Privacy for 5G-Supported Vehicular Networks

Li, Meng; Zhu, Liehuang ; Zhang, Zijian; Lal, Chhagan; Conti, Mauro; Martinelli, Fabio

DOI
10.1109/OJCOMS.2021.3103445

Publication date
2021

Document Version
Final published version

Published in
IEEE Open Journal of the Communications Society

Received 29 June 2021; revised 16 July 2021; accepted 5 August 2021. Date of publication 11 August 2021; date of current version 27 August 2021.

Digital Object Identifier 10.1109/OJCOMS.2021.3103445

Privacy for 5G-Supported Vehicular Networks

MENG LI [1] (Member, IEEE), LIEHUANG ZHU [2] (Member, IEEE), ZIJIAN ZHANG [2] (Member, IEEE), CHHAGAN LAL [3] (Member, IEEE), MAURO CONTI [4] (Senior Member, IEEE), AND FABIO MARTINELLI [5]

[1]School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230601, China

[2]School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100811, China

[3]Department of Intelligent Systems, CyberSecurity Group, Delft University of Technology, 2628 CD Delft, The Netherlands

[4]Department of Mathematics, University of Padua, 35122 Padua, Italy

[5]Institute for Informatics and Telematics, National Research Council of Italy, 56127 Pisa, Italy

CORRESPONDING AUTHOR: L. ZHU (e-mail: liehuangz@bit.edu.cn)

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 62002094; in part by the Anhui Provincial Natural Science Foundation under Grant 2008085MF196; in part by the EU LOCARD Project under Grant H2020-SU-SEC-2018-832735; and in part by the EU Project E-CORRIDOR.

ABSTRACT Vehicular networks allow billions of vehicular users to be connected to report and exchange real-time data for offering various services, such as navigation, ride-hailing, smart parking, traffic monitoring, and vehicular digital forensics. Fifth generation (5G) is a new radio access technology with greater coverage, accessibility, and higher network density. 5G-supported Vehicular Networks (5GVNs) have attracted plenty of attention from both academia and industry. Geared with new features, they are expected to revolutionize the mobility ecosystem to empower a portfolio of new services. Meanwhile, the development of such communication capabilities, along with the development of sensory devices and the enhancement of local computing powers, have lead to an inevitable reality of massive data (e.g., identity, location, and trajectory) collection from vehicular users. Unfortunately, 5GVN are still confronted with a variety of privacy threats. Such threats are targeted at users' data, identity, location, and trajectory. If not properly handled, such threats will cause unimaginable consequences to users. In this survey, we first review the state-of-the-art of survey papers. Next, we introduce the architecture, features, and services of 5GVN, followed by the privacy objectives of 5GVN and privacy threats to 5GVN. Further, we present existing privacy-preserving solutions and analyze them in-depth. Finally, we define some future research directions to draw more attention and down-to-earth efforts into this new architecture and its privacy issues.

INDEX TERMS Vehicular networks, 5G, privacy, privacy-preserving solutions.

I. INTRODUCTION

VEHICULAR Network (VN) consists of a group of vehicular users sharing real-time on-road data by communicating with each other directly or to a Service Provider (SP) via Road-Side Units (RSUs). The vehicular user usually refers to a vehicle equipped with a wireless-enabled On-Board Unit (OBU) and Electronic Controlled Units (ECU), and a pedestrian holding a mobile device. Such user-side equipment is manufactured with computation powers and communication capabilities. After registering to a Trusted Third Party (TTP) to obtain credentials and keys, users can participate in the activities of VNs. Communication in VN includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) communications [1]. There are two categories of communication technology: Dedicated Short-Range Communications (DSRC) and Long Term Evolution (LTE)-based Vehicle-to-Everything (V2X) technology (i.e., LTE-based V2X or LTE-V) [2], [3]. Following a specific communication protocol, a vehicular user can submit a report to the SP as a contributing worker and submit a request as a querier.

Providing many benefits to users, VN has transformed traditional and isolated transportation into a modern and connected one in the new era of communications by linking the physical vehicular world to the digital world. It has revolutionized how modern vehicles are manufactured, purchased, and operated. Typical vehicular services are navigation [4], [5], [6], ride-hailing [7], [8], [9], smart parking [10], [11], [12], road monitoring [13], [14], [15], and Vehicular Digital Forensics (VDF) [16], [17], [18]. Navigation enables a requesting user to obtain an optimal route(s) from a pick-up location to a destination. Two popular navigation services are Google Maps [19] and Waze [20]. Ride-hailing allows a rider to find an available independent driver of ride services nearby and take her/him to a destination. Among the multiple Ride-Hailing Services (RHSs), Uber and DiDi are the most favored ones in United States [21] and China [22], respectively. Smart parking updates the occupation conditions of parking lots and distributes the parking lots to cruising drivers who are requesting to park. We are also witnessing the emergence of smart parking practices [23], [24], [25]. Traffic monitoring assists the local transportation department to timely acquire the conditions of road information (road traffic and road surface). It shares real-time road information with vehicular users through a public platform. The market of in-vehicle services is estimated to be worth 60 million by 2023 and covering numerous domains such as health, road safety, security, fuel economy, and insurance liability [26]. VDF collects transmitted messages in VNs in a cloud-based storage or in a blockchain [27], [28], [29], guaranteeing that the vehicular data are verifiable and users' actions are accountable. We can consider VDF as a useful mechanism of keeping track of the data in the above-mentioned four services and further securing the underlying motivations.

Reports say that there will be more than two billion vehicles on roadways worldwide by 2050 [30] and the global in-vehicle infotainment market will reach USD 54.8 billion by 2027 [31]. Moreover, the overwhelming rise of electric vehicles, such as Tesla [32] and Nio [33], has boosted the vehicle industry once again. Therefore, it is widely acknowledged that VNs with ubiquitous connectivity, ultra-reliable and low-latency transmissions [34] have profoundly impacted our daily lives.

The fifth generation communication [35] is a new access technology and a user-centric concept that addresses the application requirements of all the players in the digital world [34]. It does not change the existing communications architecture but offers a unifying platform that leverages existing techniques to provide multiple services to the users with different application requirements. 5G utilizes the newly assigned spectrum to support new air interfaces and access techniques. The basic building blocks of 5G include the technology to discover and provide services using proximity information, software defined networks, network slicing, millimeter-wave communications, and mobile edge computing (MEC) [34].

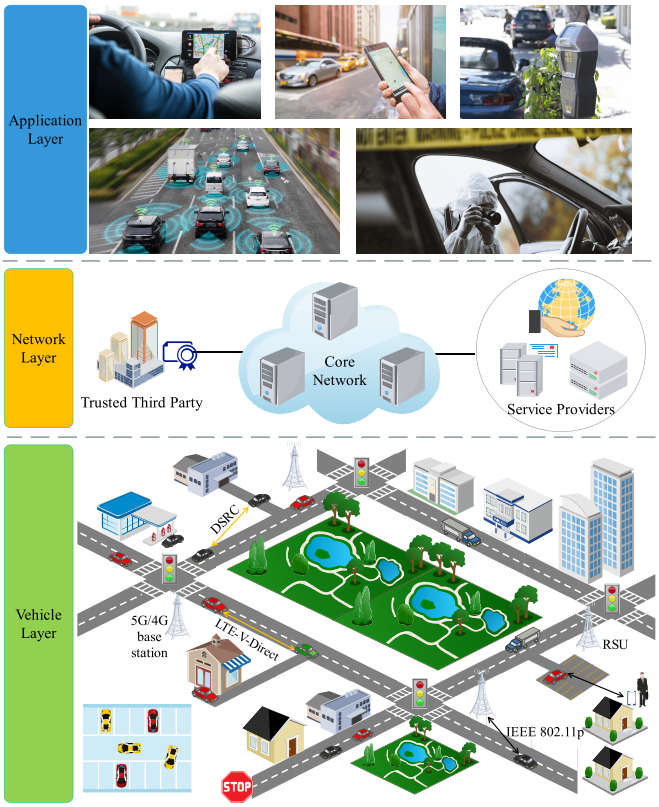


FIGURE 1. The Architecture of 5G-Supported Vehicular Networks.

The existing communication technologies such as LTE and LTE-advanced have already paved the way for the adoption of V2X communications to 5G [36] by providing flexible and cost-effective solutions [37]. 5G features extremely high bandwidth, ultra low latency, and high density connections [2], which can support promising vehicular services. In 5GVN as depicted in Fig. 1, which is transforming the current transportation into intelligent transportation systems (ITS) [38], [39], [40], [41], [42], vehicular users will enjoy diverse, low-latency, highly reliable services due to the advanced hardware, enhanced computation powers, and improved communication capabilities.

A large-scale analysis of vehicular data can lead to valuable insights that address public transportation challenges and come across new scientific discoveries [43]. However, as a nontrivial combination and extension built upon existing infrastructures and technologies, it is inevitable that some issues remain in 5GVNs, especially privacy issues [44], [45], [46], [47], [48], [49], [50], [51]. SPs may have malicious or mischievous employees who steal users' data and sell them to the black market. Edge nodes are deployed by SPs, which makes them not trustworthy, and they are also exposed in the field, being vulnerable to be compromised. New sensors and interfaces on vehicles expand the attack surfaces for adversaries to remotely monitor transmitted messages and even access vehicles [37]. Consequently, new privacy challenges arise and they should be further investigated in 5GVNs. Although user-side devices have been upgraded

to a high level, they still have some vulnerabilities to be exploited [52], [53], [54], [55], [56].

For example, Tesla's in-car cameras are used to alert drivers when the drivers are not focusing on the road. However, some Tesla cars transmit video footage of in-car people from in-car cameras [57]. A forensic engineer helped a technology columnist access the contents of his Chevrolet's infotainment computer. They found that the data in the Infotainment system contain precise locations, phone call record, and contact list. To make things worse, the system reports data to General Motors over an always-on Internet connection [58]. Another example is that we always carry a smartphone anywhere we go nowadays including when we are driving, but it is possible to detect whether a driver is drunk driving by monitoring the driver's behaviors via smartphones [59]. Furthermore, it is also practical to infer a user's location just by reading the smart phone's aggregate power consumption [55].

Existing privacy-preserving mechanism in cloud computing can be leveraged to address some of the privacy issues, yet 5GVN has its own privacy challenges due to its distinctive features, such as diverse data sources, large data volume, high transmission speed. 5GVN collects data from more vehicles and handhold devices which surely lead to all kinds of data sources and a great amount of data. Along with the high-speed transmission afforded by 5G, 5GVN will certainly pose more requirements on processing efficiency. The advent of new architectures, techniques, and services in 5GVN will generate higher privacy risks for users. Moreover, the integration of technologies with 5GVNs will expose the networks to more privacy challenges [36]. Unfortunately, the privacy issues in 5GVN have not been systematically identified and the privacy solutions used in previous generations will not suffice for 5G [36]. Therefore, studying privacy objectives of 5GVN and privacy threats to 5GVN ate quite important prior to the design and implementation of 5GVN services.

This survey first anatomizes the 5GVN architecture and its features, services, privacy objectives and threats, and state-of-the-art solutions. Next, we give a brief introduction of 5G technology, followed by the architecture and features of 5GVN. We introduce some popular and distinctive services of 5GVN, including navigation, ride-hailing, smart parking, road monitoring, and vehicular digital forensics. We also discuss the privacy objectives, including data privacy, identity privacy, location privacy, and trajectory privacy. Then, we discuss the privacy threats to 5GVN, including eavesdropping, man-in-the-middle, tampering, forgery, spam, impersonation, sybil, jamming, collusion, and inference attack. We review some popular and well-acknowledged privacy-preserving techniques and show how they achieve the privacy objectives. We also give our insights on their highlights and disadvantages. Finally, we present open research directions.

The remainder of the survey is organized as follows. In Section II, we discuss the difference between this survey and the existing ones. We review the architecture, features, and services of 5GVN in Section III. We discuss privacy objectives and privacy threats in Section IV and Section V, respectively. We introduce privacy-preserving solutions for 5GVNs in Section VI. We discuss future research directions in Section VII and conclude our survey in Section VIII.

II. RELATED WORKS

In this section, we review some state-of-the-art articles. They are focused on discussing security and privacy issues in vehicular ad hoc network, fog computing, vehicular crowdsensing, 5G, 5G V2X, 5G-enabled vehicular networks, vehicular cloud computing, and V2X.

Qu *et al.* [45] provided background of Vehicular Ad Hoc Network (VANET) including requirements of security and privacy, challenges, types of adversaries. Specifically, they stated that authentication in a mobile environment of high mobility vehicles poses a privacy risk to users because the network will know the locations of a specific user at a specific time. Then, they classified and discussed advantages and disadvantages of three commonly used anonymous authentication methods. Next, they discussed the tradeoff between security and privacy.

Ni *et al.* [46] reviewed the model and features of Fog Computing (FC) and discussed its utility in services such as real-time services, transient storage, data dissemination and decentralized computation. They classify fog-based Internet-of-Things (IoT) services based on fog nodes. They also discuss security and privacy threats to IoT services and demonstrate requirements on security and privacy in FC. Finally, they show technical challenges to secure FC and revisit existing solutions.

Ni *et al.* [47] introduced the architecture of fog-based vehicular crowdsensing and some applications, including parking navigation, road monitoring, and traffic collision reconstruction. Then, they discussed the security assurance, privacy preservation, and incentive fairness in fog-based vehicular crowdsensing as well as present some existing solutions to address these issues. Next, they give some possible future research directions to call for more attention.

Ahmad *et al.* [36] studied the state of the art of security in 5G networks. They first looked into security threats and solutions for the previous network generations. They presented security threats in 5G network and introduced existing solutions and some research directions. They also provide a brief description of post-5G cellular technologies and corresponding security vulnerabilities, i.e., security in communication networks beyond 5G (XG).

Lu *et al.* [48] also provided some background information of VANETs and some security services. Specifically, they concentrated on reviewing anonymous authentication schemes and discussed some location privacy-preserving protection mechanisms of achieving preserving vehicles' privacy and service quality simultaneously. Next, they comprehensively analyzed different trust management models in VANETs. Finally, they presented the latest simulation platforms.

Lu *et al.* [37] reviewed the architecture of 5G V2X and some use cases of 5G V2X including cooperative awareness, cooperative sensing, cooperative maneuvering. They discussed some trust, security, and privacy issues in 5G V2X as well as the potential attacks. Then, they analyzed the state-of-the-art solutions and expounded how to achieve trust, security, and privacy in each solution. Finally, they show some research directions and expect more attention on 5G V2X services.

