A Survey on Privacy-Preserving Computing in the Automotive Domain

NERGIZ YUCA, University of Passau, Germany
NIKOLAY MATYUNIN, Honda Research Institute Europe GmbH, Germany
EKTOR ARZOGLOU, Aalto University, Finland
NIKOLAOS ATHANASIOS ANAGNOSTOPOULOS, University of Passau, Germany
STEFAN KATZENBEISSER, University of Passau, Germany

As vehicles become increasingly connected and autonomous, they accumulate and manage various personal data, thereby presenting a key challenge in preserving privacy during data sharing and processing. This survey reviews applications of Secure Multi-Party Computation (MPC) and Homomorphic Encryption (HE) that address these privacy concerns in the automotive domain. First, we identify the scope of privacy-sensitive use cases for these technologies, by surveying existing works that address privacy issues in different automotive contexts, such as location-based services, mobility infrastructures, traffic management, etc. Then, we review recent works that employ MPC and HE as solutions for these use cases in detail. Our survey highlights the applicability of these privacy-preserving technologies in the automotive context, while also identifying challenges and gaps in the current research landscape. This work aims to provide a clear and comprehensive overview of this emerging field and to encourage further research in this domain.

CCS Concepts: • **Security and privacy** → *Cryptography*; **Privacy-preserving protocols**; **Domain-specific security and privacy architectures**; *Privacy protections*; • **Theory of computation** → *Cryptographic primitives*; • **General and reference** → **Surveys and overviews**.

Additional Key Words and Phrases: privacy-enhancing technologies, secure multi-party computation, homomorphic encryption, privacy-preserving machine learning, intelligent transportation system

1 INTRODUCTION

In recent years, modern automotive architectures have evolved into highly connected, software-defined systems that aggregate substantial amounts of data. This shift has been driven by advancements in Intelligent Transportation Systems (ITSs) and Software-Defined Vehicles (SDVs), which integrate connectivity and smart data processing capabilities. Autonomous driving technologies further contribute to this data collection, with vehicles equipped with numerous sensors to continuously monitor the environment and vehicular performance. It is estimated that connected autonomous vehicles alone could generate exabytes of data each month, representing a significant increase over current data volumes [111]. These advancements are further developed into concepts of fully connected vehicular networks, such as Vehicular Ad-hoc Networks (VANETs) and the Internet of Vehicles (IoV), which aim to facilitate extensive data exchange across vehicles, servers, and infrastructure, supporting services for enhanced safety, assistance, and infotainment.

However, as vehicles become more connected, they gather increasing amounts of sensitive data. The development of services that utilize this information presents a challenge in ensuring privacy during data sharing and processing. One of the primary privacy concerns centers on location data, as the collection and analysis of user locations, travel routes, and behavioral patterns may reveal sensitive information such as user interests, profiles, and habits. These challenges have led research to the application of Privacy-Enhancing Technologies (PETs) in the automotive domain.

Authors' addresses: Nergiz Yuca, nergiz.yuca@uni-passau.de, University of Passau, Faculty of Computer Science and Mathematics, Passau, Germany; Nikolay Matyunin, nikolay.matyunin@honda-ri.de, Honda Research Institute Europe GmbH, Offenbach am Main, Germany; Ektor Arzoglou, ektor.arzoglou@aalto.fi, Aalto University, School of Electrical Engineering, Espoo, Finland; Nikolaos Athanasios Anagnostopoulos, nikolaos.anagnostopoulos@uni-passau.de, University of Passau, Faculty of Computer Science and Mathematics, Passau, Germany; Stefan Katzenbeisser, stefan.katzenbeisser@uni-passau.de, University of Passau, Faculty of Computer Science and Mathematics, Passau, Germany.

In this survey, we review the application of PETs based on two key technologies of privacy-preserving computation: (1) Secure Multi-Party Computation (MPC), allowing several parties to jointly compute a function over their inputs while keeping these inputs private from each other, and (2) Homomorphic Encryption (HE), a form of encryption that allows computations to be carried out on encrypted data without requiring access to the corresponding plaintexts. Applications of MPC and HE have been studied in various domains, such as healthcare [7], blockchain [116], and deep learning [145]. However, there has been limited work to holistically survey their applications within the automotive domain. This survey aims to fill this gap by exploring the role of these technologies in enhancing privacy for automotive use cases.

While other privacy-preserving approaches such as Differential Privacy (DP) have shown promise in automotive domains such as vehicular crowdsourcing and query services in IoV, they typically achieve privacy by injecting calibrated noise into computation outputs. Zhao et al. [146] concluded that applying local DP to IoV presents several challenges. For instance, the high-dimensional nature of vehicle data makes it difficult to apply LDP, as it leads to high global query sensitivity, introduces excessive noise, and makes it challenging to preserve correlations among attributes after independent perturbation. Furthermore, the privacy-accuracy trade-off introduced by DP might be unsuitable for automotive scenarios that require privacy/accuracy results, such as the computation of ride-sharing matches or some practical ITS applications (e.g. eTolling fees) [55]. In contrast, MPC and HE allow for exact computation over sensitive data, making them particularly relevant for secure and precise processing of vehicle data. While we acknowledge that MPC and HE incur performance overhead in terms of computation and communication costs, they remain promising solutions for automotive use cases where accuracy is critical and performance requirements can be optimized through system-level design. For this reason, and given that DP has already been extensively surveyed in [84, 146], our work focuses specifically on MPC and HE approaches.

To identify the scope of scenarios suitable for applying these technologies, we first survey 230 recent papers to understand the current privacy challenges and solutions in the automotive domain and to identify specific use cases in vehicular systems where privacy is a major concern. Second, we aim for completeness of MPC/HE solutions by closely examining 62 studies that specifically apply these technologies to the identified use cases. Third, we compare these works in terms of their setups, functions, protocols used, security model, and evaluation datasets. Finally, we also document the cases in which MPC or HE is combined with other privacy-preserving technologies (e.g., Differential Privacy or Federated Learning).

Our survey reveals that privacy-preserving computing technologies are applicable in various settings within the automotive domain. However, we also note several challenges in their application, identify gaps in current research, and suggest areas where further work is needed. To the best of our knowledge, this is the first comprehensive survey that studies in detail and compares existing works applying MPC and HE to privacy-sensitive use cases specifically in the automotive domain.

We summarize the main contributions of this work as follows:

- First, we review 26 privacy-sensitive use cases across four key areas in the automotive domain: location-based services, mobility infrastructure, vehicular data analysis, and dynamic traffic management.
- Second, we conduct a comprehensive analysis of 62 state-of-the-art works that apply MPC and HE to the identified use cases, and categorize these works based on their computational setting (client-to-client, client-to-server, distributed).
- Finally, we draw conclusions about the applicability of MPC and HE in the automotive domain and identify directions for future research.

2 CRYPTOGRAPHIC BACKGROUND

In this section, we provide an overview of the cryptographic primitives, focusing on MPC and HE. We briefly introduce the fundamental principles of these technologies here and discuss in the next sections how they offer strong security guarantees to address vehicle privacy concerns.

2.1 Secure Multi-Party Computation

Secure Multi-Party Computation (MPC) is a cryptographic method that enables multiple parties to compute a function without revealing their inputs to the other parties [38]. MPC has been a widely studied topic in cryptography for more than two decades, beginning with Yao's seminal work, where he introduced the millionaire problem [126]. The problem involves two millionaires, Alice and Bob, who want to determine who is wealthier without disclosing their actual wealth. This scenario is an instance of a broader problem involving two numbers, a and b, where the objective is to establish whether the inequality $a \geq b$ is true or false without revealing the values of a and b.

A Garbled Circuit (GC) is a generic approach for secure two-party computation [127]. In this protocol, party A (the garbler) generates a garbled version of a Boolean circuit that represents the function to be computed and sends it to party B (the evaluator). B uses its inputs to evaluate the GC. To securely obtain encrypted inputs from A, B employs the Oblivious Transfer (OT) [69] protocol, where A holds two messages m_0 and m_1, and B holds a choice bit $b \in \{0, 1\}$. The protocol ensures that B learns only m_b (the message corresponding to its choice), while A learns nothing about B's choice b. The Beaver-Micali-Rogaway (BMR) [11] scheme adapts the main idea of Yao's GC to a multi-party setting, allowing each party to independently evaluate the GC.

Another fundamental primitive for MPC is Secret Sharing (SS) [15, 98]. A t-out-of-n secret sharing allows a secret to be divided into n shares, where any t or more shares can reconstruct the secret, but any fewer than t shares reveal no information about it. There are two main secret sharing schemes: (1) Additive Secret Sharing (ASS), applicable only in the specific case of $t = n$, and (2) Shamir's Secret Sharing (SSS), which is applicable to any positive $t \leq n$. Both schemes satisfy linearity, such that the sum of two secret shares is equivalent to the share of the sum.

One key sub-area of MPC emphasizes specific functionalities such as the Private Set Intersection (PSI) method [32]. It enables two parties to securely compute the intersection of their respective private datasets, such that no information beyond the common elements is disclosed to either party. Threshold PSI (TPSI) [91] is a variant of PSI that allows the parties to compute the intersection of their sets only if it exceeds a defined threshold. A Private Equality Test (PEQT) enables two parties to compare their private values to determine if they are equal without revealing any information to each other if the values are not equal [91]. Finally, a Private Information Retrieval (PIR) allows a client to obtain a specific item from a server without disclosing which item was retrieved [27].

