j.ins.2018.09.013.
- [91] X. Zhang, J. Zhao, C. Xu, H. Wang, and Y. Zhang, “DOPIV: Post-quantum Secure Identity-based Data Outsourcing with Public Integrity Verification in Cloud Storage,” *IEEE Transactions on Services Computing*, pp. 1–1, 2019, doi: 10.1109/TSC.2019.2942297.
- [92] E. Hossain *et al.*, “Vehicular telematics over heterogeneous wireless networks: A survey,” *Computer Communications*, vol. 33, no. 7, pp. 775–793, May 2010, doi: 10.1016/j.comcom.2009.12.010.
- [93] A. Mahmood, W. E. Zhang, and Q. Z. Sheng, “Software-Defined Heterogeneous Vehicular Networking: The Architectural Design and Open Challenges,” *Future Internet*, vol. 11, no. 3, Art. no. 3, Mar. 2019, doi: 10.3390/fi11030070.
- [94] S. S. Mudengudi and M. S. Kakkasageri, “Agent Based Trust Establishment between Vehicle in Vehicular Cloud Networks,” *I. J. Computer Network and Information Security*, vol. 7, pp. 29–36, 2019, doi: 10.5815/ijcnis.2019.07.05.
- [95] B. Hurl, R. Cohen, K. Czarniecki, and S. Waslander, “TruPercept: Trust Modelling for Autonomous Vehicle Cooperative Perception from Synthetic Data,” in *2020 IEEE Intelligent Vehicles Symposium (IV)*, Oct. 2020, pp. 341–347. doi: 10.1109/IV47402.2020.9304695.
- [96] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, “Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,” *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017, doi: 10.1109/IIOT.2017.2740569.
- [97] H. Yang, J. Yuan, H. Yao, Q. Yao, A. Yu, and J. Zhang, “Blockchain-Based Hierarchical Trust Networking for JointCloud,” *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1667–1677, Mar. 2020, doi: 10.1109/IIOT.2019.2961187.
- [98] P. Goyal, V. Parmar, and R. Rishi, “Manet: vulnerabilities, challenges, attacks, application,” *IJCEM International Journal of Computational Engineering & Management*, vol. 11, pp. 32–37, 2011.
- [99] S. O. Kuyoro, F. Ibikunle, and O. Awodele, “Cloud Computing Security Issues and Challenges,” *International Journal of Computer Networks (IJCN)*, vol. 3, no. 5, pp. 247–255, 2011.
- [100] M. Aloqaily, B. Kantarci, and H. T. Mouftah, “Vehicular clouds: State of the art, challenges and future directions,” in *2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, Nov. 2015, pp. 1–6. doi: 10.1109/AEECT.2015.7360550.
- [101] H. Noroozi, M. Khodaei, and P. Papadimitratos, “VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,” in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, Stockholm, Sweden, Jun. 2018, pp. 302–304. doi: 10.1145/3212480.3226100.
- [102] K. Lim, W. Liu, X. Wang, and J. Joung, “SSKM: Scalable and Secure Key Management Scheme for Group Signature Based