Lai *et al.* [2] introduced the infrastructure of 5G-enabled vehicular networks. They showed the critical security and privacy aspects of V2X in LTE. Specifically, they chose 5G-enabled autonomous platoon as a use case and discussed its security and privacy issues. They presented some alternative solutions, including group setup, key management, and message authentication. They also described the security and privacy issues in 5G-enabled vehicular networks.

Masood *et al.* [49] gave a state-of- the-art review of Vehicular Cloud Computing (VCC) including its architecture, features, and services. They presented the attacker model in VCC and discussed the security and privacy issues in VCC in a layered approach: physical resource layer, V2X network layer, and vehicular cloud layer, and a complete system level. Then, they provided corresponding attacks and countermeasures. Next, they pointed out challenges and research directions.

Ghosal and Conti [1] presented a comprehensive overview of solutions in V2X, focusing on its the security issues. They introduced main features of V2X and standardization techniques. They explored security requirements and challenges of V2X. Further, they classified and discussed existing security solutions. Finally, they gave possible and promising research directions of V2X especially related to security.

In contrast to the these surveys, we present a comprehensive analysis on privacy requirements and challenges in 5GVN, including (1) architecture and features of 5GVN, (2) typical services of 5GVN, (3) privacy requirements and challenges of 5GVN, and their existing solutions; (4) insights on the privacy issues that the state-of-the-art solutions cannot tackle due to 5G's features; (5) future research directions of privacy preservation in 5GVN, including user-defined privacy, privacy computing, zero trust, and standardization.

TABLE 1. Acronym and definition.

Acronym	Definition
5G, VN	Fifth generation, vehicular network
5GVN	5G-supported vehicular network
ECU	Electronic controlled units
RSU, OBU	Road-side unit, on-board unit
SP, TTP	Service provider, trusted third party
V2V, V2I	Vehicle-to-vehicle, vehicle-to-infrastructure
V2P, V2X	Vehicle-to-pedestrian, vehicle-to-everything
DSRC	Dedicated short-range communications
LTE	Long term evolution
VDF, RHS	Vehicular digital forensics, ride-hailing service
MEC	Mobile edge computing
5GVN	5G-supported vehicular networks
ITS	Intelligent transportation system
VANET	Vehicular Ad Hoc Network
IoT, FC	Internet-of-Things, fog computing
XG	Communication networks beyond 5G
VCC	Vehicular cloud computing
QoS	Quality of service
NGMN	Next generation mobile network
D2D, mmWave	Device-to-device, millimeter-wave
DDoS	Distributed Denial-of-Service
PSI	Private set intersection
AC	Anonymous credential
AVP	Automated valet parking
PSI	Private set intersection
PC	Privacy computing
FL	Federated learning
SMC	Secure multiparty computation
TEE	Trusted execution environment
ZT	Zero Trust

III. OVERVIEW OF 5G-ENABLED VEHICULAR NETWORKS

In this section, we first provide building blocks of 5G, then we present the architecture of 5GVN as well as its key features. Specifically, we introduce five typical vehicular services, namely navigation, ride-hailing, smart parking, road monitoring, and VDF. We further discuss their new function requirements and privacy under 5GVN.

A. 5G

The proliferation of digital infotainment services and smart devices (e.g., smartphones, laptops) has intensified the crowd demand for high-rate services [60]. 5G is a new access technology and a user-centric concept that addresses the application requirements of all the "digital" users' requirements [34]. It is also a collective and enormous effort to specify, standardize, design, manufacture, and deploy the next cellular network generation [61]. However, as extremely transformative as it seems, it does not change the existing communications architecture but leverages existing techniques on a unifying platform. 5G is not a simple improvement over its predecessors but a significative leap forward regarding data rates, latency, and network reliability [62]. It is envisioned to support the inundation of data traffic with lessened energy consumption and advanced Quality of Service (QoS) [60].

New mobile generations are allocated new frequency bands and wider spectral bandwidth per frequency channel (1G/30 KHz, 2G/200 kHz, 3G/5 MHz, and 4G/20 MHz) [63]. 5G, the next telecommunication standard based on 4G, aims for a higher capacity. While 4G was designed to offer mobile broadband communications, 5G strives for becoming a key asset in the introduction of the digital technologies [61]. The building blocks of 5G include the technology to offer services using proximity information, software defined networks, network slicing, millimeter-wave communications, and mobile edge computing [34]. It has some requirements defined by the Next Generation Mobile Network (NGMN), such as improved coverage, data rates of 10s of Mb/s for 10s of thousands of users, and significantly reduced latency, etc. [63]. In other words, 5G can meet diversified service requirements, including logically independent network slicing, radio access networks reconstruction, core network architecture simplification, and automatic network service implementation [64].

5G is also expected to stimulate the evolution, especially in-depth digitalization, of multiple societal and economic fields [61] such as entertainment [65], energy [66], healthcare [67], Industry 4.0 [68], [69], [70], and automotive [71]. As a result, a wide range of advanced and novel use cases and business models will emerge with 5G innovation. Not only will 5G creates many opportunities for these fields, but it poses new privacy challenges toward business models, technologies, and privacy. Meanwhile, the 5G development will drive the academic community to put efforts into estimate future demands and pinpoint potential problems. It will prompt the industry community to develop and implement more systems and platforms in 5GVN.

B. ARCHITECTURE

5GVN architecture can be split into three layers: vehicle layer at the bottom (layer I), network layer in the middle (layer II), and application layer at the top (layer III), as depicted in Fig. 1. The three layers are displayed in the order of service cycle. Vehicular users communicate from layer I through layer II to interact with services in layer III.

In the vehicle layer, vehicles collect real-time on-road information such location, speed, fuel temperature, road surface condition, and road traffic. The collection is enabled by using automobile sensors including GPS, vehicle speed sensor, fuel temperature sensor, and monitor [72]. These sensors are the main data source in 5GVN, yet there are some complementary sources such as in-vehicle smartphones equipped with rich sensors, roadside sensors, and pedestrians carrying a smartphone. To achieve communications between different entities, many communication technologies are adopted. Vehicles communicate with each other via Device-to-Device (D2D) millimeter-wave (mmWave), DSRC, and LTE-V-Direct.

Vehicles can access the core network in the network layer through intermediaries, i.e., RSUs or 5G/4G base stations. The network layer contains all players of the 5G core network, namely, TTP, SPs, and cloud. The TTP is responsible for managing identities, keys, and certificates of vehicular users for a variety of services. The SPs provide to users various services from a global perspective which can be extracted and put in the application layers. We will introduce them in Section III-D. The cloud has strong computing capabilities and abundant storage space. It can be accessed by users any time any where. The cloud receives data from intermediaries and conduct request/response matching and analysis on the data to return results to corresponding users.

Each of the three layers is scalable, meaning that it is expandable to adjust to new vehicular demands. For example, in the vehicle layer, a new user can register to the TTP and then participate in some vehicular activities. In the network layer, it is possible to upgrade an existing RSU and deploy new base stations. In the application layer, if a new service is developed, it can be made accessible to users through the cloud. The three layers constitute a dynamic 5GVN which has several distinctive features.

C. FEATURES

A problem in the current vehicular communication standards (i.e., IEEE 802.11p) [73] is the absence of spectrum, low latency, and ultra reliable transmission of periodic communications [34]. 5G sheds light on new possibilities of communication and is integrating with many services. It also facilitates further research on all aspects of 5GVN, including infrastructure, efficiency, security, and privacy. 5GVN is a new framework that delivers vehicular services with improved QoS. The main feature of 5GVN is to process vehicular data for users by leveraging fog computing [46], [74], [75] and cloud computing to provide benefits in data collection, computation, and communication. 5GVN has eight prominent features, as shown in Fig. 2. There are many features of 5GVN. In this work, we only list the main features that are related to services and privacy.

1) *Diverse Data Sources:* The development of 5G enables various devices to use multiple radio access technologies [76], [77] to communication in 5GVN. The technology refinement and cost reduction of modern industry have further promoted the ubiquity of smart devices among vehicular user. For example, many smartphones support 5G lately, e.g., Xiaomi [78] and iPhone [79]. Inevitably, 5GVN will embrace devices manufactured with varying configurations.
2) *Huge User Number:* The ubiquity of smart devices and the need for real-time services will promote user participation in 5GVN. As China Telecom reported, its 5G user numbers were 10.73 million by the end of February, 2020 [80]. Meanwhile, electric vehicles reduce oil use by more than 1 million barrels a day in U.S. by 2035 [81] which will incentivise procurement. Business Insider Intelligence predicted that connected vehicle shipments will amount to 77 million by 2025 [82].
3) *Large Data Volume:* Along with the source diversity and user increment, 5GVN confronts an astonishing large volume of data. According to China Telecom, it has data usage growing 16.8% and average revenue per user up 6.5 percent compared with pre-migration levels [80]. StreetLight process billions of location records in North America every month to illuminate traffic patterns to acquire how vehicular users move on roads [83].
4) *Ultra Reliable Transmission:* 5GVN is more reliable than 4G-supported VN. There is a requirement of extremely reliable communications in 5G, i.e., 10^{-7} packet loss probability and reliability of 99.999% [84]. To enhance the reliability of V2X communication, it is recommended to utilize slicing [85], [86], [87] and mobile edge computing [88], [89], [90]. The ultra reliability of 5GVN will support high precision services, e.g., autonomous vehicular communications.
5) *High Transmission Speed:* 5G is significantly faster than 4G. It aims at latency times of a few milliseconds and supports peak data rates of up to 300 Mbps [91].

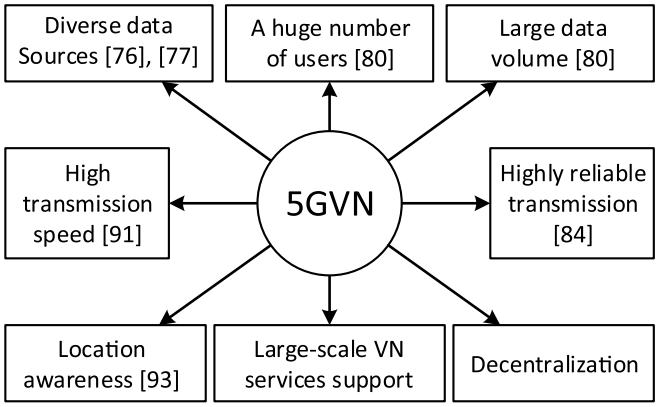


FIGURE 2. Main features of 5GVN.

5GVN will allow vehicular users to enjoy services of high-speed. For example, in-vehicle movie download time will decrease from minutes to seconds. Opensignal data says that 5G download speeds from the three U.S. operators range from 47 Mbps to 58 Mbps [92].

6) *Location Awareness:* The fine-grained location of a user (device) is traceable to support rich services for users. 5G positioning [93] is an integral part of 5G which improves the positioning accuracy down to the centimeter [94]. To achieve the excellent accuracy, 5G utilizes a wide bandwidth for better time resolution, new frequency bands in the mm-wave range and massive MIMO for precise angle measurement [95].
7) *Decentralization:* 5GVN supports a decentralized architecture such that in certain services there are no centralized servers. Vehicular users communicate only to the RSUs or base stations at the network edge, which does not need to report to any cloud servers. These mini-servers at edge self-organize to cooperatively offer real-time services to users.
8) *Large-Scale VN Services Support:* The core function of 5GVN is to support large-scale VN services of high QoS. Besides the fact that traditional VN has already generated numerous services, 5GVN will not only optimize existing services to the next level, but also produce more new services to users. Such services include but not limited to navigation, ride-hailing, smart parking, traffic monitoring, and vehicular digital forensics.

D. SERVICES

Due to rich information exchange among vehicles, pedestrians, infrastructure, and servers, 5GVN significantly improves traffic efficiency and driving safety, and offers infotainment services [37]. Now we introduce five typical services of 5GVN, including navigation, ride-hailing, smart parking, traffic monitoring, and vehicular digital forensics as depicted in Fig. 3. The first four services are common in our daily lives, and they contribute a lot of real-time and sensitive vehicular data to 5GVN. The last service is a service platform that searches targeted information from the four services and feeds modern vehicular investigation [96], [97] with these information.

1) NAVIGATION

As one of the most common services of 5GVN, navigation provides an optimal route to a requesting vehicular user. Such a user first submits a starting location and a destination to a navigation service provider. The provider checks the traffic database and computes an optimal route based on a shortest distance algorithm. Finally, the provider returns the route to the user. Navigation is important to users when they are eager to find a driving route or walking route. A good navigation service will help users bypass congested roads and save traveling time.

2) RIDE-HAILING

In traditional taxi services, riders suffer from deficiency of drivers. Cloud computing and smartphones have alleviated this situation by the shining advent of ride-hailing. Nowadays, ride-hailing is already one of the most popular vehicular services [98]. It helps riders find a ride and save waiting time, facilitates drivers to money by taking ride orders, and assists ride-hailing companies in making profit by charging commission from drivers. The benefits of ride-hailing are obvious. It improves vehicle utility, reduces automobile exhaust, and optimizes traffic efficiency.

3) SMART PARKING

Smart parking is another appealing vehicular service that aims to help cruising drivers quickly find an available parking spot. With the growth of gasoline vehicles and electric vehicles, it is more and more difficult for drivers to park their vehicles, especially when the number of parking lots does not increase proportionately. As an intermediary, a smart parking platform dynamically update the status of each parking lot and respond to drivers' parking requests. Smart parking is categorized into public parking [10], [11] and private parking [12]. The first one only provides parking spots in public regions, such as supermarket and cinema, while the second one utilizes parking spots from private sectors including residence community.