2.2 Homomorphic Encryption

Homomorphic Encryption (HE) is a cryptographic technique that enables arithmetic operations to be performed directly on encrypted data without requiring decryption [95]. It can be categorized into four main types based on the number of operations allowed on the encrypted data: (1) Additive Homomorphic Encryption (AHE), (2) Multiplicative Homomorphic Encryption (MHE), (3) Somewhat Homomorphic Encryption (SHE), and (4) Fully Homomorphic Encryption (FHE). AHE schemes, such as the Paillier cryptosystem [87], are suitable only for specific applications where algorithms involve predominantly addition operations. AHE schemes, such as the Paillier cryptosystem [67], allow computations where the encrypted result of two ciphertexts corresponds to the sum of their original plaintexts. In contrast, MHE schemes, such as the RSA cryptosystem [68], support computations where the encrypted result corresponds to the multiplication of plaintexts,

Table 1. Overview of existing related surveys

Survey	Year	Topic of the survey	Comparison to our survey's contributions
I. Surveys on MPC and HE in non-automotive applications			
[125]	2019	Security threats and requirements for secure outsourced computation and its applications	Our work focuses on the automotive domain applications of MPC and HE, and not on generic secure outsourcing schemes only.
[145, 148]	2021, 2024	Secure Multi-Party Computation-based machine learning	Our scope includes the overall automotive domain, and we do not consider only machine-learning applications.
[1]	2018	Homomorphic Encryption Schemes	We survey MPC and HE applications in the automotive domain instead of focusing on generic HE implementations.
[64]	2023	Trusted execution environments-based secure computation protocols	Our work covers secure computing in automotive use cases using MPC and HE, and does not focus on TEE-based protocols only.
II. Surveys on privacy-preserving technologies in the automotive domain			
[102]	2020	Homomorphic Encryption applications in VANETs	We extend their focus with MPC applications and give a holistic analysis of specific automotive use cases.
[80]	2021	Security and privacy requirements, architectures, and cryptographic schemes in VANETs	MPC and HE applications in automotive use cases, which form the focus of our work, have not been covered in their survey.
[54]	2021	Privacy-preserving location-based services	Unlike their focus on privacy-preserving LBSes, our work examines MPC/HE solutions across a broader scope of automotive applications.
[42]	2022	Security and privacy issues in autonomous vehicles	Our automotive use case examination and analysis of MPC and HE are more comprehensive than their work.
[136]	2022	Solutions and future directions for carpooling in CAVs	Our survey considers various automotive use cases, and does not focus only on carpooling.
[129]	2022	Security and privacy concerns in vehicular communication systems	Our work focuses on privacy-preserving solutions for automotive applications using MPC and HE, whereas their work centers on analyzing security and privacy gaps in V2X communication standards.
[103]	2024	Cryptographic authentication techniques for secure vehicular communication	Unlike their specific focus on cryptographic authentication in vehicular communication, our work specifically addresses privacy-preserving computing in automotive use cases, emphasizing MPC and HE solutions.

although RSA without padding is not semantically secure. SHE schemes, such as the BGN cryptosystem [37], support both addition and a limited number of multiplications. Finally, FHE schemes allow an unlimited number of both addition and multiplications as well as the evaluation of arbitrary functions (such as searching, sorting, computation of max or min, etc.) over ciphertexts [1].

Both MPC and HE enable privacy-preserving computations over private data but differ in their approaches. MPC relies on distributed computation among multiple parties, which may require communication during the computation. Specifically, SS-based MPC, while promising, requires multiple parties to be online for the computation. In outsourcing MPC, clients can reduce communication overhead by distributing their data as secret shares to servers who perform computation on their behalf and are readily available. As a natural primitive for outsourcing scenarios, HE allows a data owner to outsource computation to an untrusted server, minimizing communication during the computation phase. However, HE schemes have several drawbacks. First, the computational cost is high, as many privacy-preserving computation protocols require encryption of individual bits. Second, FHE relies on a key technique called bootstrapping to periodically reduce ciphertext noise, which can drastically reduce the system's efficiency. Third, there is considerable storage overhead, as ciphertexts can be several times larger than plaintexts. Finally, a Trusted Authority may be needed to generate and distribute public and private keys for all parties [125].

3 RELATED WORK

In this section, we review surveys relevant to privacy-preserving computing in the automotive domain, with a particular focus on those addressing MPC and HE. We distinguish between works that cover these technologies in generic application domains and works that specifically focus on automotive applications. In Table 1, we further highlight distinctions between our work and existing surveys and discuss the enhancements in our survey.

Several works survey PETs in a broader, non-domain-specific context. Acar et al. [1] survey HE schemes and recent developments. Yang et al. [125] provide a technical review and comparison of secure outsourcing schemes, focusing on various secure computation methods, including MPC and HE, and conclude with an analysis of security, performance, and future directions in the field. Zhang et al. [145] and Zhou et al. [148] review the state of the art in privacy-preserving machine learning, focusing on secure multi-party computation and categorizing techniques used during the training and inference phases. Li et al. [64] give a comparison of secure computation protocols based on Trusted Execution Environments (TEEs), offering a taxonomy and assessment criteria to evaluate various protocols and highlighting their applicability to both general-purpose and specialized tasks, such as privacy-preserving machine learning and encrypted database queries.

Additionally, domain-specific surveys explore privacy risks, attacks, and other solutions in ITSs, vehicular networks, such as VANETs, and autonomous vehicles. To this end, Sun et al. [102] survey HE in VANETs, detailing the relevant framework, security issues, and data handling. Zafar et al. [136] present a comprehensive survey on carpooling in autonomous and connected vehicles, discussing the relevant architecture, components, and solutions, and addressing existing challenges in carpooling. Yoshizawa et al. [129] identify and analyze security and privacy concerns in vehicle-to-everything communication standards and provide recommendations to address these issues for the improvement of security and privacy in vehicular networks. Sudrathar et al. [103] classify and analyze various cryptographic authentication techniques for secure vehicular communication, discussing their properties, advantages, and limitations.

On the contrary, our survey focuses on the application of MPC and HE in the overall automotive domain, clearly distinguishing itself from existing surveys that either concern privacy challenges and cryptographic techniques in general or consider only a very limited area of the automotive domain. In this way, we address substantial gaps left in the current literature, particularly regarding the practical application of MPC and HE in automotive privacy scenarios, which has not so far been the central focus of another similar study. Our article highlights the role of MPC and HE in solving privacy issues in the context of connected and autonomous vehicles, providing a significant contribution to the ongoing discussion on ways of improving data privacy and security in this field.

4 METHODOLOGY

We conduct a comprehensive literature review in two steps. First, we begin by identifying existing privacy-preserving use cases in the automotive domain to understand the scope of relevant applications. We focus on selected scenarios that are identified as privacy-sensitive. Second, we specifically examine how MPC and HE are applied to privacy-sensitive use cases.

To conduct a comprehensive investigation, we employ keyword searches in the IEEE Xplore and Google Scholar databases, chosen for their broad scientific coverage. In the first step, to retrieve a relevant and exhaustive set of works, we develop two sets of keywords. The first set includes domain-specific keywords, while the second set includes privacy-related keywords that indicate relevance to privacy concerns or solutions. A complete list of the keywords used is provided in Table 2. We generate all possible combinations of domain- and privacy-related keywords and construct search queries by combining them with logical operators. Specifically, we use the `OR` operator within each set of keywords to include synonyms and related terms, and the `AND` operator between the domain and privacy keyword sets to ensure that the results are relevant to both areas. The queries are constructed in the form of: `(“domain keyword” OR “domain synonym”) AND (“privacy keyword” OR “privacy synonym”)`. For example, a search query would be `(“Vehicle” OR “Car”) AND (“Privacy-preserving” OR “Data privacy”)`. Due to the potential overlap with papers on Model Predictive Control, we avoided the acronym “MPC” and used the explicit term “Secure Multiparty Computation” or “Secure Multi-Party Computation” in our search.

Table 2. Keywords Used in Literature Search

Domain Keywords	Privacy Keywords
vehicle, car, VANETs, location-based services, autonomous vehicles, connected cars, intelligent transportation, vehicular networks, mobility, traffic management, vehicular data analysis	privacy-preserving, privacy-sensitive, secure multi-party computation, homomorphic encryption, data privacy, privacy protection, secure computation, cryptographic protocols, privacy-enhancing technologies, secret sharing, garbled circuits, oblivious transfer, private set intersection

Our aim is to collect research works that address selected scenarios in the automotive domain as privacy-sensitive. In this approach, we thus do not expect the complete coverage of all possible automotive use cases, and to not aim to discover *new* privacy-sensitive use cases, but rather scope existing use cases and determine if the surveyed technologies address them or leave gaps.

As a result of the first step, we identified a total of 243 papers. Subsequently, we refined this pool by selecting only publications written in English, published within the last five years, and with a citation count of at least ten. In addition, we filtered out irrelevant work, e.g., papers focused on security rather than on privacy. We also excluded papers that address privacy in communication protocols (e.g., specific authentication schemes in VANETs). Finally, we excluded 48 papers where the applied methods were unclear or lacked substantial details. Recognizing the potential existence of recent relevant works that may not fully meet the aforementioned criteria but still be important (e.g., very recent works with only a few citations), we conduct an additional screening of the works in the original pool of papers. This results in the inclusion of 16 more papers with direct relevance to the scope of our survey, despite not initially meeting the set criteria. As a result, our final analysis dataset consists of 230 papers, selected through criteria-based filtering and our targeted search.

In the second step, for the detailed analysis in Section 6, we filter the collected papers to select works that apply MPC or HE as a privacy-preserving solution. To ensure comprehensive coverage, we perform an additional verification step by conducting targeted searches combining each reviewed use case (Section 5) with MPC and HE technologies. These searches use queries in the form of: `(“Use Case Name”) AND (“Technology Name”)`. The final dataset consists of 62 papers.