- Authentication and CRL in VANET,” *Electronics*, vol. 8, no. 11, Art. no. 11, Nov. 2019, doi: 10.3390/electronics8111330.
- [103] A. Mansour, K. M. Malik, A. Alkaff, and H. Kanaan, “ALMS: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–16, 2020, doi: 10.1109/TITS.2020.2975226.
- [104] C. Wang, J. Shen, J.-F. Lai, and J. Liu, “B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs,” *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2020, doi: 10.1109/TETC.2020.2978866.
- [105] H. Li, D. Ma, B. Medjahed, Y. S. Kim, and P. Mitra, “Analyzing and Preventing Data Privacy Leakage in Connected Vehicle Services,” *SAE Int. J. Adv. & Curr. Prac. in Mobility*, vol. 1, no. 3, Art. no. 2019-01-0478, Apr. 2019, doi: 10.4271/2019-01-0478.
- [106] R. N. Fries, M. R. Gahroei, M. Chowdhury, and A. J. Conway, “Meeting privacy challenges while advancing intelligent transportation systems,” *Transportation Research Part C: Emerging Technologies*, vol. 25, pp. 34–45, Dec. 2012, doi: 10.1016/j.trc.2012.04.002.
- [107] S. Cadzow, D. Van Duren, J. Petit, W. Whyte, and R. Rausch, “Connected Vehicle Pilot Deployment Program Phase 2 : Data Privacy Plan – New York City,” FHWA-JPO-17-453, Dec. 2016. [Online]. Available: <https://rosap.nhtl.bts.gov/view/dot/32311>
- [108] A. C. Squicciarini, G. Petraceca, and E. Bertino, “Adaptive data protection in distributed systems,” in *Proceedings of the third ACM conference on Data and application security and privacy*, San Antonio, Texas, USA, Feb. 2013, pp. 365–376. doi: 10.1145/2435349.2435401.
- [109] S. Chen, D. Thilakanathan, D. Xu, S. Nepal, and R. Calvo, “Self Protecting Data Sharing Using Generic Policies,” in *2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, May 2015, pp. 1197–1200. doi: 10.1109/CCGrid.2015.84.
- [110] D. Thilakanathan, S. Chen, S. Nepal, and R. Calvo, “SafeProtect: Controlled Data Sharing With User-Defined Policies in Cloud-Based Collaborative Environment,” *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 2, pp. 301–315, Apr. 2016, doi: 10.1109/TETC.2015.2502429.
- [111] N. Papanikolaou, S. Pearson, M. C. Mont, and R. K. L. Ko, “A toolkit for automating compliance in cloud computing services,” *International Journal of Cloud Computing*, vol. 3, no. 1, pp. 45–68, Jan. 2014, doi: 10.1504/IJCC.2014.058830.
- [112] H. B. Rahmouni, T. Solomonides, M. C. Mont, and S. Shiu, “Ontology-based privacy compliance on European healthgrid domains,” in *HealthGrid*, 2009, pp. 183–189.
- [113] M. Mowbray, S. Pearson, and Y. Shen, “Enhancing privacy in cloud computing via policy-based obfuscation,” *J Supercomput*, vol. 61, no. 2, pp. 267–291, Aug. 2012, doi: 10.1007/s11227-010-0425-z.
- [114] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “SPECS: Secure and privacy enhancing communications schemes for VANETs,” *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, Mar. 2011, doi: 10.1016/j.adhoc.2010.05.005.
- [115] F. Kargl and J. Petit, “Security and privacy in vehicular networks,” in *Vehicular Communications and Networks*, W. Chen, Ed. Woodhead Publishing, 2015, pp. 171–190. doi: 10.1016/B978-1-78242-211-2.00009-X.
- [116] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” in *Advances in Cryptology*, Berlin, Heidelberg, 1985, pp. 47–53. doi: 10.1007/3-540-39568-7_5.
- [117] P. Kamat, A. Baliga, and W. Trappe, “An Identity-based Security Framework for VANETs,” in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, New York, NY, USA, Sep. 2006, pp. 94–95. doi: 10.1145/1161064.1161083.
- [118] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, “A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks,” *IEEE Communications Surveys Tutorials*, vol. 14, no. 2, pp. 380–400, 2012, doi: 10.1109/SURV.2011.020211.00045.
- [119] J. Y. Choi, M. Jakobsson, and S. Wetzel, “Balancing auditability and privacy in vehicular networks,” in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, New York, NY, USA, Oct. 2005, pp. 79–87. doi: 10.1145/1089761.1089775.
- [120] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, “Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks,” in *Eighth International Symposium on Autonomous Decentralized Systems (ISADS’07)*, Mar. 2007, pp. 344–351. doi: 10.1109/ISADS.2007.37.
- [121] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, New York, NY, USA, Sep. 2007, pp. 19–28. doi: 10.1145/1287748.1287752.
- [122] J. Serna, J. Luna, and M. Medina, “Geolocation-Based Trust for Vanet’s Privacy,” in *2008 The Fourth International Conference on Information Assurance and Security*, Sep. 2008, pp. 287–290. doi: 10.1109/IAS.2008.21.
- [123] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong, and N. Yu, “Fog-Aided Verifiable Privacy Preserving Access Control for Latency-Sensitive Data Sharing in Vehicular Cloud Computing,” *IEEE Network*, vol. 32, no. 3, pp. 7–13, May 2018, doi: 10.1109/MNET.2018.1700341.
- [124] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, “Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1654–1667, 2020, doi: 10.1109/TIFS.2019.2946933.
- [125] C. Miao *et al.*, “Cloud-Enabled Privacy-Preserving Truth Discovery in Crowd Sensing Systems,” in *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, New York, NY, USA, Nov. 2015, pp. 183–196. doi: 10.1145/2809695.2809719.
- [126] S. S. Yau and H. G. An, “Protection of users’ data confidentiality in cloud computing,” in *Proceedings of the Second Asia-Pacific Symposium on Internetware - Internetware ’10*, Suzhou, China, 2010, pp. 1–6. doi: 10.1145/2020723.2020734.
- [127] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, “Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds,” in *2010 IEEE 3rd International Conference on Cloud Computing*, Jul. 2010, pp. 244–251. doi: 10.1109/CLOUD.2010.42.
- [128] T. Wüchner and A. Pretschner, “Data Loss Prevention Based on Data-Driven Usage Control,” in *2012 IEEE 23rd International Symposium on Software Reliability Engineering*, Nov. 2012, pp. 151–160. doi: 10.1109/ISSRE.2012.10.
- [129] F. Kelbert and A. Pretschner, “Data usage control enforcement in distributed systems,” in *Proceedings of the third ACM conference on Data and application security and privacy*, San Antonio, Texas, USA, Feb. 2013, pp. 71–82. doi: 10.1145/2435349.2435358.
- [130] F. Kelbert and A. Pretschner, “A Fully Decentralized Data Usage Control Enforcement Infrastructure,” in *Applied Cryptography and Network Security*, Cham, 2015, pp. 409–430. doi: 10.1007/978-3-319-28166-7_20.
- [131] Y.-Y. Chen, P. A. Jamkhedkar, and R. B. Lee, “A software-hardware architecture for self-protecting data,” in *Proceedings of the 2012 ACM conference on Computer and communications security*, Raleigh, North Carolina, USA, Oct. 2012, pp. 14–27. doi: 10.1145/2382196.2382201.
- [132] S. Trabelsi and J. Sendor, “Sticky policies for data control in the cloud,” in *2012 Tenth Annual International Conference on Privacy, Security and Trust*, Jul. 2012, pp. 75–80. doi: 10.1109/PST.2012.6297922.
- [133] J. Brown and D. M. Blough, “Distributed Enforcement of Sticky Policies with Flexible Trust,” in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, Aug. 2015, pp. 1202–1209. doi: 10.1109/HPCC-CSS-ICESS.2015.235.
- [134] S. De Capitani di Vimercati, R. F. Erbacher, S. Foresti, S. Jajodia, G. Livraga, and P. Samarati, “Encryption and Fragmentation for Data Confidentiality in the Cloud,” in *Foundations of Security Analysis and Design VII: FOSAD 2012/2013 Tutorial Lectures*, A. Aldini, J. Lopez, and F. Martinelli, Eds. Cham: Springer International Publishing, 2014, pp. 212–243. doi: 10.1007/978-3-319-10082-1_8.
- [135] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, “Intelligent cryptography approach for secure distributed big data storage in