4) ROAD MONITORING

In road monitoring, a road monitoring service provider collects traffic reports from contributing vehicular users to acquire real-time road information, and provides road information to requesting vehicular users. According to the type of road information, road monitoring is classified into road traffic monitoring [13], [15] and road surface monitoring [14]. When compared to navigation, road monitoring can be considered as a building block of navigation, i.e., a service provider invokes road monitoring to acquire necessary information to energize navigation. In addition, road

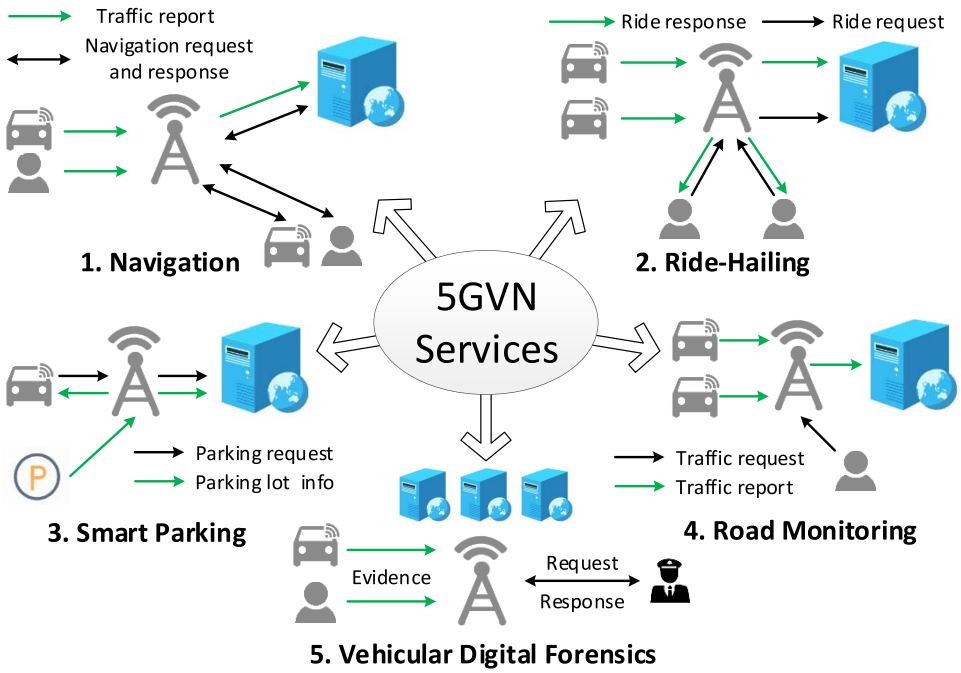


FIGURE 3. Services of 5GVN.

monitoring is valued as a powerful tool for the transportation department and construction department to fuel city planning.

5) VEHICULAR DIGITAL FORENSICS

VDF [99] originates from digital forensics to make user activities accountable in VN. It concerns how data are collected, stored, updated, and accessed. First, data authenticity needs to be guaranteed before data are collected. Afterward, the process of data storage determines whether the data can be retrieved successfully. Next, updating data, e.g., add and delete, should leave a trace or a piece of evidence for future auditing. Further, the policy on who can access which part of a dataset must be developed. Finally, each access must be recorded in a centralized manner [100] or a distributed manner [17], [106]. Specifically, blockchain-based VDF has drawn much attention. Instead of storing forensic data in a cloud, several stakeholders maintain a consortium blockchain [27], [101], [102] to protect the chain-of-custody.

VDF leverages multiple sources, e.g., vehicle speed sensor and brake, to accurately track the data flow corresponding to the initial human behaviors. Such human behaviors are not easy to capture directly, making an automatic and precise examination extremely important when road accidents happen. Therefore, VDF is crucial for liability cognizance and vehicular crime fighting, given that we are now living in a big data era [103], [104], [105], [106], [107] and we are faced with all kinds of true and fake information. Although corresponding techniques of locating authentic data logic are not in their maturity, VDF is destined to gain more attention.

IV. PRIVACY OBJECTIVES OF 5G-SUPPORTED VEHICULAR NETWORKS

Privacy has been given many definitions and standards. In a word, privacy is the things that you want to keep from others. Privacy remains a fundamental issue in any communication systems since the awareness of privacy protection. It resembles the concept of confidentiality in modern cryptography [108] but has its own characters. Privacy is more about analyzing user data while not leaking user's sensitive information to the analyzer or adversary. Protecting privacy is out of the users' perspective and is also not on the stakeholders' to-do list. However, privacy protection increases the acceptance by users and developers [109]. In other words, it is a value-added feature for the stakeholders' services, which will help them to enhance their commercial models for bigger revenues [36].

The 5G appearance will open up new privacy threat to users, and the integration of technologies with 5GVN services will expose users to more privacy challenges. In this section, we examine some main privacy objectives of 5GVN. They are data privacy, identity privacy, location privacy, and trajectory privacy. We note that these privacy objectives have been addressed in current solutions, the successful deployment of 5GVN need to address new privacy challenges.

A. DATA PRIVACY

Data privacy [110], [111], [112] aims to protect user data against passive/eavesdropping adversaries. Intuitively, it is equal to confidentiality and only requires simple asymmetric or symmetric encryption to secure the data. However, we argue that data privacy has more to put on the table. In some

cases, data privacy includes location privacy and trajectory privacy. For better readability, we focus on confidentiality and access control when referring to data privacy in this work.

- *Confidentiality:* Confidentiality is one of the traditional security requirement along with integrity and authentication. It requires that an adversary cannot know the contents of user data, e.g., key, request, and response. This objective is rather straightforward and is achievable by using encryption chosen from a reservoir of cryptographic primitives. Note that we focus on privacy in this work, readers are referred to [36] for more introduction on security.
- *Access Control:* To make confidentiality a little bit complicated, access control realizes a further decryption management on a group of users when they are accessing a dataset. This is raised in VN from the fact that some vehicular users with a set of attributes are only allowed to access certain services or data.

B. IDENTITY PRIVACY

Identity is the key information that is used to recognize a person. It is probably the most sensitive information that a user may want to hide. In VN, identities are used when users are requesting services and are asked to authenticate themselves.

Identity privacy [113], [114], [115] targets to protect users' real identities including name, cellphone number, license plate number, credential, and cryptographic key. In order to prove the participation quality, a user first provides her/his identity to a TTP to receive a token and then uses this token for authentication. There are two aspects of identity privacy: anonymity and unlinkability.

- *Anonymity:* A user's identity should be hidden during vehicular activities from others, including the service provider, RSUs, and other users. It means that a user either does not use her/his identity or proves the identity by using zero-knowledge proofs.
- *Unlinkability:* Unlinkability extends anonymity to the requirement that a user's messages, e.g., requests and responses, are not linkable. To hide an identity once may not be difficult, but to cut off the relation between two messages that includes the same identity is not trivial.

C. LOCATION PRIVACY

Locations are used in a large number of location-based services [116], [117], [118]. Users submit a location to SPs to receive corresponding services, such as location recommendation [119] and friend finding [120]. Generally, users send locations to different SPs without any encryption or sanitation, which leaves a huge loophole. Even if a location can be encrypted and sent via a public channel, the SP will eventually see it after decryption. Location is not identity in the sense that it looks harmless to users regarding character recognition. Unfortunately, a specific location (e.g., home, work, frequent stops) reflects a user's activity. For example, a user suddenly visits a cancer hospital twice a week, indicating that the user has cancer or just sees a patient who has cancer. Since activities are linked to users' privacy, it is safe to say that location is a part of user privacy as well. Sending a sensitive location to an SP without any pre-processing will result in a privacy breach.

Location privacy refers to location indistinguishability [121], [122], [123]. If an adversary cannot tell which location belongs to a target user, we say that location privacy is preserved. This is achieved by adding a random noise to the location, forging dummy locations, leveraging k-anonymity and cloaking, and adopting a widely acknowledged privacy standard differential privacy [124].

D. TRAJECTORY PRIVACY

A trajectory, i.e., a human mobility trace [125], [126], [127], [128], is a series of locations. Users submit a sequence of locations to SPs of a sport app [129] and trajectory collection project [21], [130]. Unlike the independence of a location, a trajectory describes how a user moves with time. This observation reveals more than just the sensitivity of a single location, but a moving pattern of a user. For example, say we have a user who successively visits a park, a restaurant, a cinema, and an apartment building. This location sequence speaks with a high probability for the user's eating preferences and home. To make things worse, it shows a typical pattern of a date that is inferred by the sequence of locations.

Trajectory publication services are classified into publication of one trajectory [131] and publication of a set of trajectories [132]. Therefore, trajectory privacy [133], [134], [135] refers to location indistinguishability and trajectory indistinguishability. Given that locations are correlated [136], it is more difficult to protect trajectory privacy.

E. THE ROAD AHEAD FOR 5GVN PRIVACY

The various privacy requirements apply to many 5GVN applications [2] as they share a similar system model or communication standards. However, when facing a specific application, we should look deep into its functional requirements that may have complicated its privacy requirements. Beside the existing attacks, we will face new privacy threats as well. Therefore, careful considerations are in need.

Since 5G is not merely an enhancive version of 4G, privacy mechanisms should also be re-considered based on the new architecture and service requirements of 5G. Motivated by the vision of secure 5G systems that are outlined by NGMN [137], [138], we give three similar design principles: (1) flexible privacy services, (2) supreme built-in privacy, and (3) privacy automation. The design objective is that 5G services must provide highly guaranteed privacy against various attacks. The privacy mechanisms are flexible for integrating new technologies and using suited privacy-enhancing techniques at different layers or network

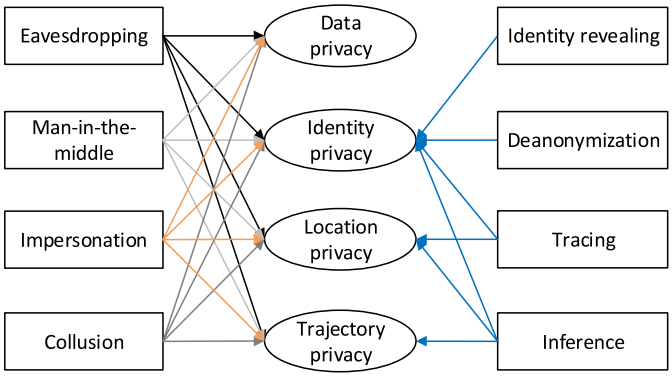


FIGURE 4. Threats in 5GVN.

perimeters. Privacy by design is inevitable because 5G services converge diverse techniques, introducing privacy vulnerabilities in the network. The diversity of services and techniques necessitated the automated privacy to ingeniously adapt and adjust to users and threats [36].

V. PRIVACY THREATS TO 5G-SUPPORTED VEHICULAR NETWORKS

5GVN is faced with cyber attacks [37], [46], [49] due to its open architecture. Since 5GVNs are built upon VNs of the previous communication generations, they still inherit various privacy threats. These threats are raised from both external and internal. We introduce some typical privacy threats in the following subsections: eavesdropping, man-in-the-middle, impersonation, collusion, identity revealing, deanonymization/reidentification, tracing, and inference. We map them to privacy objectives in Fig. 4.

A. EAVESDROPPING

Due to the broadcast and open nature of wireless communication, a malicious adversary eavesdrop on open communication channels to easily capture data packets by installing a receiver by the roadside. The data packets include messages sent among vehicles, pedestrians, and RSUs. Next, the adversary attempts to reveal the underlying contents. This threat is passive but still effective when the data packets are not encrypted. Even though they are encrypted, it is yet to trace the source and the destination of data packets [139].

B. MAN-IN-THE-MIDDLE ATTACK

An adversary is assumed to posit in the middle of two vehicular entities (including vehicular user, RSU, etc.) to relay or falsify the transmitted data between them. Under this attack, the two vehicular entities still assume that they are in direct communication with each other. If such a man-in-the-middle attack is successful and it will continue to acquire data contents and even sensitive information of the two entities.

C. IMPERSONATION

An adversary attempts to impersonate a legal vehicle user to communicate with another legal vehicle user and look for sensitive information. It can also impersonate a legal RSU or SP to receive reports and queries from vehicular users. To successfully initiate this attack, the adversary should be able to steal or forge an authentication credential. The consequences of an impersonation attack are more severe than the above two attacks and the attack opens a possibility for more attacks.

D. COLLUSION

In a collusion attack, two or more malicious entities share information to deceive other legal vehicular entities or gain information of a target vehicular user. For example, a driver colludes with SP to identify an anonymous rider in a RHS. A group of colluding drivers send false traffic reports to an RSU and fake a traffic jam [140].

E. IDENTITY REVEALING

After collecting a vehicular user's data packets, an adversary attempts to reveal the user's identity by analyzing the data packets. In some cases, identity is not involved in the transmitted messages, the adversary can only recover a key or credential of the user. It has to leverage some side information to link the recovered information to the identity.

F. DEANONYMIZATION/REIDENTIFICATION

Besides identity revealing attack, the adversary can only be interested in deanonymize a vehicular user from a pool of collected data packets. It needs to analyze the data packages and find correlations between them.

G. TRACING

By tracing, we mean two types of tracking attacks. The first one is an adversary eavesdropping on communication channels to locate the source the destination of data packets. The second one is an adversary monitoring a specific vehicular user to track her/his future locations. In a tracing attack, the adversary does not have to learn the data contents if tracing is successful.

H. INFERENCE

Holding some background knowledge, an adversary aims to learn various knowledge about a vehicular user by identifying the user's messages from collected messages and acquiring a unique pattern of the user. The target knowledge include location, health condition, diet preference, etc.

VI. PRIVACY-PRESERVING 5G-SUPPORTED VEHICULAR NETWORKS

In Section IV, we have discussed privacy objectives of 5GVN. In this Section, we will follow that classification and introduce privacy-preserving solutions correspondingly. In each subsection, we arrange the order of solutions according to their service types. To favor readability, we list some distinguished privacy-preserving solutions according to their service type in Table 2. We refer the interested reader to the references for more detailed information.

TABLE 2. 5GVN Applications.