5 USE CASES

In this section, we present a set of use cases in the automotive domain based on the first step of our literature review. Each use case illustrates specific scenarios that involve the processing, analysis, or sharing of privacy-sensitive data among multiple parties. We cluster use cases into four categories: location-based services, mobility infrastructures, vehicular data analysis, and dynamic traffic management and V2X communication. While we identify specific groups for different use cases, it is important to note that there are natural overlaps among them. For example, traffic signal control use case (Section 5.4.5) can be classified to vehicular data analysis and traffic management groups. However, we categorize it under traffic management because its primary focus is on optimizing road traffic flow. Later in Section 6, we analyze in detail the concrete applications of MPC and HE in these use cases.

5.1 Privacy in Location-Based Services

In this section, we discuss privacy concerns associated with Location-Based Services (LBSs). LBSs include various services that utilize the geographic location of a user as input to specific functions, such as recommending nearby points of interest, or connecting users to the taxi drivers. Service providers, typically centralized, require users to disclose their location to access the desired services. This centralization leaves users unable to verify whether their data is being used as intended, and poses risks of tracking and profiling. Therefore, finding a way to offer users personalized LBSs

without compromising their location is an essential concern. Below, we summarize concrete use cases representing LBSs with works addressing privacy issues in these use cases.

5.1.1 Points of Interest. Points of Interest (POI) are specific locations that are beneficial for drivers, such as restaurants, gas stations, and landmarks. Vehicles often request these locations to improve navigation and provide access to nearby amenities. In this scenario, vehicles query for POIs by sending requests to a server. The server processes these queries and returns relevant information without determining the exact locations of the vehicles [107, 147].

5.1.2 Navigation and Route Planning. One of the prominent services in vehicular networks is providing drivers with optimal routes and real-time navigation assistance based on traffic conditions and data collected from other vehicles. This service requires users to share their current location, travel routes, and destinations, which might be exploited for user movement profiling [108, 149].

5.1.3 Localization. Vehicle localization is the process of precisely determining a vehicle's location, speed, and direction using GPS, sensors, maps, and communication systems. Constant data collection and transmission may expose vehicle location history, travel patterns, and sensitive user information, highlighting the need for privacy-preserving measures [53, 115].

5.1.4 Vehicular Crowdsourcing. This use case involves outsourcing tasks related to specific locations to a group of mobile workers. Task requesters register through a centralized server and publish tasks with target locations or spatial routes. Available workers are considered for task assignment and are responsible for reporting their locations to the server [93, 124, 142].

5.1.5 Ride-Sharing. Ride-sharing services match drivers with passengers in order to share a journey. To facilitate this coordination, ride-sharing systems collect vast amounts of sensitive data, including pick-up and drop-off locations, the identities of riders and drivers, and specific timings. Therefore, the server or any entity accessing this data can infer sensitive information about riders' activities by monitoring their locations [4, 5, 41, 43, 74, 75, 86, 90, 131, 133].

5.1.6 Vehicle Sharing. Vehicle sharing is a smart mobility service that provides users with access to vehicles for short-term use, often on an as-needed basis. It utilizes in-vehicle telematics and portable devices, such as smartphones, and allows vehicle owners to distribute temporary digital keys or access tokens to other users, enabling them to access the vehicle [104, 105].

5.2 Privacy in Mobility Infrastructure

In this section, we discuss the privacy use cases associated with mobility infrastructure. This category focuses on services where vehicles interact with physical infrastructure, such as toll stations or charging stations. The primary privacy risks stem from the sharing of vehicle and user data with centralized systems or third-party infrastructure providers.

5.2.1 Toll Data Collection. Electronic toll collection systems use sensors and toll transponders to track vehicles. Information stored in toll records can be utilized to monitor a vehicle's movements, making vulnerable to unauthorized tracking and user profile breaches [56].

5.2.2 Electric Vehicle (EV) Charging. The EV charging process involves various interactions between users and charging infrastructure. In the payment process, EV users engage in transactions with Charging Service Providers (CSP). The chosen Charge Station (CP) generates a service order including payment amount, charging duration, and location, which the user typically authorizes through a a mobile application. After the payment, the charging session begins. CPs can aggregate data from these transactions, including geographic location, charging patterns, and battery usage [34]. Over time, this accumulated data may enable the inference of users' driving behaviors and

frequently visited locations [117]. EV charging can also be optimized to fill the overnight demand valley, reducing grid operation costs. However, in this process, participants need to communicate frequently, thereby revealing an EV owner's charging profiles [52].

5.2.3 Parking. An autonomous vehicle parking system integrates service providers, parking infrastructure, users, vehicles, and authorities. It relies on secure registration and communication protocols, encrypted data handling, and user authentication mechanisms. Protecting user location and identity data is important in parking systems, as registration with central authorities for reservations can expose sensitive information and compromise privacy [67, 92, 150].

5.3 Privacy in Vehicular Data Analysis

In this section, we discuss use cases that target privacy aspects related to analysis of vehicular data. As the SDVs continue to advance, organizations and institutions are increasingly interested in gathering vehicle data of various kinds for analysis purposes. Substantial amounts of personal data collected and processed by service providers can pose serious privacy risks. Research works address these concerns by proposing privacy-preserving solutions for data aggregation (5.3.1), or architectures for privacy-preserving federated learning (5.3.2). Vehicular data analysis often includes learning models of vehicle or driver behavior (5.3.3–5.3.6). These use cases rely on sensitive data streams (e.g., driving patterns, locations, images) for training accurate models. A primary privacy concern is protecting this data from misuse and profiling. Another class of applications (5.3.7–5.3.10) involves learning from the vehicles' *external* environment. These applications often require collaborative sharing of sensitive data, which introduces distinct privacy challenges. In the following, we discuss concrete use cases for vehicular data collection and analysis.

5.3.1 Data Processing in IoV. Several works address the generic use case of aggregating data in IoV environments. Each vehicle node provides data, partially aggregated by Roadside Units (RSUs) and then fully aggregated by a central server. The privacy of vehicle data needs to be protected from being misused by RSUs and the server [21]. Decentralized VANETs are designed to reduce centralization and minimize network communication overhead by involving vehicles, RSUs, and edge nodes to aggregate or even process data. For example, vehicles and RSUs can share real-time traffic condition information, while edge nodes train machine learning models and distribute results. In these multi-party setups, privacy has to be taken into account in all existing data flows [22].

5.3.2 Federated Learning (FL). Several works address a generic scenario of training machine learning models on vehicular data using Federated Learning (FL) [23, 49]. Although FL allows clients to avoid sharing raw data, a malicious server can still reveal sensitive information from the model updates. Addressing the trust concerns associated with a central aggregator, Decentralized Federated Learning (DFL) has been increasingly applied in the vehicular domain. It enables participants to share model updates directly among themselves or with intermediate edge nodes [13, 48, 49, 65].

5.3.3 Training Driving Assistance Systems. This use case involves training models for Advanced Driving Assistance Systems (ADAS). Particularly, lane-keeping systems are trained on driving patterns combined with image data, to predict optimal steering angles. The collected training data can expose sensitive information such as locations and driving patterns [96], [89].

5.3.4 Detecting Misbehavior in VANETs. Misbehavior detection systems aim to identify malicious data sharing in vehicular networks. They analyze reported data, such as location and traffic details, sometimes combined with trust scores or feedback, to model and identify anomalies [40, 99, 109].

5.3.5 Traffic Anomaly Detection. This use case involves monitoring the behavior of surrounding vehicles, e.g., to identify unsafe or malicious driving. An example is detecting stalking vehicles,

which follow a vehicle for a long duration through various turns and speed changes. This is achieved using sensor data, such as cameras and IMU sensors, to track proximity and movements [101].

5.3.6 Predictive Maintenance. Data from vehicle sensors and historical repair records can be analyzed to model and predict potential breakdowns and schedule timely maintenance. This approach aims to minimize unexpected vehicle failures and extend vehicle lifespan [60].

5.3.7 FL-based Navigation. A concrete use case of DFL in vehicular networks is collaborative learning a navigation model, studied by Kong et al. [61]. In scenarios where GPS signals are weak, such as in urban centers or tunnels, vehicles can maintain accurate localization by combining high-sampling Inertial Measurement Unit (IMU) data and low-sampling GPS data. This process risks exposing sensitive navigation information during the exchange of FL model updates [61].

5.3.8 Object Classification in CAVs. CAVs use cameras to capture images of their surroundings, which aids in tasks such as obstacle avoidance and enhancing situational awareness. However, these images may contain a vast amount of sensitive information, including faces, license plates, or locations related to the vehicle's environment [118–121].

5.3.9 Road Profile Estimation. In this setting, multiple vehicles work together to accurately assess road conditions and identify surface anomalies like potholes. Instead of relying on data from a single vehicle, which can be affected by sensor limitations, the collaborative approach allows vehicles on the same road segment to share and combine their data [36].

5.3.10 Vehicle Emission Control. Utilizing traffic light cycle data shared with other vehicles can help reduce vehicle emissions at intersections. A reinforcement learning model processes this data to help vehicles optimize their speed for lower emissions. Achieving this requires the collection, sharing, and analysis of privacy-sensitive vehicle data, such as speed, location, and traffic conditions [9].

5.4 Privacy in Dynamic Traffic Management and V2X Communication.

This section discusses privacy-sensitive traffic management scenarios involving real-time vehicular data exchange between vehicles (V2V) or between vehicles and infrastructure (V2X). The primary privacy risks come from constantly sharing sensitive vehicle data during these interactions. Compared to use cases within the Mobility infrastructure (Section 5.2) that involve more static exchanges, in this group, we focus on dynamic, real-time communication.