- cloud computing,” *Information Sciences*, vol. 387, pp. 103–115, May 2017, doi: 10.1016/j.ins.2016.09.005.
- [136] M. Bahrami and M. Singhal, “CloudPDB: A light-weight data privacy schema for cloud-based databases,” in *2016 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2016, pp. 1–5. doi: 10.1109/ICCNC.2016.7440634.
- [137] P. Mell, J. Shook, and R. Harang, “Measuring and improving the effectiveness of defense-in-depth postures,” in *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, 2016, pp. 15–22.
- [138] P. Sandner, J. Gross, and R. Richter, “Convergence of Blockchain, IoT, and AI,” *Frontiers in Blockchain*, vol. 3, p. 42, 2020, doi: 10.3389/fbloc.2020.522600.
- [139] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, “A Review of Blockchain in Internet of Things and AI,” *Big Data and Cognitive Computing*, vol. 4, no. 4, Art. no. 4, Dec. 2020, doi: 10.3390/bdcc4040028.
- [140] A. Hammoud, H. Sami, A. Mourad, H. Otrouk, R. Mizouni, and J. Bentahar, “AI, Blockchain, and Vehicular Edge Computing for Smart and Secure IoV: Challenges and Directions,” *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 68–73, Jun. 2020, doi: 10.1109/IOTM.0001.1900109.
- [141] M. Islam, M. Chowdhury, Z. Khan, and S. M. Khan, “Hybrid Quantum-Classical Neural Network for Cloud-supported In-Vehicle Cyberattack Detection,” *arXiv:2110.07467 [cs]*, Oct. 2021, Accessed: Oct. 17, 2021. [Online]. Available: <http://arxiv.org/abs/2110.07467>
- [142] J. Taiber, “Unsettled Topics Concerning the Impact of Quantum Technologies on Automotive Cybersecurity,” SAE International, Warrendale, PA, SAE Technical Paper EPR2020026, Dec. 2020. doi: 10.4271/EPR2020026.
- [143] L. Chen *et al.*, “Report on Post-Quantum Cryptography,” National Institute of Standards and Technology, NIST IR 8105, Apr. 2016. doi: 10.6028/NIST.IR.8105.
- [144] M. Chowdhury, M. Islam, and Z. Khan, “Security of Connected and Automated Vehicles,” *The Bridge on Cybersecurity*, vol. 49, no. 3, Sep. 2019, Accessed: Mar. 28, 2021. [Online]. Available: <https://nae.edu/216540/Security-of-Connected-and-Automated-Vehicles>