Application	Solution
Navigation	VANET-based secure and privacy-preserving navigation (VSPN) [4] VANET and fog-based secure and privacy-preserving navigation (SPNS) [5] Privacy-preserving navigation supporting similar queries (PiSim) [6]
Ride-Hailing	Privacy-preserving computation of meeting points in ridesharing (Priv-2SP-SP) [7] Differentially private scheduling for ridesharing (JDP-Ride) [8] Privacy-preserving and accountable ride-hailing (ORide) [9] Privacy-enhanced ride-hailing (PrivateRide) [109] Efficient and privacy-preserving dynamic spatial query for ride-hailing [143] Privacy-preserving ride-hailing matching with prediction (pRide) [144] Privacy-preserving group ridesharing matching (PGRide) [145] Efficient and privacy-preserving carpooling using fog computing and blockchain (FICA) [146] Privacy-preserving ride matching (pRide) [147] Lightweight and privacy-preserving ride matching (lpRide) [148] Privacy-preserving collaborative-ride hailing (CoRide) [149] Privacy-preserving ride-hailing with verifiable order-linking (OLink) [150] Privacy-preserving ride-hailing without a third trusted server [151]
Smart Parking	VANET-based smart parking (SPARK) [10] Privacy-preserving pay-by-phone parking [11] Anonymous smart-parking and payment (ASAP)[12] Privacy-preserving smart parking navigation (P-SPAN) [152] Secure automated valet parking for for autonomous vehicles [153] Privacy-preserving valet parking for autonomous driving (PrivAV) [154] Privacy-enhanced private parking spot sharing based on blockchain (PEPS)) [155] Distributed mobile system for free parking assignment (DFPS) [156] Privacy-preserving decentralized parking recommendation (PriParkRec) [157]
Road Monitoring	Distributed privacy-preserving traffic monitoring [13] Privacy-preserving vehicular crowdsensing based road surface condition monitoring (CLASC) [14] Privacy-preserving cloud-based road condition monitoring with source authentication [15] Privacy-preserving traffic monitoring with false report filtering (PAM) [141] IoT-enabled smart urban traffic control and management [158] Privacy-preserving compressive sensing for real-time traffic monitoring (PPCS) [159] VANET-based secure and privacy-preserving traffic monitoring [160] Estimation of urban traffic state with probe vehicles [161]
Vehicular Digital Forensics	Forensics model of smart city automated vehicles [16] Integrated lightweight blockchain framework for vehicular forensics (Block4Forensic) [17] Smart vehicle forensics [18] General process for automotive forensics [162] Forensic of a hit and run car accident [163]
Others	Trajectory privacy-preserving framework (TrPF) [164] Privacy-preserving route sharing service via vehicular fog computing [128] Trajectory privacy protection with utility guarantee (QLDS) [165] Real-time privacy-preserving data release over vehicle trajectory (RPTR) [166]

A. DATA PRIVACY

Chim *et al.* [4] utilized proxy re-encryption to allow an RSU to re-encrypt the ciphertext of a vehicle's master key encrypted under the public key of the trusted authority into a new ciphertext of the same master key encrypted under the public key of the vehicle. This enables translation of ciphertexts, i.e., an update of an vehicle's master key via RSUs, while the RSUs do not know the data contents due to the property of proxy re-encryption [166], [167]. The vehicles encrypt their navigation request by using asymmetric encryption. Wang *et al.* [5] first used ElGamal cryptosystem [168] to encrypt a secret key and then encrypted navigation queries with AES encryption and the secret key. The RSU that receives the ciphertext recovered the secret key to decrypt the navigation query.

TRACE [142] protected the sensitive data of RHS provider, i.e., space division, based on a quadtree structure and symmetric encryption. To obtain the density of drivers and rides, the provider had to divide the ride service area into subregions and optimize the space division periodically through analyzing users' locations. The privacy breach of the space division information would disclose business secrets and cause economic costs. The provider encrypted the space division, which was further stored at rider/driver side until it was updated. After a driver is assigned to a rider, they need a secure communication channel to negotiate a specific pick-up location. FICA [145] established a secret key between a rider and a driver to enable secure communication. pRide [143] used somewhat homomorphic encryption cryptosystem and deep learning algorithms to achieve efficient and private matching. PGRide [144] designed an encrypted aggregate distance computation method based on somewhat homomorphic encryption to compute the aggregate distances from a set of riders to large-scale drivers.

Garra *et al.* [11] uses blind signatures [180] to prevent the system server from knowing the signed data during e-coin requesting. Therefore, an adversary cannot gain any useful information about the e-coins when they are withdrawn. PriParkRec [156] utilizes additive homomorphic encryption [169], [170] to allow aggregation of encrypted data.

CLASC [14] proposes a certificateless aggregate signcryption scheme to encrypt and aggregate road surface condition reports sent by vehicles. Each vehicle signcrypts a reports and sends it to an aggregator, e.g., RSU. The aggregator aggregates received reports and verifies their signatures in a batch. In the privacy-preserving cloud-based road condition monitoring scheme [15], a vehicle encrypts the road condition information with the root authority's public key. PPCS [158] leverages secureMmulti-Party Computation (MPC) [171] to ensure the privacy of data processing. In data collection, each vehicle randomly splits vehicular data into two parts, and sends the two parts to two RSUs. Each of the two RSUs computes an intermediate result and also splits the result into two parts before sending them to which are sent to two cloud platforms. The two cloud platforms secure data processing to acquire road congestion rates and the spatial-temporal correlation matrix. Roy and Madria [159] uses AES encryption at vehicle side to encrypt vehicular data including vehicle ID, location, and speed velocity, before sending them via an RSU to the edge server. Each edge server adopts the Schmidt-Samoa cryptosystem [172] to produce a public/private key pair, which is used by nearby vehicles for secure key exchange and identity broadcasting.

Insights: Although many encryption schemes provide data privacy in VNs, their natural disadvantage that researchers can possibly point out is low efficiency. With the advancement of user-side devices regarding computational capability, memory, and energy storage, most encryption schemes are further supported. However, 5GVNs have significantly improved the downloading speed, which in turn puts extra pressure on local processing powers. Lightweight cryptography [173], [174], [175] is a potential candidate to solve this issue. It is tailored to be implemented efficiently on constrained devices including sensors and RFID tags. To fully support processing a huge amount of data that a device or a server will encounter, it still remains a challenge to testify whether it could satisfy the new demands of 5GVN services.

B. IDENTITY PRIVACY

PiSim [6] utilizes anonymous authentication [176] to authenticate users while not revealing their real identities. Each user registers to a trusted authority to obtain a group secret key, which is used to generate a temporary identity token for authentication. If a user misbehaves, the proposed scheme can disclose her/his real identity from the identity token with the help of the trusted authority and guarantee conditional privacy [10]. PiSim also integrates request-limiting property [177] in authentication process to resist multiple requesting attacks. Users' service rates are controlled while preserving their anonymity.

ORide [9] leverages the computationally efficient and provably secure anonymous credentials light [178] based on the DDH assumption to make users' messages unlinkable. Users have to request a set of Anonymous Credentials (ACs) from the SP. One drawback of using ACs issued by the SP is that the issuer, i.e., verifier, can de-anonymize users by correlating time when ACs are created with the time they are used. To solve this problem, the user are asked to choose the time of requesting ACs carefully. PrivateRide [109] provides rider anonymity and rider anonymity during logins, payments, and reputation rating. A rider logins in the RHS by using an AC. After a ride is over, the rider pays the SP with E-cash [179] issued on settled denominations at a random time. A rider and the matched driver exchange reputation tokens created by blind signatures [180] to anonymously rate each other. CoRide [148] constructs a consortium blockchain among different RHS providers. It preserves users' identity privacy in a conditional way [181] and only reveals a misbehaved user if all providers are present. A user registers to a certificate authority to receive an AC and stores her/his real identity under multiple public encryption at a service provider. If the user has some malicious behavior, the certificate authority compute the secret key of the users from his/her AC and then all the providers decrypt the pre-stored ciphertext to recover the real identity. OLink [149] is a special RHS that aims to address the privacy issues raised in a new function order-linking, i.e., a driver who is taking a rider can take the order of another rider who is near the current rider's destination. It allows riders and drivers to request several certified pseudonyms used for identity authentication.

SPARK [10] provides convenient parking services to drivers by employing RSUs to monitor and manage the parking lots. It converts each vehicle's real identifier into a pseudo-ID via symmetric encryption. When a vehicle has some malicious behaviors, the RSUs can learn the vehicle's real identifier by asking the trusted authority to decrypt the pseudo-ID. ASAP [12] calls upon utilizing private parking spots from residential communities and company-owned parking spots to alleviate public parking problems. It leverages a short randomizable group signature scheme [176] to protect the identity privacy of cruising drivers and parking spot suppliers. Each user registers to a trusted authority to obtain a group secret key and the group public key. In each driver querying/supplier reporting, a driver/supplier randomizes the group secret key and computes an AC for anonymous identity verification. ASAP also uses fixed denominations and E-cash [180] to achieve anonymous payment from drivers to suppliers. Huang *et al.* [152] protect drivers' identity privacy by using zero-knowledge proofs [182] and explicitly defend the double reservation attack, where an anonymous driver repetitively sends reservation requests to the parking service provider. In PrivAV [153], each user registers to the Automated Valet Parking (AVP) service provider to acquire a service credential [183] and use the credential to request AVP service without revealing identity information. In the private parking scheme based on blockchain [154], drivers and suppliers self-generate a random pseudonym and a corresponding AC based on distributed anonymous credentials [184] and a blockchain. Such ACs improve the privacy of traditional ACs by using blockchain to remove a trusted certificate authority. PriParkRec [156] also resorts to

decentralized anonymous credentials [184] for anonymous authentication.

CLASC [14] asks users to select a random number and multiply it by the group generator to compute a pseudo identity. Wang *et al.* [15] proposes a method to verify the source when processing a road condition report. After a driver sends a report to the cloud server, the cloud serve performs soundness verification on the report to filter out fake information sent by malicious drivers. PAM [140] is a privacy-preserving traffic monitoring scheme with a false report filtering function. It utilizes BBS signature [185] to offer anonymous authentication and conditional identity revealing.

Block4Forensic aims to offer a lightweight privacy-preserving blockchain by covering all stakeholders such as vehicle manufacturers, drivers, factories, and law enforcement officers. It adopts pseudo identities from the vehicular public key infrastructure model defined in IEEE 1609.2 to satisfy user anonymity.

Insights: Traditional identity privacy-preserving mechanisms, e.g., k-anonymity, have their own inherent deficiency for only giving a generalization method to protect a user's privacy. Pseudonyms and ACs can hide users' identity, but have to solve the linkability problem. If they can be linked, identity privacy is still at risk. Meanwhile, identity is always correlated to the user's activity, e.g., request and response. Even if we manage to mask the identity and guarantee identity unlinkability, it would still be in vain if we cannot eliminate the relation between identity and activity.

C. LOCATION PRIVACY

Li *et al.* [6] argue that repeatedly submitting the same locations to a navigation server will result in serious location privacy violation even if differential privacy is leveraged to perturb locations. In order to protect the drivers' location privacy, they transform querying a navigation route into querying traffic congestion. Drivers have to request the traffic congestion on each road section along their navigation route. Next, they process locations by using privacy-preserving multi-keyword fuzzy search [186]. Contributing drivers generate an traffic indicator and a secure index of locations, while requesting drivers generate a trapdoor to match the indexes stored at a nearby fog node. If the matching result, i.e., inner product, is higher than a pre-defined threshold, the corresponding indicators are returned to the requesting drivers.

Aïvodji *et al.* [7] allow users to collaboratively calculate common pick-up location and drop-off location via Private Set Intersection (PSI) [187]. The two users build two private input sets: integer identifiers of candidate pick-up locations and integer identifiers of candidate drop-off locations. Next, they encrypt the inputs and learn only the common ridesharing locations via PSI. Performance is another important service metric for ride-hailing. To protect location privacy protection without sacrificing much performance, Tong *et al.* [8] proposed a scheduling protocol. Riders are first scheduled to a driver group by a jointly differentially private optimization process according to the private dual decomposition [188]. Next, a driver is assigned to each rider to be served based on private rider assignment. ORide [9] utilizes somewhat homomorphic encryption [189] to enable operations over users' ciphertexts without decrypting them. A rider encrypts her location with a public key. The ride sends the location zone, the public key, and the encrypted location. The SP broadcasts the public key to drivers in the location zone, which responds to the SP with their encrypted locations. Next, the SP computes the encrypted squared Euclidean distances between the rider and drivers. PrivateRide [109] uses cloaking to hide the real pick-up locations. TRACE [142] protects locations by transforming them into a square and then encrypting them with a quadtree and random numbers. CoRide [148] facilitates private proximity test [190] to authenticate users' locations and leverages SkNN [191] to complete user matching. A rider collects environmental signals within a certain area to compute a location tag. Next, the rider inserts her public key into the location tag for the proximity test. The drivers can recover this public key correctly only if they are near the rider. Meanwhile, the rider inserts her conditions and a destination into an indistinguishable Bloom filter. A nearby driver computes two trapdoors of conditions and a possible destination. An RSU will finally complete the matching process by querying the trapdoors to the Bloom filter. Calculating shortest distances on massive road networks is computationally extensive. It is also difficult to compute the nearest driver for a rider in the ciphertext domain. To solve this problem, pRide [146] uses road network embedding [192] and homomorphic encryption [193], [194], [195] to efficiently and privately compute the shortest distances between users. It converts the current road network into a higher embedding space and estimates the road distance between users using their corresponding sketches. Homomorphic encryptions and garbled circuits are further used to achieve privacy-preserving and efficient user matching. Similarly, lpRide [147] achieves efficient computation of shortest road distance over ciphertexts based on road network embedding and a modified Paillier cryptosystem. In OLink [149], an RSU conducts user matching through querying a driver's ride response to a rider's ride request by using secure k nearest neighbor query [196]. Xie *et al.* [150] presented a ride-hailing matching protocol to enable private distance computation without a trusted third-party. They also realize distance computation based on road network embedding and achieve private ride-matching based on property-preserving hash. Specifically, road network embedding vectors are encrypted into bit-blocks through bilinear mapping. The rider service provider privately conducts distance comparisons via bilinear mappings.

ASAP [12] borrows a cloaking technique to cover a driver or a supplier's area. First, it divides Beijing's map multiple cells and expands a user's location to cell index. The drivers and suppliers send a cell index to the parking service provider for matching. Second, the provider returns a result to the

driver. The supplier and the driver know each other's detailed location when they negotiate successfully. P-SPAN [151] uses AES encryption to protect the current location and the destination of drivers. A driver first encrypts the location information with a hash value of the server's public key exponentiate by a random number. The server decrypts the received ciphertext with a hash value on the group generator exponentiated by its secret key. Huang *et al.* [152] resort to differential privacy to protect drivers' location privacy. They generate random noises from the geo-indistinguishable mechanism [121] and add them to the drivers' locations. PrivAV [153] encrypts drivers' current location based on the AES encryption and encrypts the pickup code based on the ElGamal encryption. Wang *et al.* [154] also make use of cloaking to hide the real locations of drivers and suppliers. DFPS [155] protects location privacy problems with entropy-based cloaking. It conceals drivers' destinations from the parking dispatcher, which cannot associate different parking requests sent by the same driver. Each driver has a unique privacy profile, including a pseudonym and k. The integer k means that a driver's destination should be indistinguishable among $k-1$ neighbor destinations, i.e., $k-$anonymous.

Since anonymous drivers can be tracked by linking anonymous location traces with other sources, Hoh *et al.* [13] utilize virtual trip lines, i.e., geographical markers, to update a position and speed when a probe vehicle drivers by. Instead of asking contributing drivers to upload traffic reports periodically, virtual trip lines are deployed to avoid traffic updates from sensitive locations. PAM [140] adopts range query processing [196] and variant Bloom filters for local RSUs to learn traffic conditions from encrypted driving reports without sacrificing drivers' location privacy. Each contributing driver encodes her/his location and speed by prefix encoding [197] and then inserts the encoded information with a random number into a Bloom filter, which is an index. The index is uploaded to an RSU which acquires the driver's location range and speed range by computing a trapdoor and querying the trapdoor to the index.