5.4.1 Message Transmission. Message exchanges in VANETs enable vehicles and pedestrians to communicate with each other directly (V2V) and with infrastructure such as RSUs. Although increased connectivity and information flow benefit transportation systems, they also introduce privacy risks by tracking and revealing personal patterns and locations [76].

5.4.2 Driver Profile Matching. A concrete use case in V2V exchange includes driver profile matching, which allows drivers to recognize and connect with others based on shared characteristics such as destinations, interests, or travel routes. For example, this process allows people to add each other as friends and share information based on similar interests [114].

5.4.3 Energy Storage Sharing. This use case allows multiple users to access and benefit from shared energy storage systems, either through community sharing, outsourcing to third-party energy storage operators, or peer-to-peer sharing. This approach improves cost-effectiveness by distributing the storage capacity and associated costs among users. This process can involve the disclosure of energy consumption data, users' daily routines, or working patterns [113].

Table 3. Overview of specific use cases with relevant privacy concerns.

Use Case	Privacy Concern	Use of MPC	Use of HE
Location-Based Services			
Points of Interest (5.1.1)	Location data	✔	✗
Navigation and Route Planning (5.1.2)	Location and trajectory data	✔	✗
Localization (5.1.3)	Location data	✔	✗
Vehicular Crowdsourcing (5.1.4)	Worker's and task requester's location	✔	✔
Ride-Sharing (5.1.5)	Pick-up and drop-off locations and driving patterns	✔	✔
Vehicle Sharing (5.1.6)	Booking, transaction, and location data	✔	✗
Mobility Infrastructure			
Toll Data Collection (5.2.1)	Location data and driving patterns	✗	✔
Electric Vehicle (EV) Charging (5.2.2)	Charging location, energy consumption patterns	✔	✗
Parking (5.2.3)	Location and identity data	✔	✔
Vehicular Data Analysis			
Data Processing in IoV (5.3.1)	Data leakage during training process	✔	✔
Federated Learning (FL) (5.3.2)	Data leakage from model updates	✔	✔
Training Driving Assistants (5.3.3)	Driving patterns, location and user's identity data	✗	✗
Detecting Misbehavior in VANETs (5.3.4)	Location exposure, driving patterns	✗	✔
Traffic Anomaly Detection (5.3.5)	Location data and driving patterns	✗	✗
Predictive Maintenance (5.3.6)	Location and identity data	✗	✔
FL-based Navigation (5.3.7)	Privacy disclosure during navigation updates	✗	✔
Object Classification in CAVs (5.3.8)	Image data leakage	✔	✗
Road Profile Estimation (5.3.9)	Vehicle's sensitive information	✗	✗
Vehicle Emission Control (5.3.10)	Location and speed data	✗	✗
Traffic Management			
Message Transmission (5.4.1)	Location and trajectory data	✗	✔
Driver Profile Matching (5.4.2)	Personal data based on interests or destination	✔	✗
Energy Storage Sharing (5.4.3)	Energy consumption and travel patterns	✗	✗
Speed Advisory (5.4.4)	Vehicle speed and arrival time	✔	✗
Traffic Signal Control (5.4.5)	Location data	✔	✗
Platooning (5.4.6)	Location and travel route information	✗	✔
Traffic Monitoring (5.4.7)	Location data and travel patterns	✗	✔

5.4.4 Speed Advisory. The aim of Consensus-Based Speed Advisory Systems (CSAS) is to provide real-time, privacy-preserving speed recommendations for groups of vehicles, with a focus on reducing emissions and enhancing energy efficiency. They require collecting sensitive data, such as vehicle type, fuel consumption, and driver's arrival time while optimizing consensus speed [71].

5.4.5 Traffic Signal Control. In traditional intelligent traffic signal control systems, users' vehicle information, such as location and speed, is transmitted to RSUs to improve service efficiency. Servers collect this data to train machine learning models, which automate the formulation of traffic signal control strategies, optimizing road traffic management. The transmission of this vehicle information can result in privacy breaches, disclosing sensitive user details [128].

5.4.6 Platooning. Platooning is a fuel-efficient transportation method where multiple vehicles, typically trucks, follow each other in proximity on highways, for enhanced privacy and increased road capacity. Forming a platoon typically requires the disclosure of sensitive information, such as the real-time geographic position and intended routes of participating vehicles [24, 63, 94, 139].

5.4.7 Traffic Monitoring. Crowdsourcing-based traffic flow statistics can optimize traffic light scheduling and mitigate congestion. Gathering drivers' directional intentions via RSUs and Traffic Management Centers (TMC) may expose sensitive information [137].

5.5 Summary

In this section, we briefly reviewed a variety of privacy-sensitive use cases within the automotive domain, grouped into four subdomains, and listed in Table 3. Our review shows many cases where privacy-sensitive data is exchanged between multiple parties, such as drivers, data requesters, infrastructure providers, and service providers. This highlights the relevance of exploring privacy-preserving computing technologies, such as MPC and HE, in these multi-party environments.

6 APPLICATIONS OF PRIVACY-PRESERVING COMPUTING

In this section, we examine privacy-preserving computing applications (concerning either MPC or HE) in the automotive domain proposed in the literature more closely.

6.1 Overview

To achieve a comprehensive overview, we categorize the surveyed works into three application settings based on similar architectural setups and requirements for applying MPC or HE. The three primary settings we focus on are: a *client-to-client setting*, which involves direct data exchange between clients, such as vehicles or drivers, without intermediary infrastructure; a *client-to-server* setting, where clients transfer data to one or more central server(s), for processing and/or storage; and finally, a *distributed setting*, which leverages a network of servers and edge nodes to handle computational tasks closer to data sources in a decentralized way. Following the structure of Section 5, we then group surveyed works within each setting by their application domains: location-based services, mobility infrastructures, vehicular data analysis, and dynamic traffic management, to show how different settings are observed in each use case group.

An overview of the surveyed works can be found in Table 4. The first column lists the publications and the names of the authors. The second and third columns indicate the specific addressed use case and its application domain, respectively. The fourth column details the protocols used in the implementation of the works. The fifth column indicates the security model considered in the publication: semi-honest and malicious. In the semi-honest security model, it is assumed that the participants follow the prescribed protocol but may be curious to derive additional information from the process. On the contrary, in the malicious security model, participants are assumed to actively attempt to undermine the protocol by modifying inputs or deviating from the protocol.

In addition, we observe that many implementations of MPC and HE serve two primary purposes in reviewed works. First, numerous works employ MPC or HE to perform privacy-preserving aggregation, computing an aggregate (e.g., a sum) of data collected from multiple sources. These functions are used in various use cases, such as aggregating model updates in federated learning, predictive maintenance, etc. Second, several works employ MPC or HE to implement matching functionality. In these works, the technologies are used to identify pairs or subsets of data entries that meet specific criteria without revealing privacy-sensitive information. They are widely used in contexts such as ride-sharing services and task allocation in spatial crowdsourcing. The remaining works implement customized functionalities that do not fall under aggregation or matching. Examples of custom functions include training machine learning models [22], performing joined decision-making [128], and optimization [71]. We list these three categories in the sixth column.

The seventh column shows whether HE and MPC are combined with technologies such as Blockchain, Differential Privacy, Federated Learning, and Machine Learning. Finally, the last column indicates whether real-world data or simulated data was used in the papers.

6.2 Client-to-Client Setting

In this section, we discuss how MPC and HE, help to solve privacy issues in various client-to-client settings, where clients (e.g., vehicle drivers) directly interact with each other to share or exchange sensitive data, such as locations or travel paths. This approach eliminates the need for a server or centralized infrastructure to process, store, or transmit data, reducing the privacy risks associated with centralized systems. In this setting, privacy risks mainly involve the potential exposure or misuse of sensitive data by malicious clients. To counter these risks, clients use MPC and HE to jointly process the data without revealing sensitive information to each other. Here, clients typically

Table 4. Overview of works that employ MPC and HE in the automotive domain.