M Sabbir Salek is a Ph.D. student at Clemson University. His Ph.D. thesis is focused on Connected and Automated Vehicular Technology. He received his B.S. in Mechanical Engineering in 2016 from Bangladesh University of Engineering & Technology (BUET), Dhaka, Bangladesh, and M.S. in Civil Engineering in 2021 from Clemson University. His research interest includes cloud computing, connected and automated vehicles, transportation cyber-physical systems (TCPS), and machine learning.

Sakib Mahmud Khan is the assistant director of the Center for Connected Multimodal Mobility (C²M²). Before joining the center, he was a post-doctoral research scholar working at California Partners for Advanced Transportation Technology (PATH), University of

California Berkeley. He received his Ph.D. and M.Sc. in Civil Engineering from Clemson University in 2019 and 2015, respectively.

Hsien-wen Deng is a master student at Clemson University. He received his B.S. degree in Computer Science and Information Engineering in 2017 from National Central University (NCU), Chung-li, Taiwan (R.O.C). His research interests include cloud computing, transportation cyber-physical systems (TCPS), and internet of things (IoT).

Mizanur Rahman is an assistant professor in the Department of Civil, Construction and Environmental Engineering at the University of Alabama, Tuscaloosa, Alabama. He received his M.Sc. and Ph.D. degrees in Civil Engineering (Transportation systems), from Clemson University, in 2013 and 2018, respectively. After his graduation in August 2018, he joined as a postdoctoral research fellow for the Center for Connected Multimodal Mobility (C²M²), a U.S. Department of Transportation Tier 1 University Transportation Center (cecas.clemson.edu/c2m2). After that, he has also served as an Assistant Director of C²M². He was closely involved in the development of South Carolina Connected Vehicle Testbed (SC-CVT). His research focuses on traffic flow theory, and transportation cyber-physical systems for connected and automated vehicles and smart cities.

Mhafuzul Islam received the BS degree in Computer Science and Engineering from the Bangladesh University of Engineering and Technology (BUET) in 2014 and MS degree in Civil Engineering from Clemson University at 2018. He is currently a Ph.D. student in the Glenn Department of Civil Engineering at Clemson University. His research interests include Transportation Cyber-Physical Systems with an emphasis on Data-driven Connected Autonomous Vehicle. He is a student member of IEEE.

Zadid Khan received the BS degree in Electrical and Electronic Engineering from the Bangladesh University of Engineering and Technology (BUET) in 2015 and MS degree in Civil Engineering from Clemson University at 2018. He is currently a Ph.D. student in the Glenn Department of Civil Engineering at Clemson University. His research interests include Machine/Deep Learning, Data Science, Cybersecurity and Software Defined Networking.

Mashrur "Ronnie" Chowdhury is the Eugene Douglas Mays Professor of Transportation at Clemson University. He is the director of the USDOT Center for Connected Multimodal Mobility (C²M²) (<http://cecas.clemson.edu/c2m2>). He is the co-director of the Complex Systems, Analytics and Visualization Institute (CSAVI) (<http://clemson-csavi.org>) at Clemson University. He previously served as an elected member of the IEEE ITS Society Board of Governors and is currently a senior member of the IEEE. He is a Fellow of the American Society of Civil Engineers (ASCE) and an alumnus of the National Academy of Engineering (NAE) Frontiers of Engineering program. Dr. Chowdhury is a member of the Transportation Research Board (TRB) Committee on Artificial Intelligence and Advanced Computing Applications, and the TRB Committee on Intelligent Transportation Systems. He is the founding advisor of the "IEEE Intelligent Transportation Systems Society (ITSS) Student Chapter" at Clemson University. He is a registered professional engineer in Ohio.

Mitch Shue is a professor of practice in the School of Computing at Clemson University, and the executive director of Clemson's AI Research Institute for Science and Engineering (AIRISE), leaving a long career in industry to join the faculty in 2019. Prior to Clemson, Professor Shue served as chief technology officer for Morningstar (Nasdaq: MORN), a leading global provider of independent investment research and data. He previously held leadership roles with several companies and has helped grow three startups into publicly traded companies, and two others into successful acquisitions. Professor Shue holds a bachelor's degree in computer science from Trinity University in Texas and a master's degree in conflict analysis and resolution from George Mason University in Virginia.