Insights: Simple but common location privacy-preserving techniques, e.g., cloaking, cannot provide rigorous privacy guarantees in 5GVN. It is well-acknowledged to utilize differential privacy [121] to perturb the real location to a noisy one. However, enforcing differential privacy in 5GVN has to address three issues in real deployment, i.e., correlation with activity [136], repeated submission [198], [199], and utility. Similar to identity privacy, if the inner correlation with activity is exposed, users' locations are endangered. If one repeatedly uses differential privacy to submit the same location, the privacy budget will eventually be consumed. How to find the right balance between privacy and utility is also another interesting topic. We notice that some works only focus on location privacy while not protecting identity privacy [7]. It is also an important task to protect data privacy, identity privacy, and location privacy at the same time.

D. TRAJECTORY PRIVACY

TrPF [163] is a trajectory privacy-preserving framework that improves the theoretical mix-zones model while integrating a time factor based on graph theory. It divides the whole trajectories into nonsensitive trajectory segments and sensitive trajectory segments. It protects the sensitive trajectory segments by using a mix-zones model and pseudonyms. PROS [128] is a privacy-preserving route-sharing scheme that allows vehicular friends to share real-time trajectories in a navigation app. A group leader sends a group formation request to a local RSU and several group members send a group participation to a nearby RSU. The RSUs computes a group via private equality test [200]. Finally, the leader and her/his group members share their routes through communication protected by the same group communication key. QLDS [164] is a trajectory privacy-preserving scheme with utility guarantee. It records the critical query logics related to personal privacy at user side client while storing the unclustered location tuples at server side. Next, 100 percent trajectory reconstruction is performed at user side and privacy preservation is guaranteed at server side. RPTR [165] is a trajectory privacy-preserving mechanism with differential privacy. It utilizes a dynamic sampling approach to process trajectories to meet the application load and practicability. At the same time, it proposes a privacy budget allocation scheme to better protect regions with high user density based on regional privacy weight.

Insights: Trajectory privacy relies on location privacy, except that it raises more challenges for a sequence protection. Not only the locations on the same trajectory is generated by the same user, but they follow a mobility pattern of a human. Therefore, it is quite tricky to design a trajectory privacy-preserving solution given a specific 5GVN service.

VII. FUTURE RESEARCH DIRECTIONS

In this section, we discuss five future research directions in 5GVN as shown in Fig. 5: semantic privacy, user-defined privacy, privacy computing, zero trust, and quantification and standardization.

We first concentrate on discussing semantic privacy in location privacy to advocate utilizing location semantics. Meanwhile, it is also important to support user-defined privacy to meet different user requirements. This is extremely urgent in the current digital world with various customized services. Such services have promoted the idea of privacy computing which posits as a combination of existing privacy-enhancing techniques and aims at addressing privacy issues in extensive areas. Furthermore, trust will continue to influence users' behaviors and systems' decision in 5GVN. Reliable trust management is more appealing to both users and systems. Last but not least, we need well-acknowledged metrics to quantify privacy and expect to promote standardization when we are building a privacy-preserving 5GVN.

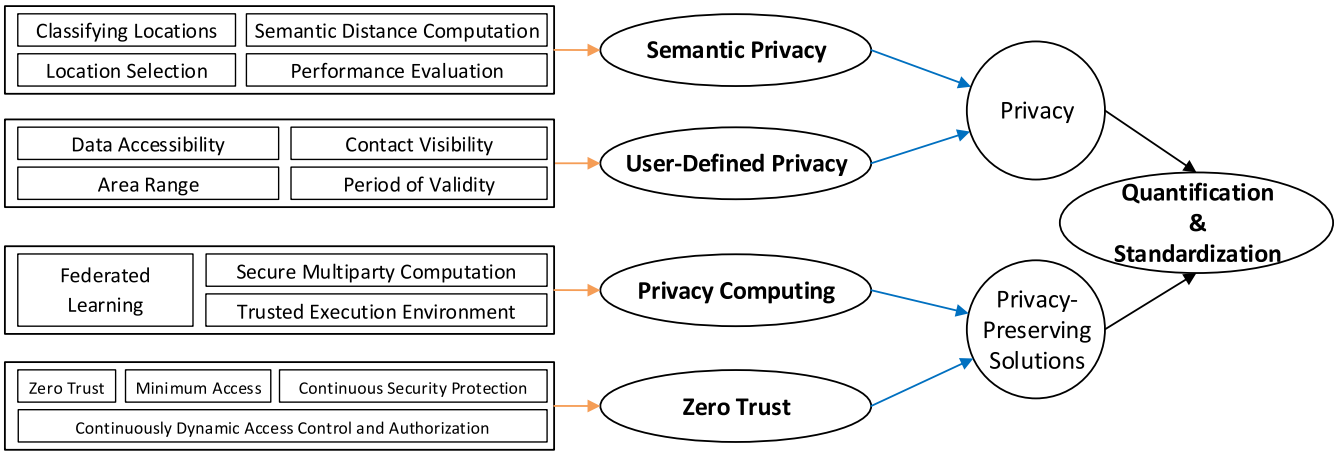


FIGURE 5. Future Research Directions.

A. SEMANTIC PRIVACY

We first discuss semantic privacy [201], [202], [203] in location privacy. Our observation is that protecting a location merely based on differential privacy is not enough. This is because a location is more than just two coordinates. Here, by location, we mean an actual place, e. g., a restaurant, a supermarket, and a hospital. Each location has its own semantic meanings that can be classified into different categories, such as diet, life necessity, and health, corresponding to the examples above. Furthermore, a location is not only just geographically correlated to other locations, but semantically attached to other locations. For example, a visit to a hot pot restaurant is sometimes followed by a purchase in an adjacent ice cream shop. Therefore, a semantically meaningful location tells much about a user's activity, let alone a location with a specific time.

To protect location privacy while considering location semantics, we should proceed in four steps. (1) Classifying locations. We first give each location a semantic tag and classify them into different semantic groups. (2) Semantic distance computation. For two locations within the same group and two locations belonging to two groups, we need to compute the semantic distance between the two locations. (3) Location selection. After comprehending the locations semantically, we can select a set of candidate locations to protect our real location by using a proper method. (4) Performance evaluation. After obtaining a set of candidate locations, we have to validate their efficacy to see to what extent we can lower the adversary's expected estimation error [204], [205].

B. USER-DEFINED PRIVACY

User-defined privacy [206], [207], [208] is not a new concept. It allows users to define their privacy level and how much privacy can be exposed in exchange for service quality. The users can define their privacy level by two means. First, we allow users to define their privacy level. For example, a user can choose a grid of 50x50 meter^2 or a grid of 100x100 meter^2 to submit to a location server for a restaurant recommendation service. The two different grids indicate two different privacy levels where the first one is higher than the second one. Second, we can recommend a privacy level for users based on users' choices.

In 5GVN services, users will come up with more privacy demands which raise more requirements on privacy-preserving solutions. Such demands include data accessibility, contact visibility, area range (as we explained above), and period of validity. Data accessibility refers to which part of a user's uploaded data can be accessed. The privacy concern behind this point is that a user may consider her data partially sensitive, and she does not want anyone other than the service provider to access it. Contact visibility means which group of users can know the identity of activity of a user. Since a user puts her contacts in different circles of trust, she tends to hide her identity or activity from certain contacts. It resembles access control [209], [210], [211] in modern cryptography, but it requires a higher processing efficiency toward a huge number of users. Period of validity addresses the fact that a user can customize the expiration date of her data. If she revokes consent or considers the uploaded data unnecessary, she has the right to ask for secure data deletion [212], [213], [214] from the service provider.

C. PRIVACY COMPUTING

Existing privacy-preserving solutions cannot provide systematic privacy preservation [215], given the new system architecture and service requirements in 5GVNs. The new concept Privacy Computing (PC) opens a new possibility to address this issue. PC is a new technical framework that covers the whole life-cycle preservation of sensitive information. Generally, PC is about a computing theory and methodology that facilitates the processing of sensitive information in a pervasive network. The four principles of privacy computing are *atomicity*, *consistency*, *sequence*, and *reversibility*.

PC integrates three distinctive components, namely Federated Learning (FL), Secure Multiparty Computation (SMC), and Trusted Execution Environment (TEE). The first two techniques compute a function of raw data

information together without transferring the raw data. In FL [216], [217], [218], the model training is distributed over user devices, and each device conduces to the learning model by individually calculating the gradient with local training data. FL supports data privacy and a huge number of devices. SMC [219], [220], [221] allows multiple parties to collaborate and achieves data privacy while guaranteeing the correctness of outputs. TEE [222], [223], [224] is a secure execution environment for raw data, and it is separated from the processing environment where the operating system and applications run. It is foreseeable that PC will be fully integrated with 5GVN in the near future [225], [226], [227].

D. ZERO TRUST

The National Institute of Standards and Technology (NIST) has put forth the idea and model of Zero Trust (ZT). ZT [228], [229], [230] is a new framework as well as a technical concept that believes in trusting no one and continuously authenticating everyone. Its core idea is that anyone and anything (including users, devices, applications, and packets) inside and outside a system are untrustworthy by default, and they should be authenticated when they are requesting resources. It has four basic principles: all zero trust, minimum access, continuously dynamic access control and authorization, and continuous security protection. It is predictable that ZT will be adopted in 5GVN to enhance authentication.

E. QUANTIFICATION AND STANDARDIZATION

After we are provided a set of privacy-preserving solutions to privacy issues in 5GVNs, we need to evaluate their protection efficacy [204], [231]. Many metrics [232], [233], [234] have been proposed to quantify privacy in VNs, these metrics are targeted to measure how users' privacy is leaked, including identity privacy and location privacy. Despite the differences between 5GVNs and traditional VNs, these metrics are applicable to 5GVNs. Still, there are three aspects to be explored: quantification metrics for multimedia privacy and dynamic adjustment of quantification metrics [231].

Last but not the least, we need to standardize the privacy-preserving techniques in real-world systems for convenient deployment and integration. The standardization are two folds. The first one is to formulate a general framework and parameters of techniques. The second one is to recommended a specific set of deployment details for a target system, given that different systems vary in privacy requirement. On the other hand, although technologies may come to rescue [235] to some extent, we still need further regulations such as the EU General Data Protection Regulation [236] and Personal Information Security Specification in China [237].

VIII. CONCLUSION

5GVN is a new architecture that revolutionizes vehicular networks by bringing new features and supporting a large-scale services. With the ubiquity of 5G and electric vehicles, 5GVN will further merge into our lives. However, there still exist privacy threats, which raise various privacy concerns towards vehicular users. In this paper, we have presented a comprehensive survey of privacy-preserving solutions for 5GVN. We have first reviewed the architecture, features, and services of 5GVN. We have discussed the privacy objectives and privacy threats in 5GVN. Next, we have introduced the privacy-preserving solutions techniques for 5GVNs. Finally, we have discussed the future research directions to call for attention and efforts into 5GVN and its privacy issues.

ACKNOWLEDGMENT

This work was carried out during the tenure of an ERCIM 'Alain Bensoussan' Fellowship Programme granted to Dr. Meng Li.

REFERENCES

[1] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093.

[2] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar./Apr. 2020.

[3] X. Xu, Y. Zeng, Y. L. Guan, and Y. Li, "Cellular-V2X communications with weighted-power-based mode selection," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 386–400, 2020.

[4] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.

[5] L. Wang, G. Liu, and L. Sun, "A secure and privacy-preserving navigation scheme using spatial crowdsourcing in fog-based VANETs," *Sensors*, vol. 17, no. 4, p. 668, 2017.

[6] M. Li, Y. Chen, S. Zheng, D. Hu, C. Lal, and M. Conti, "Privacy-preserving navigation supporting similar queries in vehicular networks," *IEEE Trans. Depend. Secure Comput.*, early access, Aug. 18, 2020, doi: 10.1109/TDSC.2020.3017534.

[7] U. M. Aïvodji, S. Gambs, M.-J. Huguet, and M.-O. Killijian, "Meeting points in ridesharing A privacy-preserving approach," *Transport. Res. C Emerg. Technol.*, vol. 72, pp. 239–252, Nov. 2016.

[8] W. Tong, J. Hua, and S. Zhong, "A jointly differentially private scheduling protocol for ridesharing services," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2444–2456, Oct. 2017.

[9] A. Pham *et al.*, "ORide: A privacy-preserving yet accountable ride-hailing service," in *Proc. 26th USENIX Security Symp.*, Aug. 2017, pp. 1235–1252.

[10] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A new VANET-based smart parking scheme for large parking lots," in *Proc. 28th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1413–1421.

[11] R. Garra, S. Martínez, and F. Sebé, "A privacy-preserving pay-by-phone parking system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5697–5706, Jul. 2017.

[12] L. Zhu, M. Li, Z. Zhang, and Z. Qin, "ASAP: An anonymous smart-parking and payment scheme in vehicular networks," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 4, pp. 703–715, Jul./Aug. 2020.

[13] B. Hoh *et al.*, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proc. 6th Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Jun. 2008, pp. 15–28.

[14] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing based road surface condition monitoring system using fog computing," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 772–782, Jun. 2017.

[15] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1779–1790, Jul. 2019.

[16] X. Feng, E. S. Dawam, and S. Amin, "A new digital forensics model of smart city automated vehicles," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Exeter, U.K., Jun. 2017, pp. 274–279.

[17] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.

[18] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.-K. R. Choo, "Smart vehicle forensics: Challenges and case study," *Future Gener. Comput. Syst.*, vol. 109, pp. 500–510, Aug. 2020.

[19] *Google Maps*. Accessed: May 6, 2021. [Online]. Available: https://www.google.com/maps

[20] *Waza*. Accessed: May 6, 2021. [Online]. Available: https://www.waze.com

[21] *Uber Rides Unchallenged in the Top Spot of the Global Taxi and Limousine Market*. Accessed: May 6, 2021. [Online]. Available: https://www.globenewswire.com/news-release/2020/11/25/2133871/0/en/Uber-Rides-Unchallenged-In-The-Top-Spot-Of-The-Global-Taxi-And-Limousine-Market.html

[22] *After $1 Billion Profit From Rides, Didi Chuxing Considers Second-Half IPO*. Accessed: May 6, 2021. [Online]. Available: https://www.theinformation.com/articles/after-1-billion-profit-from-rides-didi-chuxing-considers-second-half-ipo

[23] *Smart Parking Mobile App*. Accessed: May 6, 2021. [Online]. Available: https://www.smartparking.com/smartpark-system/smart-app

[24] *We Automate Your Parking*. Accessed: May 6, 2021. [Online]. Available: https://landing.smartparking apps.com

[25] *4Park, 4Bus, 4Business: The App for Payments, Booking and Authorizations*. Accessed: May 6, 2021. [Online]. Available: https://smartparkingsystems.com/en/4-park-smart-parking-app

[26] *In-Car Apps Market Size, Industry Analysis Report, Regional Outlook, Application Development, Price Trend, Competitive Market Share & Forecast, 2021–2027*. Accessed: May 6, 2021. [Online]. Available: https://www.gminsights.com/industry-analysis/in-car-apps-market

[27] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: May 6, 2021. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[28] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[29] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[30] D. Sperling and D. Gordon, "Two billion cars: Transforming a culture," *TR News*, vol. 259, pp. 3–9, Nov. 2008. Accessed: May 6, 2021.