Reference & Authors	Use Case	Domain	Protocols	Security Model	Function	Integrated Tech.	Data
Client-to-Client Setting							
[53] Hussain and Koushanfar	Localization (5.1.3)	LBS	BMR (mp), GC(2p)	◑	Custom	-	▶
[4] Aïvodji et al.	Ride-Sharing (5.1.5)	LBS	PSI (2p)	◑	Matching	-	⛁
[41] Hallgren et al.	Ride-Sharing (5.1.5)	LBS	TPSI (2p)	◑	Matching	-	⛁
[86] Pagnin et al.	Ride-Sharing (5.1.5)	LBS	AHE, PSI (2p)	◑	Matching	-	⛁
[52] Huo et al.	EV Charging (5.2.2)	MI	SSS (mp)	◑	Aggregation	-	▶
[23] Chen et al.	Federated Learning (5.3.2)	VDA	PVSS (mp)	●	Aggregation	FL	⛁
[114] Wang et al.	Driver Profile Matching (5.4.2)	DTM	OT, PSI (2p)	◑	Matching	-	🗎
[76] Magaia et al.	Message Transmission (5.4.1)	DTM	AHE	●	Matching	-	⛁ ▶
Client-to-Server Setting							
[88] Peng et al.	Vehicular Crowdsourcing (5.1.4)	LBS	ASS (mp)	◑	Aggregation	-	⛁
[59] Kong et al.	Vehicular Crowdsourcing (5.1.4)	LBS	AHE	◑	Custom	-	▶
[107] Tan et al.	Points of Interest (5.1.1)	LBS	PIR (mp)	◑	Matching	-	⛁
[147] Zhou et al.	Points of Interest (5.1.1)	LBS	OT (2p), PIR (2p)	◑	Custom	-	⛁
[143] Zhang et al.	Points of Interest (5.1.1)	LBS	PSI (2p)	◑	Matching	DP	▶
[90] Pham et al.	Ride-Sharing (5.1.5)	LBS	SHE	◑	Matching	-	⛁
[5] Aïvodji et al.	Ride-Sharing (5.1.5)	LBS	SHE, PEQT, SS	◑	Matching	-	⛁
[43] He et al.	Ride-Sharing (5.1.5)	LBS	AHE	◑	Matching	-	⛁
[51, 75] Luo et al., Huang et al.	Ride-Sharing (5.1.5)	LBS	AHE, GC (2p), SHE	◑	Matching	-	⛁
[132] Yu et al.	Ride-Sharing (5.1.5)	LBS	AHE	◑	Matching	-	⛁
[133] Yu et al.	Ride-Sharing (5.1.5)	LBS	SHE	◑	Matching	-	⛁
[131] Yu et al.	Ride-Sharing (5.1.5)	LBS	AHE, GC (2p)	◑	Matching	-	⛁
[130] Yu et al.	Ride-Sharing (5.1.5)	LBS	SHE	◑	Matching	-	⛁
[123] Xu et al.	Ride-Sharing (5.1.5)	LBS	GM	◑	Matching	-	▶
[141] Zhang et al.	Ride-Sharing (5.1.5)	LBS	PSI (2p)	●	Matching	-	▶
[74] Luo et al.	Ride-Sharing (5.1.5)	LBS	PEQT (2p)	◑	Matching	-	⛁
[57] Karmakar et al.	Ride-Sharing (5.1.5)	LBS	FSS (3p)	◑	Matching	-	▶
[21] Zhou et al.	Data Processing in IoV (5.3.1)	VDA	ASS (mp)	●	Aggregation	-	▶
[71] Liu et al.	Speed Advisory (5.4.4)	DTM	SS (mp)	◑	Custom	-	▶
[50] Liang et al.	Message Transmission (5.4.1)	DTM	OT (2p)	●	Custom	-	▶
[137] Zhang et al.	Traffic Monitoring (5.4.7)	DTM	BGN	◑	Aggregation	DP	▶
[94] Quero et al.	Platooning (5.4.6)	DTM	CKKS	◑	Matching	-	▶
[139] Zhang et al.	Platooning (5.4.6)	DTM	AHE	●	Aggregation	-	▶
[24] Cheng et al.	Platooning (5.4.6)	DTM	AHE	●	Aggregation	-	▶
Distributed Setting							
[142] Zhang et al.	Vehicular Crowdsourcing (5.1.4)	LBS	AHE, OPE	●	Matching	BC	⛁
[124] Xu et al.	Vehicular Crowdsourcing (5.1.4)	LBS	OT, PEQT (2p)	◑	Matching	-	▶
[25] Cheng et al.	Vehicular Crowdsourcing (5.1.4)	LBS	AHE	◑	Matching	-	▶
[39] Guan et al.	Vehicular Crowdsourcing (5.1.4)	LBS	SHE	◑	Custom	-	⛁
[134] Yu et al.	Vehicular Crowdsourcing (5.1.4)	LBS	SSS (mp)	◑	Custom	-	▶
[149] Zhou et al.	Navigation and Route Planning (5.1.2)	LBS	MPDC	◑	Custom	-	▶
[108] Tiausas et al.	Navigation and Route Planning (5.1.2)	LBS	PIR (mp)	◑	Custom	-	▶
[104, 105] Symeonidis et al.	Vehicle Sharing (5.1.6)	LBS	SSS (mp)	◑	Custom	-	⛁
[56] Karim and Rawat	Toll Data Collection (5.2.1)	MI	FHE	◑	Custom	BC	⛁
[138] Zhang et al.	Parking Systems (5.2.3)	MI	AHE	◑	Custom	BC	⛁
[67] Li et al.	Parking Systems (5.2.3)	MI	AHE, PSI (2p)	◑	Matching	-	▶
[6] Amiri et al.	Parking Systems (5.2.3)	MI	PIR (mp)	●	Custom	BC	▶
[22] Chen et al.	Data Processing in IoV (5.3.1)	VDA	FHE	●	Custom	BC, DL	▶
[70] Liu et al.	Data Processing in IoV (5.3.1)	VDA	SSS (mp)	◑	Aggregation	-	▶
[65] Li et al.	Federated Learning (5.3.2)	VDA	SSS (mp)	◑	Aggregation	FL, DP	▶
[49] Hu et al.	Federated Learning (5.3.2)	VDA	SSS (mp), CKKS	◑	Aggregation	BC, FL	▶
[66] Li et al.	Federated Learning (5.3.2)	VDA	DGHV	●	Aggregation	BC, FL	⛁
[61] Kong et al.	FL-based Navigation (5.3.7)	VDA	SSS (mp), AHE	●	Aggregation	FL, DP	▶
[118, 119] Xiong et al.	Object Classification in CAVs (5.3.8)	VDA	ASS (mp)	◑	Custom	DL	⛁
[14] Bi et al.	Object Detection in CAVs (5.3.8)	VDA	ASS (mp)	◑	Custom	DL	⛁
[60] Kong et al.	Predictive Maintenance (5.3.6)	VDA	AHE	◑	Aggregation	DP	🗎
[40] Gyawali et al.	Det. Misbehavior in VANETs (5.3.4)	VDA	AHE	●	Aggregation	DL	▶
[113] Wang et al.	Energy Storage Sharing (5.4.3)	DTM	SSS (mp)	●	Aggregation	BC	▶
[128] Ying et al.	Traffic Signal Control (5.4.5)	DTM	ASS (2p)	◑	Custom	DL	▶
[2] Adelipour et al.	Traffic Signal Control (5.4.5)	DTM	ASS (mp)	◑	Custom	-	▶

Application Domains: **LBS** — Location-Based Services. **MI** — Mobility Infrastructures. **VDA** — Vehicular Data Analysis. **DTM** — Dynamic Traffic Management and V2X Communications. **Protocols:** **ASS** — Additive Secret Sharing. **BGN** — Boneh, Goh, and Nissim cryptosystem. **BMR** — Beaver-Micali-Rogaway protocol. **DGHV**— Dijk-Gentry-Halevi-Vaikutanathan Algorithm. **CKKS**— Cheon-Kim-Kim-Song Algorithm. **FHE** — Fully Homomorphic Encryption. **GC** — Garbled Circuit. **OPE** — Order Preserving Encryption. **OPRF** — Oblivious Pseudorandom Function. **OT** — Oblivious Transfer. **AHE** — Additive Homomorphic Encryption (Paillier cryptosystem). **PEQT** — Private Equality Test. **PSI** — Private Set Intersection. **TPSI** — Threshold Private Set Intersection. **PIR** — Private Information Retrieval. **PVSS** — Publicly Verifiable Secret Sharing. **SHE** — Somewhat Homomorphic Encryption. **GM** — Goldwasser–Micali Algorithm. **SSS** — Shamir's Secret Sharing. **FSS** — Function Secret Sharing. **MPDC** — Multiparty Delegated Computation. **Number of parties in MPC protocols:** **2p** — Two-Party. **mp** — Multi-Party (three or more parties). **Security Model:** ◑ — semi-honest. ● — malicious. **Integrated Technology:** BC — Blockchain. **DL** — Deep Learning. **DP** — Differential Privacy. **FL** — Federated Learning. **Evaluation:** ⛁ — Real-world data. ▶ — Simulated data. 🗎 — Theoretical work.

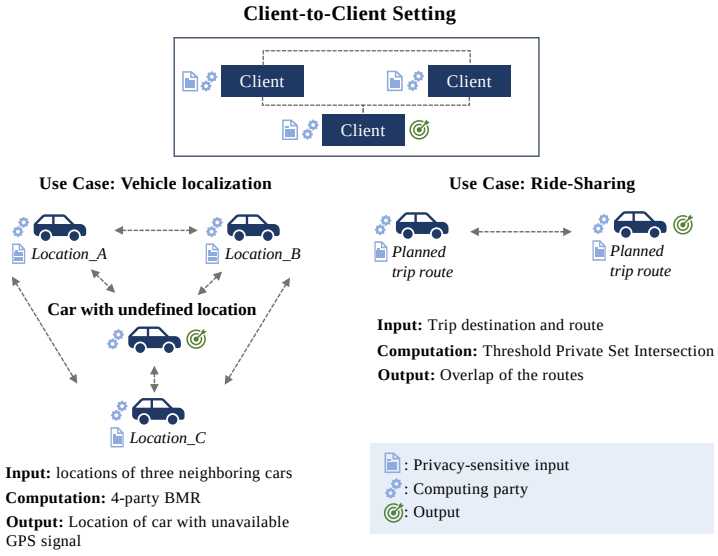

Fig. 1. Generic client-to-client setting, with two specific example use cases under the same setting. In this setting, clients typically act as computing parties on their own inputs, with output used by all or some clients.

act as both data providers and computing parties, performing computations on their own inputs. The result of the computation can be used by all or specific parties, depending on the use case.

Figure 1 demonstrates the client-to-client setting with two specific use cases. In the first example, localization [53], a car performs secure 4-party computation with three neighboring cars to compute its location (the output) based on the locations of the neighboring cars (the inputs). The MPC allows vehicles to not reveal their actual locations to each other. The second example shows the use of ride-sharing. Here, two drivers compute on their planned routes using PSI protocol, allowing them to identify potential overlaps without disclosing the full routes. These examples show how different implementations of the client-to-client setting follow a similar pattern where multiple clients interact as computing parties on their own inputs. Below, we survey existing works in detail.