[31] *The Global In-Vehicle Infotainment Market Is Projected to Reach USD 54.8 Billion by 2027 From an Estimated USD 24.3 Billion in 2019, at a CAGR of 10%*. Accessed: May 6, 2021. [Online]. Available: https://www.globenewswire.com/news-release/2020/02/06/1980888/0/en/The-global-in-vehicle-infotainment-market-is-projected-to-reach-USD-54-8-billion-by-2027-from-an-estimated-USD-24-3-billion-in-2019-at-a-CAGR-of-10-7.html

[32] *Tesla*. Accessed: May 6, 2021. [Online]. Available: https://www.tesla.com

[33] *Nio*. Accessed: May 6, 2021. [Online]. Available: https://www.nio.cn/about

[34] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[35] D. Soldani and A. Manzalini, "Horizon 2020 and beyond: On the 5G operating system for a true digital society," *IEEE Veh. Technol. Mag.*, vol. 10, no. 1, pp. 32–42, Mar. 2015.

[36] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[37] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.

[38] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," *IEEE Veh. Technol. Mag.*, vol. 5, no. 1, pp. 77–84, Mar. 2010.

[39] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 1, pp. 383–398, Jan. 2019.

[40] A. Moubayed, A. Shami, P. Heidari, A. Larabi, and R. Brunner, "Edge-enabled V2X service placement for intelligent transportation systems," *IEEE Trans. Mobile Comput.*, vol. 20, no. 4, pp. 1380–1392, Apr. 2021.

[41] M. Tariq, F. Naeem, M. Ali, and H. V. Poor, "Vulnerability assessment of 6G enabled smart grid cyber-physical systems," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5468–5475, Apr. 2021.

[42] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain based lightweight and secured V2V communication in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021.

[43] E. Horvitz and D. Mulligan, "Data, privacy, and the greater good," *Science*, vol. 349, no. 6245, pp. 253–255, 2015.

[44] M. Li, F. Wu, G. Chen, L. Zhu, and Z. Zhang, "How to protect query and report privacy without sacrificing service quality in participatory sensing," in *Proc. 34th IEEE Int. Perform. Comput. Commun. Conf. (IPCCC)*, Nanjing, China, Dec. 2015, pp. 1–7.

[45] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[46] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2017.

[47] J. Ni, A. Zhang, X. Lin, and X. Shen, "Security, privacy, and fairness in fog-based vehicular crowdsensing," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 146–152, Jun. 2017.

[48] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[49] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, 4th Quart., 2020.

[50] H. M. Furqan, M. S. J. Solaija, H. Türkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 287–321, 2021.

[51] Y. Li, Y. Yu, W. Susilo, Z. Hong, and M. Guizani, "Security and privacy for edge intelligence in 5G and beyond networks: Challenges and solutions," *IEEE Wireless Commun.*, vol. 28, no. 2, pp. 63–69, Apr. 2021.

[52] L. Zhu and M. Li, "DoS-resilient secure data aggregation in wireless sensor networks," in *Proc. 17th ACM Annu. Int. Conf. Mobile Comput. Netw. (ACM MobiCom)*, Sep. 2011, pp. 1–2.

[53] L. Zhu and M. Li, "An energy efficient and integrity-preserving aggregation protocol in wireless sensor networks," in *Proc. 30th IEEE Int. Perform. Comput. Commun. Conf. (IPCCC)*, Orlando, FL, USA, Dec. 2011, pp. 1–6.

[54] K. Fawaz, H. Feng, and K. G. Shin, "Anatomization and protection of mobile apps' location privacy threats, in *Proc. 24th USENIX Security Symp. (USENIX Security)*, Washington, DC, USA, Aug. 2015, pp. 753–768.

[55] Y. Michalevsky, A. Schulman, and G. Nakibly, "PowerSpy: Location tracking using mobile device power analysis," in *Proc. 24th USENIX Security Symp. (USENIX Security)*, Washington, DC, USA, Aug. 2015, pp. 785–800.

[56] N. Sivan, R. Bitton, and A. Shabtai, "Analysis of location data leakage in the Internet traffic of Android-based mobile devices," in *Proc. 22nd Int. Symp. Res. Attacks Intrusions Defenses (RAID)*, Beijing, China, Sep. 2019, pp. 243–260.

[57] K. Barry. *Tesla's In-Car Cameras Raise Privacy Concerns*. Accessed: May 6, 2021. [Online]. Available: https://www.consumerreports.org/privacy/teslas-in-car-cameras-raise-privacy-concerns

[58] G. A. Fowler. *What Does Your Car Know About You? We Hacked a Chevy to Find Out*. Accessed: May 6, 2021. [Online]. Available: https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out

[59] Y. Xie, F. Li, Y. Wu, S. Yang, and Y. Wang, "D^3-guard: Acoustic-based drowsy driving detection using smartphones," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, May 2019, pp. 1225–1233.

[60] D. Liu *et al.*, "User association in 5G networks: A survey and an outlook," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1018–1044, 2nd Quart., 2016.

[61] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 905–929, 2nd Quart., 2020.

[62] M. Shafi *et al.*, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE Commun. Surveys Tuts.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[63] *IEEE 5G and Beyond Technology Roadmap White Paper*. Accessed: May 6, 2021. [Online]. Available: https://futurenetworks.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf

[64] Huawei. *5G Network Architecture: A High-Level Perspective*. Accessed: May 6, 2021. [Online]. Available: https://www-file.huawei.com/-/media/corporate/pdf/mbb/5g_nework_architecture_whitepaper_en.pdf?la=en

[65] G. Caruso *et al.*, "Embedding 5G solutions enabling new business scenarios in media and entertainment industry," in *Proc. 2nd IEEE 5G World Forum*, Dresden, Germany, Sep./Oct. 2019, pp. 460–464.

[66] F. Tang, L. Liu, H. Dai, N. Xu, C. Wang, and N. Zhang, "Integrated energy service for '5G' in China: Market prediction and case study," in *Proc. 4th IEEE Conf. Energy Internet Energy Syst. Integrat. (EI2)*, Wuhan, China, Oct./Nov. 2020, pp. 670–683.

[67] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, Aug. 2018.

[68] L. Zhu *et al.*, "Privacy-preserving authentication and data aggregation for fog-based smart grid," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 80–85, Jun. 2019.

[69] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.

[70] W. Tärneberg *et al.*, "Towards intelligent industry 4.0 5G networks: A first throughput and QoE measurement campaign," in *Proc. 28th Int. Conf. Softw. Telecommun. Comput. Netw. (SoftCOM)*, Split, Croatia, Sep. 2020, pp. 1–6.

[71] A. Aissioui, A. Ksentini, A. M. Gueroui, and T. Taleb, "On enabling 5G automotive systems using follow me edge-cloud concept," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5302–5316, Jun. 2018.

[72] *Different Types of Sensors Used in Automobiles*. Accessed: May 6, 2021. [Online]. Available: https://www.elprocus.com/different-types-of-sensors-used-in-automobiles

[73] R. A. Uzcátegui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, pp. 126–133, May 2009.

[74] F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st ACM Workshop Mobile Cloud Comput. (MCC)*, Helsinki, Finland, Aug. 2012, pp. 13–16.

[75] M. Chiang, S. Ha, I. Chih-Lin, F. Risso, and T. Zhang, "Clarifyingf fog computing and networking: 10 questions and answers," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 18–20, Apr. 2017.

[76] B. Bangerter, S. Talwar, R. Arefi, and K. Stewart, "Networks and devices for the 5G era," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 90–96, Feb. 2014.

[77] W. Hong, K.-H. Baek, Y. Lee, Y. Kim, and S.-T. Ko, "Study and prototyping of practically large-scale mmWave antenna systems for 5G cellular devices" *IEEE Commun. Mag.*, vol. 52, no. 9, pp. 63–69, Sep. 2014.

[78] *Mi 10 Pro*. Accessed: May 6, 2021. [Online]. Available: https://www.mi.com/global/mi-10/specs

[79] *iPhone 12*. Accessed: May 6, 2021. [Online]. Available: https://www.apple.com/iphone/?afid=p2%7CsusbukMQN-dc_mtid_20925d2q39172_pcrid_516026392071_pgrid_112315339198_&cid=wwa-us-kwgo-iphone–slid—Brand-iPhone-Avail-

[80] *China Telecom Reveals 5G User Numbers*. Accessed: May 6, 2021. [Online]. Available: https://www.mobileworldlive.com/featured-content/top-three/china-telecom-reveals-5g-user-numbers

[81] *Top Five Reasons to Choose an Electric Car*. Accessed: May 6, 2021. [Online]. Available: https:www.ucsusa.org/resources/top-five-reasons-choose-electric-car?gclid=EAIaIQobChMIhMyK6dLK8AIVFSyzAB2MNguKEAAYAiAAEgL8u_D_BwE&utm_campaign=CV&utm_medium=search&utm_source=googlegrants

[82] *How 5G & IoT Technologies Are Driving the Connected Smart Vehicle Industry*. Accessed: May 6, 2021. [Online]. Available: https://www.businessinsider.com/iot-connected-smart-cars

[83] *Instant Access to Multimodal Traffic Data for All Regions and Roadways*. Accessed: May 6, 2021. [Online]. Available: https://learn.streetlightdata.com/traffic-data?utm_source=Google-Adwords&utm_medium=Paid-Search&utm_campaign=StreetLight-Data-NB&utm_term=traff%20data&creative=476895313907&keyword=traff%20data&matchtype=b&network=g&device=c&utm_term=traff%20data&utm_campaign=StreetLight-Data-NB-GGL&utm_source=adwords&utm_medium=ppc&hsa_acc=7146595976&hsa_cam=2074001720&hsa_grp=79997292194&hsa_ad=476895313907&hsa_src=g&hsa_tgt=kwd-297807231301&hsa_kw=traff%20data&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMInfaEkuzK8AIV7ObjBx09Qgg8EAAYBCAAEgLq4vD_BwE

[84] S. S. Husain, A. Kunz, A. Prasad, E. Pateromichelakis, and K. Samdanis, "Ultra-high reliable 5G V2X communications," *IEEE Commun. Stand.*, vol. 3, no. 2, pp. 46–52, Jun. 2019.

[85] J. Ordonez-Lucena *et al.*, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[86] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.

[87] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.

[88] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing: A key technology towards 5G," vol. 11, ETSI, Sophia Antipolis, France, White Paper, 2015, pp. 1–16.

[89] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[90] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

[91] *5G Speed Is Data Transmission in Real Time*. Accessed: May 6, 2021. [Online]. Available: https://www.telekom.com/en/company/details/5g-speed-is-data-transmission-in-real-time-544498

[92] *5G Download Speeds in U.S. at Meager 47-58 Mbps Range, Per Opensignal*. Accessed: May 6, 2021. [Online]. Available: https://www.fiercewireless.com/5g/5g-downloa
d-speeds-u-s-at-meager-47-58-mbps-range-per-opensignal

[93] Z. Chaloupka, "Technology and standardization gaps for high accuracy positioning in 5G," *IEEE Commun. Stand. Mag.*, vol. 1, no. 1, pp. 59–65, Mar. 2017.

[94] *5G Positioning: What You Need to Know*. Accessed: May 6, 2021. [Online]. Available: https://www.eric
sson.com/en/blog/2020/12/5g-positioning–what-you-need-to-know

[95] *Positioning for 5G*. Accessed: May 6, 2021. [Online]. Available: https://www.iis.fraunhofer.de/en/ff/lv/
lok/5g.html

[96] S. Savage, "Lawful device access without mass surveillance risk: A technical design discussion," in *Proc. 25th ACM Conf. Comput. Commun. Security (CCS)*, Toronto, ON, Canada, Oct. 2018, pp. 1761–1774.

[97] J. Frankle, S. Park, D. Shaar, S. Goldwasser, and D. Weitzner, "Practical accountability of secret processes," in *Proc. 27th USENIX Security Symp. (USENIX Security)*, Baltimore, MD, USA, Aug. 2018, pp. 657–674.

[98] (2021). *Ride Hailing Taxi App Revenue and Usage Statistics*. Accessed: May 6, 2021. [Online]. Available: https://www.businessofapps.com/data/ride-hailing-app-market

[99] J. Lacroix, K. El-Khatib, and R. Akalu, "Vehicular digital forensics: What does my vehicle know about me?" in *Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl.*, New York, NY, USA, Nov. 2016, pp. 59–66.

[100] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1191–1221, 2nd Quart., 2020.

[101] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th Eur. Conf. Comput. Syst. (EuroSys)*, Porto, Portugal, Apr. 2018, pp. 1–15.

[102] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[103] L. Zhu, M. Li, Z. Zhang, X. Du, and M. Guizani, "Big data mining of users' energy consumption pattern in wireless smart grid," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 84–89, Feb. 2018.

[104] L. Zhu, M. Li, and Z. Zhang, "Secure fog-assisted crowdsensing with collusion resistance: From data reporting to data requesting," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5473–5484, Jun. 2019.

[105] Y. Chen, M. Li, S. Zheng, D. Hu, C. Lai, and M Conti, "One-time, oblivious, and unlinkable query processing over encrypted data on cloud," in *Proc. 22nd Int. Conf. Inf. Commun. Security (ICICS)*, Copenhagen, Denmark, Aug. 2020, pp. 350–365.

[106] M. Li, C. Lal, M. Conti, and D. Hu, "LEChain a blockchain-based lawful evidence management scheme for digital forensics," *Future Gener. Comput. Syst.*, vol. 115, pp. 406–420, Feb. 2021.

[107] D. Hu, Y. Li, L. Pan, M. Li, and S. Zheng, "A blockchain-based trading system for big data," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107994.

[108] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. London, U.K.: Chapman and Hall, 2014, pp. 1–603.