6.2.1 Privacy in Location-Based Services. Client-to-client interactions in LBSs involve clients sharing sensitive location data directly with each other to enable services such as localization and ride-sharing, which may compromise privacy. Addressing this concern in localization, Hussain and Koushanfar [53] proposed a method where a lost car can compute its location with the help of three nearby cars while ensuring that the locations of all participating vehicles remain private. The method enables cars to communicate directly to locate a lost vehicle, computing their mutual geometric intersections for positioning. This work is one of the few examples of using GC in the automotive domain, presenting two alternatives: one using a two-party GC protocol and another using a multi-party BMR protocol. Although the BMR protocol extends GC to support multiple parties and enhances privacy, it introduces higher computational complexity. More precisely, the GC-based protocol runs in 0.35s (~1MB of data sent), while the BMR takes 2.65s due to the use of a combined circuit (TriLoc), which integrates three instances of sub-circuits that securely compute pairwise circle intersections (Intersection) and verify whether each point lies within a third car's range (Range), along with additional logic to select intersection points.

Another group of works focuses on implementing ride-sharing scenarios, which often involve a centralized server to coordinate routes, as seen in Table 4. In particular, Aïvodji et al. [4] propose a

PSI-based decentralized ride-sharing architecture, where a driver and a rider want to determine a pick-up and drop-off location without disclosing their origin and destination locations to each other or any third party. After clients encrypt their location using HE, they utilize PSI to compare them and find the common ride-sharing locations. Even though the PSI method is secure, a semi-honest adversary might infer information based on the size of the encrypted data. To address this, the authors propose to fix the size of the isochrone (a geographical boundary showing areas reachable within a certain time) for both clients to ensure indistinguishability.

Hallgren et al. [41] consider the abstract model of two parties exchanging location data in ride-sharing. They introduce PrivatePool, supporting two ride-sharing approaches. The first, proximity-based method, leverages HE to allow users to determine if starting and ending points are within a certain range, without revealing locations. The second, intersection-based approach, employs a TPSI protocol to identify overlaps in ride trajectories. Finally, Pagnin et al. [86] further develop this concept with TOPPool, that extends the PrivatePool [41] and enhances privacy-preserving ride-sharing with time-aware optimizations and the ability to handle partial schedule overlaps. Unlike PrivatePool, TOPPool employs regular PSI to perform more efficient intersection-based matching between trips represented as sets of consecutive points and AHE for ride endpoint-based matching. Due to space constraints, we omit performance descriptions for ride-sharing papers here and in Section 6.3.1, and instead provide a performance comparison in Section 7.2.

6.2.2 Privacy in Mobility Infrastructures. Although typically mobility infrastructure services involve a centralized server, there are scenarios where data exchange occurs directly between vehicles. A relevant example that utilizes MPC is EV charging control, where EVs coordinate charging without relying on a centralized charging station to manage the process. To develop a privacy-preserving EV charging control using SSS, Huo and Liu [52] adjust the charging of all EVs so that they are all charged as required by the end of the night without surpassing their maximum charging rates. In their work, the charging profile of each EV is considered the secret and is transformed into an integer before being shared. Each EV constructs a polynomial of degree k with secret as the constant term and random coefficients, then evaluates the polynomial at predefined points and shares the results with other EVs. Using these shared evaluations, the EVs can securely reconstruct the aggregate sum of the charging profiles without revealing individual profiles. Additionally, collusion among semi-honest EVs requires at least k EV's to collaborate to infer another EV's secret.

6.2.3 Privacy in Vehicular Data Analysis. Decentralized Federated Learning (DFL) is increasingly used in the automotive sector during vehicle data analysis without relying on a centralized server [13]. V2X communication, with its vehicle mobility and limited storage capacity of nodes, benefits from DFL, as it allows direct client-to-client interactions for training collaborative models. The direct exchange of gradients between clients can potentially reveal sensitive information about training data. Addressing data leakage in autonomous vehicles during the training process, Chen et al. [23] introduce a novel Byzantine-fault-tolerant decentralized FL method based on a peer-to-peer network, using a PVSS [97] scheme, which enables anyone (not just the participant) to confirm the accuracy of encrypted shares. In their method, each autonomous vehicle uses PVSS to protect its data. If a share is identified as false, the responsible participant is considered malicious and will be excluded from participating in the next communication round. Experiments show that the PVSS protocol runs in ~5.2s with 512 autonomous vehicles, with secret share distribution taking ~0.97s.

6.2.4 Privacy in Dynamic Traffic Management and V2X Communications. We observe two works leveraging privacy-preserving computing technologies within the context of vehicle-to-vehicle (V2V) communication to improve traffic management . First, to address privacy concerns in driver profile matching, where users in vehicular social networks share information based on similar

characteristics, Wang et al. [114] propose solutions based on OT and PSI. The characteristics include upcoming destinations, tourist spots, the work sector, favorite sports, preferred movies, music preferences, etc. The authors use an OT protocol to design a PSI protocol with equality tests. These protocols allow two parties in a VANET to identify similar characteristics in their sets without revealing any additional information beyond the intersection.

Second, Magaia et al. [76] focus on enhancing message delivery in vehicular delay-tolerant networks. The authors introduce a routing protocol called ePRIVO, based on AHE. It solves the problem of dynamically selecting the optimal vehicle for message forwarding. When two vehicles meet, they use the protocol to compare their routing metrics (such es ego betweenness centrality and similarity) to determine which vehicle is a better candidate for message forwarding, without exchanging privacy-sensitive metrics directly. Encryption and decryption take ~11.03ms with 1024-bit keys; and the use of encryption results in delivery ratio losses ranging from approximately 0.09% to 30.64% in different scenarios.

6.2.5 Summary. In this section, we surveyed applications of MPC and HE in the client-to-client setting, using a diverse set of technologies, including GC-based and SS-based MPC, PSI, and HE, enabling privacy-preserving interactions. Overall, we note a limited number of such implementations, likely due to the nature of vehicular settings with large fleets, real-time communication, resource constraints, and client drop-offs. These demands pose a challenge for resource-intensive MPC and HE technologies. Consequently, we observe more solutions either involving a centralized server or adopting complex decentralized setups, which we will discuss in the following sections.

6.3 Client-to-Server Setting

In this section, we discuss how MPC and HE address privacy concerns in the client-to-server setting, where clients (such as vehicles or users) interact with one or more servers that aggregate and process client data. The primary privacy concern here involves the handling and potential exposure of large-scale sensitive client data by servers, which may be vulnerable to misuse or breaches. To mitigate these risks, MPC and HE enable servers to perform computations on client data without directly accessing sensitive information.

We observe two primary cases within this setting. In the first case, servers typically function as service providers, performing computations on data collected from clients or providing specific services in response to client requests. Here, the server processes either encrypted data provided by clients (in the case of HE) or engages in an MPC protocol with clients, generating the desired outputs based on client data while preserving the privacy of individual inputs. Figure 2 illustrates this case on the left, with a concrete example of ride-sharing, where the server securely processes trip information from clients to generate suitable ride matches by computing on homomorphically encrypted client data. Note how this implementation differs from the ride-sharing use case within the client-to-client setting discussed in Section 6.2, where clients communicated with each other directly. The second case (right) involves an outsourced computation scenario, where multiple servers aggregate and process client data, where the result is further used by the server. This is represented in the figure (bottom right) by the vehicular crowdsourcing example, where three servers receive secret-shared route information from multiple clients and run an MPC protocol to identify vehicles suitable for a location-specific task without revealing individual vehicle locations.

These examples highlight how client-to-server implementations can leverage MPC and HE to protect privacy in applications involving sensitive data sharing and processing. Below, we examine relevant works that apply these techniques across different use cases.

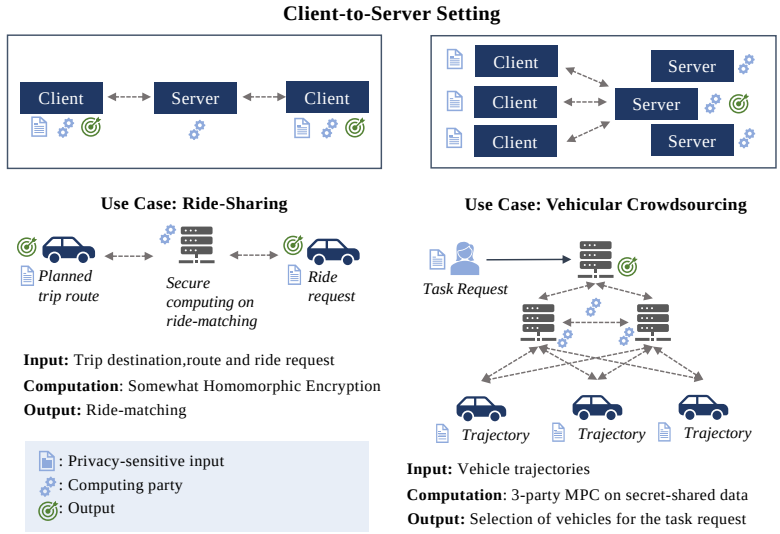

Fig. 2. Generic client-to-server setting, with two specific use cases under the same setting as examples. In this setting, clients typically provide their private inputs to the server, with output used by clients or server.