[109] A. Pham *et al.*, "PrivateRide: A privacy-enhanced ride-hailing service," in *Proc. 17th Privacy Enhanc. Technol. (PETS)*, vol. 2, 2017, pp. 38–56.

[110] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Proc. 21st Int. Conf. Data Eng. (ICDE)*, Tokyo, Japan, Apr. 2005, pp. 217–228.

[111] R. Geambasu, T. Kohno, A. A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in *Proc. 18th USENIX Security Symp.*, Aug. 2009, pp. 299–315.

[112] D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in *Proc. ACM SIGMOD Int. Conf. Manag. Data (SIGMOD)*, Athens, Greece, Jun. 2011, pp. 193–204.

[113] A. Acquisti, "Identity management, privacy, and price discrimination," *IEEE Security Privacy*, vol. 6, no. 2, pp. 46–50, Mar./Apr. 2008.

[114] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, 2020.

[115] H. Choudhury, B. Roychoudhury, and D. K. Saikia, "Enhancing user identity privacy in LTE," in *Proc. 11th IEEE Conf. Trust Security Privacy Comput. Commun. (TrustCom)*, Liverpool, U.K., Jun. 2012, pp. 949–957.

[116] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in *Proc. ACM SIGMOD Int. Conf. Manag. Data (SIGMOD)*, Vancouver, BC, Canada, Jun. 2008, pp. 121–132.

[117] Z. Zhu and G. Cao, "APPLAUS: A privacy-preserving location proof updating system for location-based services," in *Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1889–1897.

[118] X. Li and T. Jung, "Search me if you can: Privacy-preserving location query service," in *Proc. 32rd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2760–2768.

[119] K. W.-T. Leung, D. L. Lee, and W.-C. Lee, "CLR: A collaborative location recommendation framework based on co-clustering," in *Proc. 34th Int. ACM SIGIR Conf. Res. Develop. Inf. Retrieval (SIGIR)*, Beijing, China, Jul. 2011, pp. 305–314.

[120] H. Bagci and P. Karagoz, "Context-aware friend recommendation for location based social networks using random walk," in *Proc. 25th Int. Conf. Companion World Wide Web (WWW)*, Apr. 2016, pp. 531–536.

[121] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. 20th ACM Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, Nov. 2013, pp. 901–914.

[122] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proc. 21st ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Nov. 2014, pp. 251–262.

[123] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Constructing elastic distinguishability metrics for location privacy," in *Proc. 15th Privacy Enhanc. Technol. (PETS)*, vol. 2, Jun. 2015, pp. 156–170.

[124] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Colloquium Automata Lang. Program. (ICALP)*, Venice, Italy, 2006, pp. 1–12.

[125] J. Hua, Y. Gao, and S. Zhong, "Differentially private publication of general time-serial trajectory data," in *Proc. 34th IEEE Conf. Comput. Commun. (INFOCOM)*, Hong Kong, May 2015, pp. 549–557.

[126] M. Li, L. Zhu, Z. Zhang, and R. Xu, "Differentially private publication scheme for trajectory data," in *Proc. 1st IEEE Int. Conf. Data Sci. Cyberspace (DSC)*, Changsha, China, Jun. 2016, pp. 596–601.

[127] M. Li, L. Zhu, Z. Zhang, and R. Xu, "Achieving differential privacy of trajectory data publishing in participatory sensing," *Inf. Sci.*, vols. 400–401, pp. 1–13, Aug. 2017.

[128] M. Li, L. Zhu, Z. Zhang, X. Du, and M. Guizani, "PROS: A privacy-preserving route sharing service via vehicular fog computing," *IEEE Access*, vol. 6, pp. 66188–66197, 2018.

[129] A. Pham, K. Huguenin, I. Bilogrevic, I. Dacosta, and J.-P. Hubaux, "SecureRun: Cheat-proof and private summaries for location-based activities," *IEEE Trans. Mobile Comput.*, vol. 15, no. 8, pp. 2109–2123, Aug. 2016.

[130] Y. Zheng. *T-Drive Trajectory Data Sample*. Accessed: May 6, 2021. [Online]. Available: https://www.microsoft.com/en-us/research/publication/t-drive-trajectory-data-sample

[131] R. Chen, G. Acs, and C. Castelluccia, "Differentially private sequential data publication via variable-length n-grams," in *Proc. 19th ACM Conf. Comput. Commun. Security (CCS)*, Oct. 2012, pp. 638–649.

[132] L. Ou, Z. Qin, S. Liao, Y. Hong, and X. Jia, "Releasing correlated trajectories: Towards high utility and optimal differential privacy," *IEEE Trans. Depend. Secure Comput.*, vol. 17, no. 5, pp. 1109–1123, Sep./Oct. 2020.

[133] C.-Y. Chow and M. F. Mokbel, "Trajectory privacy in location-based services and data publication," *ACM SIGKDD Explor. Newslett.*, vol. 13, no. 1, pp. 19–29, 2011.

[134] S. Gao, J. Ma, C. Sun, and X. Li, "Balancing trajectory privacy and data utility using a personalized anonymization model," *J. Netw. Comput. Appl.*, vol. 38, pp. 125–134, Feb. 2014.

[135] Z. Hu, J. Yang, and J. Zhang, "Trajectory privacy protection method based on the time interval divided," *Comput. Security*, vol. 77, pp. 488–499, May 2018.

[136] Y. Cao, Y. Xiao, L. Xiong, L. Bai, and M. Yoshikawa, "Protecting spatiotemporal event privacy in continuous location-based services," *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 8, pp. 3141–3154, Aug. 2021.

[137] "NGMN 5G white paper," Next Gener. Mobile Netw. Alliance, Frankfurt, Germany, White Paper, 2015.

[138] M. Iwamura, "NGMN view on 5G architecture," in *Proc. 81st IEEE Veh. Technol. Conf. (VTC Spring)*, Glasgow, U.K., May 2015, pp. 1–5.

[139] A. Zhang and X. Lin, "Security-aware and privacy-preserving D2D communications in 5G," *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, Jul./Aug. 2017.

[140] M. Li, L. Zhu, and X. Lin, "Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing," *IEEE Trans. Services Comput.*, early access, Mar. 4, 2019, doi: 10.1109/TSC.2019.2903060.

[141] A. Griswold, *Uber Drivers Are Filming Their Riders and Sharing the Tapes Online*. Accessed: May 6, 2021. [Online]. Available: https://qz.com/985832/uber-drivers-are-filming-their-riders-with-dash-cams-to-protect-against-bad-reviews-and-false-accusations

[142] F. Wang *et al.*, "Efficient and privacy-preserving dynamic spatial query scheme for ride-hailing services," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11084–11097, Nov. 2018.

[143] J. Huang, Y. Luo, S. Fu, M. Xu, and B. Hu, "pRide: Privacy-preserving online ride hailing matching system with prediction," *IEEE Trans. Veh. Technol.*, early access, Jun. 17, 2021, doi: 10.1109/TVT.2021.3090042.

[144] H. Yu, H. Zhang, X. Yu, X. Du, and M. Guizani, "PGRide: Privacy-preserving group ridesharing matching in online ride hailing services," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5722–5735, Apr. 2021.

[145] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.

[146] H. Yu, J. Shu, X. Jia, H. Zhang, and X. Yu, "LpRide: Lightweight and privacy-preserving ride matching over road networks in online ride hailing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 10418–10428, Nov. 2019.

[147] Y. Luo, X. Jia, S. Fu, and M. Xu, "pRide: Privacy-preserving ride matching over road networks for online ride-hailing service," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1791–1802, Jul. 2019.

[148] M. Li, L. Zhu, and X. Lin, "CoRide: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing," in *Proc. 15th EAI Int. Conf. Security Privacy Commun. Netw. (SecureComm)*, Orlando, FL, USA, Oct. 2019, pp. 408–422.

[149] M. Li, J. Gao, Y. Chen, J. Zhao, and M. Alazab, "Privacy-preserving ride-hailing with verifiable order-linking in vehicular networks," in *Proc. 19th Int. Conf. Trust Security Privacy Comput. Commun. (TrustCom)*, Guangzhou, China, Dec. 2020, pp. 599–606.

[150] H. Xie, Y. Guo, and X. Jia, "A privacy-preserving online ride-hailing system without involving a third trusted server," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3068–3081, Mar. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9376938

[151] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6504–6517, Jul. 2018.

[152] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018.

[153] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Mar. 2019.

[154] L. Wang, X. Lin, E. Zima, and C. Ma, "Towards Airbnb-like privacy-enhanced private parking spot sharing based on blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2411–2423, Mar. 2020.

[155] A. Hakeem, R. Curtmola, X. Ding, and C. Borcea, "DFPS: A distributed mobile system for free parking assignment," *IEEE Trans. Mobile Comput.*, early access, May 14, 2021, doi: 10.1109/TMC.2021.3080222.

[156] Z. Li, M. Alazab, S. Garg, and M. S. Hossain, "PriParkRec: Privacy-preserving decentralized parking recommendation service," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4037–4050, May 2021.

[157] F. Zhu, Y. Lv, Y. Chen, X. Wang, G. Xiong, and F. -Y. Wang, "Parallel transportation systems: Toward IoT-enabled smart urban traffic control and management," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 10, pp. 4063–4071, Oct. 2020.

[158] W. Guo, J. Li, X. Liu, and Y. Yang, "Privacy-preserving compressive sensing for real-time traffic monitoring in urban city," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14510–14522, Dec. 2020.

[159] A. Roy and S. Madria, "Secure and privacy-preserving traffic monitoring in VANETs," in *Proc. 17th IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Delhi, India, Dec. 2020, pp. 567–575.

[160] C. N. Van Phu and N. Farhi, "Estimation of urban traffic state with probe vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2797–2808, May 2021.

[161] K. Dološ, C. Meyer, A. Attenberger, and J. Steinberger, "Driver identification using in-vehicle digital data in the forensic context of a hit and run accident," *Forensic Sci. Int. Digit. Invest.*, vol. 35, Dec. 2020, Art. no. 301090.

[162] K. K. G. Buquerin, C. Corbett, and H.-J. Hof, "A generalized approach to automotive forensics," *Forensic Sci. Int. Digit. Invest.*, vol. 36, Apr. 2021, Art. no. 301111.

[163] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, "TrPF: A trajectory privacy-preserving framework for participatory sensing," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 874–887, Jun. 2013.

[164] Z. Xiao, J.-J. Yang, M. Huang, L. Ponnambalam, X. Fu, and R. S. M. Goh, "QLDS: A novel design scheme for trajectory privacy protection with utility guarantee in participatory sensing," *IEEE Trans. Mobile Comput.*, vol. 17, no. 6, pp. 1397–1410, Jun. 2018.

[165] Z. Ma, T. Zhang, X. Liu, X. Li, and K. Ren, "Real-time priva cy-preserving data release over vehicle trajectory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8091–8102, Aug. 2019.

[166] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proc. 12th Annu. Netw. Distrib. Syst. Security Symp. (NDSS)*, San Diego, CA, USA, Feb. 2005, pp. 1–5.

[167] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proc. 5th Int. Conf. Appl. Cryptography Netw. Security (ACNS)*, Zhuhai, China, Jun. 2007, pp. 288–306.

[168] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[169] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184.

[170] D. Boneh, R. Gennaro, and S. Goldfeder, "Using level-1 homomorphic encryption to improve threshold DSA signatures for bitcoin wallet security," in *Proc. 8th Int. Conf. Cryptol. Inf. Security Latin America (LATINCRYPT)*, Sep. 2017, pp. 352–377.

[171] Y. Lindell, B. Pinkas, N. P. Smart, and A. Yanai, "Efficient constant-round multi-party computation combining BMR and SPDZ," *J. Cryptol.*, vol. 32, no. 3, pp. 1026–1069, 2019.

[172] K. Schmidt-Samoa, "A new rabin-type trapdoor permutation equivalent to factoring," *Electron. Notes Theor. Comput. Sci.*, vol. 157, no. 3, pp. 79–94, 2006.

[173] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design Test Comput.*, vol. 24, no. 6, pp. 522–533, Nov./Dec. 2007.

[174] D. Maimut and K. Ouafi, "Lightweight cryptography for RFID tags," *IEEE Security Privacy*, vol. 10, no. 2, pp. 76–79, Mar./Apr. 2021.

[175] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos, "Lightweight cryptography for embedded systems—A comparative analysis," in *Proc. 8th Int. Workshop Data Privacy Manag. Auton. Spontaneous Security*, Sep. 2013, pp. 333–349.

[176] D. Pointcheval and O. Sanders, "Short randomizable signatures," in *Proc. Topics Cryptol. Cryptographers Track RSA Conf. (CT-RSA)*, San Francisco, CA, USA, Feb./Mar. 2016, pp. 111–126.

[177] G. Maganis, E. Shi, H. Chen, and D. Song, "Opaak: Using mobile phones to limit anonymous identities online," in *Proc. 10th Int. Conf. Mobile Syst. Appl. Services (MobiSys)*, Jun. 2012, pp. 295–308.

[178] F. Baldimtsi and A. Lysyanskaya, "Anonymous credentials light," in *Proc. 20th ACM Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, Nov. 2013, pp. 1087–1098.

[179] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proc. 8th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1988, pp. 319–327.

[180] D. Chaum, "Blind signatures for untraceable payments," in *Proc. 2nd Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1982, pp. 19–203.

[181] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[182] M. Z. Lee, A. M. Dunn, J. Katz, B. Waters, and E. Witchel, "Anon-pass: Practical anonymous subscriptions," in *Proc. 34th IEEE Symp. Security Privacy (S&P)*, San Francisco, CA, USA, May 2013, pp. 319–333.

[183] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in *Proc. 5th Int. Conf. Security Cryptography Netw. (SCN)*, Maiori, Italy, Sep. 2006, pp. 111–125.

[184] C. Garman, M. Green, and I. Miers, "Decentralized anonymous credentials," in *Proc. 21st Netw. Distrib. Syst. Security Symp. (NDSS)*, San Diego, CA, USA, Feb. 2014, pp. 1–21.

[185] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. 24th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2004, pp. 41–55.

[186] B. Wang, S. C. Yu, W. J. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in *Proc. 33rd IEEE Int. Conf. Comput. (INFOCOM)*, Toronto, ON, Canada, Apr./May 2014, pp. 2112–2120.

[187] C. Aguilar-Melchor, J. Barrier, S. Guelton, A. Guinet, M.-O. Killijian, and T. Lepoint, "NFLlib: NTT-based fast lattice library," in *Proc. 16th Topics Cryptol. Cryptographers Track RSA Conf. (CT-RSA)*, San Francisco, CA, USA, Feb./Mar. 2016, pp. 341–356.

[188] J. Hsu, Z. Huang, A. Roth, and Z. S. Wu, "Jointly private convex programming," in *Proc. 27th Annu. ACM/SIAM Symp. Discr. Algorithms (SODA)*, Jan. 2016, pp. 580–599.

[189] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," Cryptol. ePrint Archive, Rep. 2012/144, 2012. Accessed: May 6, 2021. [Online]. Available: https://eprint.iacr.org/2012/144.pdf

[190] Y. Zheng, M. Li, W. Lou, and Y. T. Hou, "Location based handshake and private proximity test with location tags," *IEEE Trans. Depend. Secure Comput.*, vol. 14, no. 4, pp. 406–419, Jul./Aug. 2017.

[191] R. Li and A. X. Liu, "Adaptively secure conjunctive query processing over encrypted data for cloud computing," in *Proc. 33rd IEEE Int. Conf. Data Eng. (ICDE)*, San Diego, CA, USA, Apr. 2017, pp. 697–708.

[192] C. Shahabi, M. R. Kolahdouzan, and M. Sharifzadeh, "A road network embedding technique for k-nearest neighbor search in moving object databases," in *Proc. 10th ACM Int. Symp. Adv. Geograph. Inf. Syst. (GIS)*, Nov. 2002, pp. 94–100.

[193] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. 16th Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Prague, Czech Republic, vol. 99, May 1999, pp. 223–238.

[194] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *Proc. 2nd Int. Conf. Theory Cryptography (TCC)*, vol. 3378, Feb. 2005, pp. 325–341.

[195] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, Jun. 2009, pp. 169–178.

[196] R. Li, A. Liu, A. L. Wang, and B. Bruhadeshwar, "Fast range query processing with strong privacy protection for cloud computing," in *Proc. 40th Int. Conf. Very Large Date Bases (VLDB)*, Hangzhou, China, Sep. 2014, pp. 1953–1964.

[197] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in *Proc. 27th ACM Symp. Principles Distrib. Comput. (PODC)*, Vancouver, BC, Canada, Jun. 2008, pp. 95–104.

[198] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "A predictive differentially-private mechanism for mobility traces," in *Proc. 14th Privacy Enhanc. Technol. Symp. (PETS)*, Amsterdam, The Netherlands, Jul. 2014, pp. 21–41.

[199] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Constructing elastic distinguishability metrics for location," in *Proc. 15th Annu. Privacy Enhanc. Technol. Symp. (PETS)*, Philadelphia, PA, USA, Jun./Jul. 2015, pp. 156–170.

[200] S. Ma, Q. Huang, M. Zhang, and B. Yang, "Efficient public key encryption with equality test supporting flexible authorization," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 458–470, Mar. 2015.

[201] B. Lee, J. Oh, H. Yu, and J. Kim, "Protecting location privacy using location semantics," in *Proc. 17th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min. (KDD)*, San Diego, CA, USA, Aug. 2011, pp. 1289–1297.

[202] X. Wang *et al.*, "Semantic-based location recommendation with multimodal venue semantics," *IEEE Trans. Multimedia*, vol. 17, no. 3, pp. 409–419, Mar. 2015.

[203] B. Ağır, K. Huguenin, U. Hengartner, and J.-P. Hubaux, "On the privacy implications of location semantics," in *Proc. 16th Annu. Privacy Enhanc. Technol. Symp. (PETS)*, Darmstadt, Germany, Jul. 2016, pp. 165–183.

[204] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. 32nd IEEE Symp. Security Privacy (S&P)*, May 2011, pp. 247–262.

[205] S. Oya, C. Troncoso, and F. Pérez-González, "Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms," in *Proc. 24th ACM Conf. Comput. Commun. Security (CCS)*, Oct./Nov. 2017, pp. 1959–1972.

[206] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An online social network with user-defined privacy," in *Proc. ACM Conf. Appl. Technol. Architect. Protocols Comput. Commun. (SIGCOMM)*, Barcelona, Spain, Aug. 2009, pp. 135–146.

[207] R. Schlegel, C.-Y. Chow, Q. Huang, and D. S. Wong, "User-defined privacy grid system for continuous location-based services," *IEEE Trans. Mobile Comput.*, vol. 14, no. 10, pp. 2158–2172, Oct. 2015.

[208] G. Sun, Y. Xie, D. Liao, H. Yu, and V. Chang, "User-defined privacy location-sharing system in mobile online social networks," *J. Netw. Comput. Appl.*, vol. 86, pp. 34–45, May 2017.

[209] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure atrribute-based systems," in *Proc. 13th ACM Conf. Comput. Commun. Security (CCS)*, Alexandria, VA, USA, Oct. 2006, pp. 99–112.

[210] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. 28th IEEE Symp. Security Privacy (S&P)*, Berkeley, CA, USA, May 2007, pp. 1–14.

[211] Y. Chen, W. Sun, N. Zhang, Q. Zheng, W. Lou, and Y. T. Hou, "Towards efficient fine-grained access control and trustworthy data processing for remote monitoring services in IoT," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1830–1842, Jul. 2019.

[212] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Securirty Privacy*, vol. 8, no. 6, pp. 24–31, Nov./Dec. 2010.

[213] H. Yan, J. Li, J. Han, and Y. Zhang, "A novel efficient remote data possession checking protocol in cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 78–88, Jan. 2017.

[214] J. Li, H. Yan, and Y. Zhang, "Certificateless public integrity checking of group shared data on cloud storage," *IEEE Trans. Services Comput.*, vol. 14, no. 1, pp. 71–81, Jan./Feb. 2021.

[215] F. Li, H. Li, B. Niu, and J. Chen, "Privacy computing: Concept, computing framework, and future development trends," *Engineering*, vol. 5, no. 6, pp. 1179–1192, 2019.

[216] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.

[217] N. H. Tran, W. Bao, A. Zomaya, M. N. H. Nguyen, and C. S. Hong, "Federated learning over wireless networks: Optimization model design and analysis," in *Proc. 38th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr. /May 2019, pp. 1387–1395.

[218] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, May 2020.

[219] I. Damgård and Y. Ishai, "Scalable secure multiparty computation," in *Proc. 26th Annu. Int. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2006, pp. 501–520.

[220] P. Bogetoft *et al.*, "Secure multiparty computation goes live," in *Proc. 13th Int. Conf. Financial Cryptography Data Security (FC)*, Feb. 2009, pp. 325–343.

[221] X. Wang, S. Ranellucci, and J. Katz, "Global-scale secure multiparty computation," in *Proc. 24th ACM Conf. Comput. Commun. Security (CCS)*, Oct. 2017, pp. 39–56.

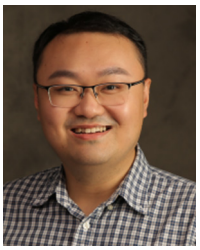
[222] J.-E. Ekberg, K. Kostiainen, and N. Asokan, "Trusted execution environments on mobile devices," in *Proc. 20th ACM Conf. Comput. Commun. Security (CCS)*, Berlin, Germany, Nov. 2013, pp. 1497–1498.

[223] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. 14th IEEE Int. Conf. Trust Security Privacy Comput. Commun. (Trustcom)*, Helsinki, Finland, Aug. 2015, pp. 57–64.

[224] J. Zhu *et al.*, "Enabling rack-scale confidential computing using heterogeneous trusted execution environment," in *Proc. 41st IEEE Symp. Security Privacy (SP)*, May 2020, pp. 1450–1465.

[225] A. Bertolino *et al.*, "A tour of secure software engineering solutions for connected vehicles," *Softw. Qual. J.*, vol. 26, no. 4, pp. 1223–1256, 2018.

[226] B. Martini *et al.*, "Pushing forward security in network slicing by leveraging continuous usage control," *IEEE Commun. Mag.*, vol. 58, no. 7, pp. 65–71, Jul. 2020.
[227] F. Martinelli, F. Mercaldo, A. Orlando, V. Nardone, A. Santone, and A. K. Sangaiah, "Human behavior characterization for driving style recognition in vehicle system," *Comput. Elect. Eng.*, vol. 83, May 2020, Art. no. 102504.
[228] C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing zero trust cloud networks with transport access control and first packet authentication," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, New York, NY, USA, Nov. 2016, pp. 5–10.
[229] D. Eidle, S. Y. Ni, C. DeCusatis, and A. Sager, "Autonomic security for zero trust networks," in *Proc. 8th IEEE Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON)*, 2017, pp. 288–293.
[230] B. Scott, "How a zero trust approach can help to secure your AWS environment," *Netw. Security*, vol. 2018, no. 3, pp. 5–8, Oct. 2018.
[231] Y. Zhao and I. Wagner, "On the strength of privacy metrics for vehicular communication," *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 390–403, Feb. 2018.
[232] A. Wasef and X. Shen, "REP: Location privacy for VANETs using random encryption periods," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 172–185, 2010.
[233] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," in *Proc. 2nd IEEE Veh. Netw. Conf.*, Dec. 2010, pp. 174–181.
[234] I. Wagner and D. Eckhoff, "Privacy assessment in vehicular networks using simulation," in *Proc. Winter Simulat. Conf.*, Dec. 2014, pp. 3155–3166.
[235] W. Ruan, M. Xu, H. Jia, Z. Wu, L. Song, and W. Han, "Privacy compliance: Can technology come to the rescue?" *IEEE Security Privacy*, vol. 19, no. 4, pp. 37–43, Jul./Aug. 2021.
[236] *General Data Protection Regulation*, Eur. Union, Brussels, Belgium, 2019. [Online]. Available: https://gdpr-info.eu
[237] M. Shi, S. Sacks and Q. Chen, and G. Webster, *Information Security Technology: Personal Information (PI) Security Specification (English Translation)*, document GB/T 35273-2020, Nat. Stand. People, China Nat. Stand. Admin. Comm., 2020. [Online]. Available: https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf



MENG LI (Member, IEEE) received the B.E. degree in information security from the Hefei University of Technology, China, in 2010, and the M.S. and Ph.D. degrees in computer science and technology from the Beijing Institute of Technology in 2013, and 2019, respectively. He is currently an Associate Professor with the School of Computer Science and Information Engineering, Hefei University of Technology. He is also a Postdoctoral Fellow of the Department of Mathematics, University of Padua, Italy, where he is with SPRITZ Research Group. He was sponsored by the ERCIM "Alain Bensoussan" Fellowship Programme in October 2019, to conduct postdoctoral research with CNR, Italy. He was sponsored by the China Scholarship Council to study in the Broadband Communications Research Lab, University of Waterloo, and Wilfrid Laurier University from September 2017 to August 2018. His research interests include security and privacy, fairness, vehicular networks, applied cryptography, edge computing, and blockchain. In this area, he published more than 30 papers in international peer-reviewed journals and conference, including IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, *ACM Transactions on Social Computing*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, *Information Sciences*, *IEEE Communications Magazine*, IEEE WIRELESS COMMUNICATIONS, MobiCom, ICICS, SecureComm, TrustCom, and IPCCC.

LIEHUANG ZHU (Member, IEEE) is a Full Professor with the School of Cyberspace Science and Technology, Beijing Institute of Technology. He is selected into the Program for New Century Excellent Talents in University from Ministry of Education, China. He has published over 60 SCI-indexed research papers in these areas, as well as a book published by Springer. His research interests include Internet of Things, cloud computing security, Internet, and mobile security. He serves on the editorial boards of three international journals, including IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He won the Best Paper Award at IEEE/ACM IWQoS 2017 and IEEE TrustCom 2018.

ZIJIAN ZHANG (Member, IEEE) received the Ph.D. degree from the School of Computer Science and Technology, Beijing Institute of Technology. He is currently a Research Fellow of the School of Computer Science, The University of Auckland. He is also with the School of Cyberspace Science and Technology, Beijing Institute of Technology. He was a Visiting Scholar with the Computer Science and Engineering Department, State University of New York at Buffalo in 2015. His research interests include design of authentication and key agreement protocol and analysis of entity behavior and preference.

CHHAGAN LAL (Member, IEEE) received the Ph.D. degree in computer science and engineering from the Malaviya National Institute of Technology, Jaipur, India, in 2014. He is currently working as a Postdoctoral Research Fellow of the Delft University of Technology, The Netherlands. Previously, he was a Postdoctoral Fellow of the Department of Mathematics, University of Padua, Italy, where he was part of the SPRITZ Research Group. He was a Postdoctoral Research Fellow of Simula Research Laboratory, Norway. His current research areas include applications of blockchain technologies, security in software-defined networking, and Internet-of-Things networks. During his Ph.D., he has been awarded with the Canadian Commonwealth Scholarship under the Canadian Commonwealth Scholarship Program to work in the University of Saskatchewan, Saskatoon, SK, Canada.

MAURO CONTI (Senior Member, IEEE) received the Ph.D. degree from the Sapienza University of Rome, Italy, in 2009. He is a Full Professor with the University of Padua, Italy. He is also affiliated with TU Delft and the University of Washington, Seattle. After his Ph.D., he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined as an Assistant Professor with the University of Padua, where he became an Associate Professor in 2015, and a Full Professor in 2018. He has been Visiting Researcher with GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of security and privacy. In this area, he published more than 400 papers in top-most international peer-reviewed journals and conferences. He has been awarded with the Marie Curie Fellowship by the European Commission in 2012, and a Fellowship by the German DAAD in 2013. He is an Area Editor-in-Chief for IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, and he has been an Associate Editor for several journals, including IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT. He was a Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and ACNS 2020, and a General Chair for SecureComm 2012, SACMAT 2013, CANS 2021, and ACNS 2022. He is Senior Member of ACM. He is a member of the Blockchain Expert Panel of the Italian Government. He is Fellow of the Young Academy of Europe.

FABIO MARTINELLI is a Senior Researcher with IIT-CNR, where he leads the cyber security project activities. He has coauthored about two hundreds scientific papers. He is also the Project Coordinator of the H2020 MSCA ITN NeCS (European Network in Cyber Security) as well as of the H2020 EU C3ISP Project. He manages Research and Development projects on information and communication security as FP6-FP7: Aniketos, Coco-Cloud, CAMINO, Connect, Contrail, SESAMO, Consequence, Sensoria, S3MS, and GridTrust. He is also the Coordinator of the EU FP7-NoE NESSoS on Engineering Secure Future Internet Services. His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He is involved in several Steering Committees of international conferences, workshops, and working groups, like the IFIP WG 11.14 on secure services and software engineering. He is also a Co-Chair of the WG3 on Secure ICT research and innovation of the European Platform on Network and Information Security a public/private cooperation promoted by the European Commission.