6.3.1 Privacy in Location-Based Services. The client-to-server setting is naturally represented in LBSs, where clients share sensitive location data with service providers to receive location-dependent services. Service providers need to process clients' location data to deliver their services while ensuring they cannot misuse this sensitive information. We observe three distinct use cases where MPC and HE are applied: mobile crowdsourcing, points of interest, and ride-sharing. Below, we examine how different works address privacy concerns in each of these scenarios.

Within the crowdsourcing scenario, mobile crowdsensing involves users collaborating through their sensing devices to complete a shared task, in applications like traffic monitoring and road condition analysis. In vehicular networks, the key challenges lie in assessing the reliability of sensing vehicles. To address these concerns, Peng et al. [88] propose a truth discovery scheme. The approach uses ASS where Sensing Users (SUs) distribute their collected sensing data to three servers in a secret-shared way. These servers jointly run a protocol to discover the most accurate information (ground truth) and to implement a quality-driven user reward mechanism. The data requester can later aggregate the shares from all servers to recover the final results. Kong et al. [59] propose a range query scheme using AHE. Vehicles equipped with air pollution sensors generate encrypted data reports containing the sensed values and their location information. In this scheme, AHE enables the protection of the location privacy of vehicles and data requesters.

In the context of querying POI, three approaches have been developed to protect privacy while allowing vehicles to obtain service results. First, Tan et al. [107] propose a computationally efficient PIR-based framework for vehicular LBS. Their approach partitions a city's road network into Natural Road Segments (NRS), with each segment maintaining an association with nearby POIs within a specified distance. This segmentation significantly reduces the dataset size, making the PIR-based protocol more efficient. When a vehicle queries POI information, it sends a PIR request that enables service retrieval without revealing either its exact location or query interests to the server. Second, Zhou et al. [147] introduce a novel POI protocol that combines multiple cryptographic techniques and is specifically designed for real road networks. The approach enables top-K POI queries through vehicle cooperation: Vehicles first obtain symmetric keys through OT, then use PIR to retrieve

encrypted POI details, while network coding ensures query interest privacy during processing. Third, Zhang et al. [143] propose a proximity testing scheme that uses two-party PSI to detect any location grids overlap, indicating proximity. For this scheme, Chebyshev polynomials are used to optimize computational efficiency and reduce energy consumption.

As observed from Table 4, ride-sharing applications have received significant attention in the context of LBSs, with multiple works proposing various privacy-preserving approaches. Pham et al. [90] proposed ORide, implementing SHE with optimized ciphertext packing for privacy-preserving ride-matching. While the system allows user matching without accessing their identities or locations, Kumaraswamy et al. [62] and Murthy and Vivek [82] revealed security limitations. A semi-honest rider can infer driver locations through a location-harvesting attack [62] or a passive triangulation attack [82] using the permuted distances of the riders in ORide. Further advancing privacy guarantees, SRide, proposed by Aïvodji et al. [5], implements ride-sharing with a two-stage approach. First, feasible matches for each rider are computed using an ASS protocol based on SHE. Then, it uses secure two-party equality testing to determine final matches. To address the efficiency concerns, He et al. [43] proposed PRIS, which uses AHE and bilinear pairing to protect location privacy. The system separates operations into offline (local generation of ride offers/requests) and online phases (secure matching), optimizing computational efficiency while maintaining privacy.

Luo et al. [75] propose a ride-matching protocol that operates in two variants: pRide and pRide_2. pRide encrypts rider and driver location data and distances using SHE (BGN [17]) and identifies the nearest driver via GC-based secure comparison. pRide_2 uses AHE (Paillier) for distance computation, GC for secure comparisons, while applying data packing and graph partitioning to reduce computation and communication costs. Huang et al. [51] present an SHE (FV [30])-based improved version of both the pRide and pRide_2 schemes, combining secure distance computation with a ride request prediction model for optimized driver matching. However, Murthy and Vivek [81] revealed that pRide_2 scheme [51] is vulnerable to driver location inference attacks, where a semi-honest rider uses decrypted distance values that were homomorphically blinded to recover the underlying distances and infer the locations of at least 80% of the drivers responding to a single ride request.

Yu et al. [132] proposed lpRide which enables efficient shortest road distance computation over encrypted rider and taxi locations using a lightweight encryption scheme based on the modified Paillier cryptosystem [83]. In addition, it securely compares two distances over the corresponding blinded ciphertexts to find the closest taxi. However, Vivek [112] showed that in lpRide, the modified Paillier cryptosystem is vulnerable to a key recovery attack, allowing any semi-honest rider or driver to extract the secret keys of other users and learn the location of riders.

Expanding the scope to group scenarios, Yu et al. [133] developed PGRide. The system uses SHE with ciphertext packing to compute aggregate distances between multiple riders and potential drivers in encrypted form. While supporting efficient group matching through separated offline (key generation) and online (secure computation) operations, the system cannot optimize the actual pickup route for multiple riders.Focusing on dynamic scheduling, Yu et al. [131] introduced PSRide. Unlike previous approaches requiring preset locations, PSRide allows real-time matching and schedule modifications even with active rides. The system uses AHE with cipher packing for computation and GCs for secure schedule feasibility checks. While this enables flexible ride-sharing, their use of upper-bound travel time estimates can lead to suboptimal matches. Another approach is proposed by Yu et al. [130], EPRide, allowing riders to submit encrypted ride requests to a server, which matches them with nearby taxis that regularly update their encrypted locations using SHE. The crypto server generates cryptographic keys and collaborates with the server to execute the secure comparison protocol based on HE to match riders with the nearest available taxi.

Leveraging the XOR-homomorphic property of the Goldwasser–Micali (GM) encryption algorithm, Xu et al. [123] proposed TAROT, route-matching scheme for ride-sharing services. It claims to

enable secure equality testing and route similarity computation between encrypted location points accurately, avoiding plaintext exposure during the matching process. However, subsequent passive attacks by Vargheese and Vivek [110] demonstrate that TAROT's GM-based equality determination algorithm leaks the Hamming weight of XORed encrypted location vectors during route similarity computation. By exploiting this leakage, colluding semi-honest users can infer other users' sensitive location data through two distinct passive attacks. In the first attack, adversaries select specific location points to infer the target's data. In the second attack, the location points of the colluding adversary are arbitrarily placed.

Taking a different approach, Zhang et al. [141] proposed a PSI-based approach. Instead of working with exact locations, their system represents user positions as sets of nearby POIs and then uses PSI to determine matching potential. This allows the platform to facilitate matches without accessing exact user locations, sharing driver information when sufficient geographical overlap exists.

Addressing scalability challenges, Luo et al. [74] introduced P^2Ride. Instead of using computationally expensive GCs, the system reduces matching to non-interactive PEQT using an overlapping partition system. This approach significantly reduces computational and communication overhead, making it more practical for large-scale deployment than GC-based solutions.

Karmakar et al. [57] proposed QuickPool, introducing two complementary approaches for simultaneous privacy-preserving ride-matching. The first uses pseudorandom functions for route intersection matching, while the second employs Function Secret Sharing (FSS) [18] to match users based on the proximity of trip endpoints. The system evaluates match compatibility through threshold-based distance comparisons while maintaining location privacy through computation.

6.3.2 Privacy in Vehicular Data Analysis. In IoV, aggregating sensitive data from vehicles to centralized servers for analysis requires privacy-preserving approaches to prevent the exposure of information during data exchanges. To aggregate vehicle perception data for analysis, Zhou et al. [21] propose a data aggregation scheme PPVDA. This scheme employs homomorphic MAC and SS to achieve lightweight, verifiable data aggregation, supporting multidimensional data inner product computation. The system operates by dividing each piece of sensed data from Vehicular Nodes (VNs) into multiple additive shares. These shares are then distributed to different RSUs. Each RSU combines its received shares and creates a partial proof, which is then sent to the central server for the reconstruction of the full data and computation of the final aggregation result. We observe similar SS-based approaches for vehicular data analysis in distributed setups in Section 6.4.3.

6.3.3 Privacy in Dynamic Traffic Management and V2X Communications. In a client-to-server setting, dynamic traffic management in vehicular networks utilizes the continuous exchange of data between vehicles and servers to optimize tasks such as emission control, energy management, and traffic management. Below, we see how different techniques are tailored to this setting.

Optimizing emissions and energy use often requires vehicles to share speed and emission data with servers. Liu et al. [71] introduce MPC-CSAS, a SS-based solution for recommending common speeds to a group of vehicles. In the conventional approach, vehicles A and B send their speed-emission mapping values directly to a base station, which aggregates these values and recommends the optimal speed. A and B split their speed-emission mappings into shares, keeping some locally and sharing others. They aggregate their local and shared data and send the results to the base station, which calculates the emissions for each speed and recommends the optimal speed. MPC-CSAS achieves real-time performance by computing the optimal speed in a single iteration using SS, with total communication less than 3KB for 20 vehicles and less than 5ms runtime.

Route planning often involves pre-sharing routes with RSUs to speed up authentication. Liang et al. [50] propose OT-based route planning scheme, where a vehicle securely obtains information about RSUs along its planned route with the help of a Certificate Authority (CA), without the

CA knowing which specific RSUs the vehicle has chosen. The vehicle uses this pre-shared RSU information to authenticate with RSUs as it enters its coverage.

Monitoring traffic flow at intersections requires driver data, introducing concerns about the privacy of their movements. Zhang et al. [137] propose VPTS, a crowdsourcing-based traffic monitoring scheme that ensures the privacy-preserving collection of traffic flow statistics at road intersections. This scheme utilizes HE and DP to secure traffic data. The process begins with initializing an instance of the BGN cryptosystem [37], where a trusted authority sets up public and private keys, selects a hash function, and communicates with the server for encrypted traffic direction data handling. Drivers report traffic conditions to an RSU that encrypts and aggregates the data before sending it to the server for processing. The server decrypts this data to predict and manage future traffic flow, which is used to control infrastructure, such as traffic light scheduling. VPTS requires ~26ms per driver for encryption, commitment, and signing, and 1.565s on the RSU for 200 drivers, with a communication overhead of 0.071KB per driver and 0.051KB on RSU-side.

Three approaches address privacy concerns in platoon formation and management. To enable clients to find and join nearby platoons without compromising their location privacy, Quero et al. [94] utilize the BFV [19] and CKKS [26]encryption schemes, which are FHE methods capable of performing multiple additions and a finite number of multiplications on encrypted data. Clients send encrypted platoon requests to the server, indicating their desired platoon location. The server responds with encrypted platoon identifiers, allowing clients to privately select and contact platoons. Their experiments show that each plaintext-ciphertext multiplication takes 1.99ms and total client-server interaction is under 6ms. A single processor core can serve up to 500 clients per second, making the system scalable to 100,000 daily users with a 10–20 core server.

To address the challenge of selecting reliable platoon leaders, Zhang et al. [139] propose a trust-based platoon recommendation scheme called TPPR, which helps potential user vehicles avoid selecting malicious head vehicles. The TPPR uses AHE to ensure secure communication between the lead vehicle and other vehicles when joining a platoon. Once the trip ends, both the lead vehicle and the joining vehicle send their driving reports, such as handshake proof and trust value, to RSUs. The RSU verifies the joining vehicle's legitimacy and calculates the lead vehicle's reliability rating using trust score and feedback. The service provider evaluates the joining vehicle's performance and shares it with the trusted authority for forecasting future actions based on historical behavior. TPPR aggregates ciphertexts for 100 users in 5.6ms and generates handshakes on vehicles in 18ms.

Addressing another concern in platooning, Cheng et al. [24] use HE to develop a recommendation system for vehicular platoons aimed at accurately calculating feedback about the lead vehicle's performance. Each vehicle encrypts its feedback score using additive homomorphic properties, ensuring that the platoon head vehicle's reputation can be computed on the aggregated encrypted data while maintaining individual score confidentiality. In the reputation score evaluation phase, AHE is applied to calculate the distances between encrypted feedback scores and to aggregate these encrypted values, allowing the determination of reputation scores while preserving the individual feedback data. Finally, trusted authorities and servers use the output for a recommendation system for vehicular platoons. Evaluation results show that AHE decryption takes 1.356ms (4 exponential operations) and encryption along with multiplication and hash operations run in 1.1673ms.

6.3.4 Summary. In this section, we surveyed applications of MPC and HE in the client-to-server setting. The solutions address privacy concerns across a diverse range of services, from location-based applications like ride-sharing and POI queries to traffic management services like platoon formation. These implementations are typically designed to scale with multiple clients, either computing on encrypted data from multiple clients (HE) or processing client data in secret-shared form (MPC). In the next section, we see how these techniques develop further in distributed settings.

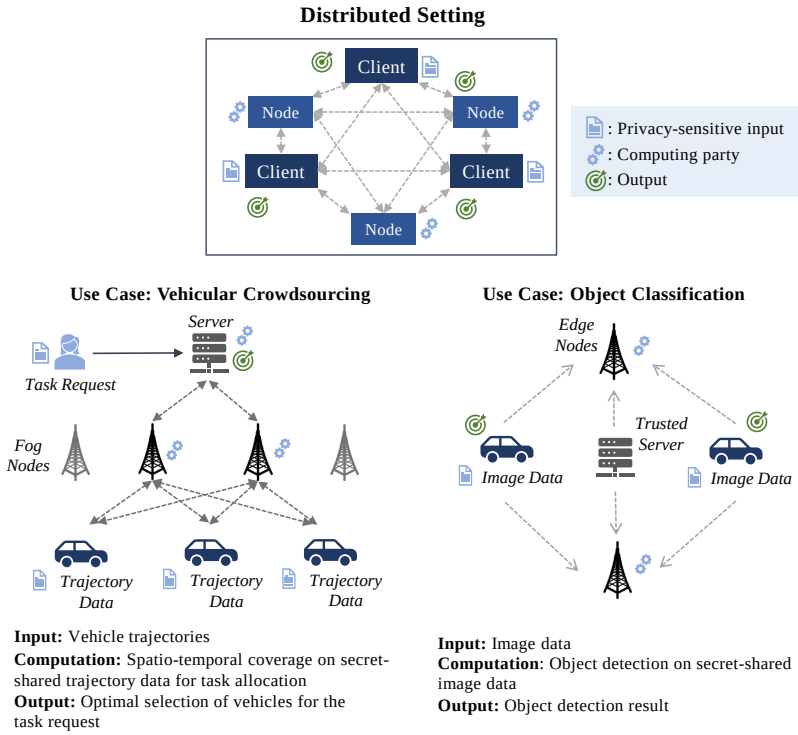

Fig. 3. Generic distributed setting, with two specific use cases under the same setting as examples. In this setting, clients typically provide their inputs to intermediate computing edge/fog nodes, with output used by all or some clients, or aggregated by a server.

6.4 Distributed Setting

In this section, we discuss the distributed setting, which extends beyond the traditional client-to-server model introduced in Section 6.3. In this setting, computational tasks are offloaded to a network of multiple servers, edge nodes, fog nodes, or other distributed resources. Edge and fog computing processes data at or near the data generation source, minimizing latency without the need to transmit data to distant servers. A layered structure supports handling large-scale data-intensive applications in vehicular networks with thousands of clients.

We illustrate two use cases within this distributed setting in Figure 3. In the first example, vehicular crowdsourcing, vehicles share trajectory data to two non-colluding fog nodes. These nodes can run an MPC protocol with a server, to select suitable vehicles for a location-based task. Compared to the vehicular crowdsourcing example in the client-to-server setting (see Figure 2), this implementation can scale to large number of computing nodes. The second example (bottom right) involves object classification, where two non-colluding edge nodes receive image data from vehicles, and run computer vision inference in a 2-party MPC protocol, allowing for privacy-preserving identification of objects in the images. Both examples illustrate how MPC and HE can support privacy in applications involving resource-intensive computations across a decentralized network. Below, we review existing research that applies these techniques to various distributed use cases.

6.4.1 Privacy in Location-Based Sevices. To protect location privacy in vehicle-based spatial crowdsourcing in IoV, Zhang et al. [142] propose a decentralized PriSC framework. Their scheme involves

requesters (such as vehicle services and traffic management) encrypting sensitive location policies using AHE, while vehicle workers submit their encrypted locations through Order-Preserving Encryption (OPE) [3] to a blockchain and verify their eligibility for the tasks. Workers also provide location proofs, enabling requesters to verify authenticity while preserving privacy, all recorded on the blockchain. PriSC incurs ∼1.7s computation per worker, ∼1.93s for encrypting 10 location policies with Paillier-1024, and ∼27.5ms for OPE-based location record generation with a 2^{40} plaintext space. Another approach is the PriTAEC scheme developed by Xu et al. [124], which utilizes OT and PEQT for securing task assignments. In this work, requesters and drivers submit their location data encoded through Hilbert curves and Bloom filters to edge nodes for range queries. In the proposed optimized model, edge nodes execute OT protocols with requesters during an offline phase, while drivers assist edge nodes to finalize the task. The edge computing framework helps reduce communication latency while preserving the location privacy. Specifically, PriTAEC achieves task assignment within ∼53ms, where OT accounts for ∼12ms and PEQT for ∼40ms.

Cheng et al. [25] address the task of reputation management in vehicle crowdsensing and propose a PPRM scheme. It is similar to the work by Peng et al. [88] (discussed in Section 6.3.1) but works in a different setting. To protect the privacy of sensing data and validate its authenticity, Cheng et al. use the Paillier algorithm for encryption and apply a comparison algorithm for Paillier ciphertext for data verification. Then, the cloud server transmits reputation feedback reports to the reputation center to efficiently update the sensing vehicles' reputation values.

Guan et al. [39] introduced a task allocation scheme for content dissemination in vehicular networks that uses SHE. In their approach, two non-colluding servers collaboratively select a certain number of vehicles to cover a near-optimal city area based on encrypted vehicle trajectory data. Although the scheme accounts for the high mobility of vehicles, processing large volumes of encrypted location data results in significant computational and communication overhead. Yu et al. [134] address task allocation in fog computing using a grid-based region encoding, where users' locations or trajectories are encrypted into binary arrays called region codes, the scheme applies bit-wise XOR-based secret sharing to split and transmit the codes to two fog servers. The cloud server then collaborates with both fog servers to allocate tasks without revealing user locations.

To address location privacy concerns in traffic navigation, Zhou et al.[149] propose a lightweight cryptographic primitive, Multiparty Delegated Computation (MPDC). It allows two non-colluding servers to perform secure addition, multiplication, and comparison over location data encrypted under different keys, providing similar privacy guarantees of MPC and FHE-based approaches with lower communication and computation overhead. Allowing a client to privately retrieve precomputed route segments without revealing which segment is being accessed, Tiausas et al. [108] introduces HPRoP, a PIR-based route planning system. More precisely, their approach provides privacy-preserving location and trajectory data processing by adding dummy queries alongside the real route planning request within a hierarchical road network structure.

Another LBS addressed in this setting is vehicle sharing, where users can share their vehicles via digital keys, known as Access Tokens (AT). HERMES, proposed by Symeonidis et al. [105], is a scalable and privacy-enhancing vehicular access system that extends SePCAR [104] by utilizing MPC to manage vehicle ATs across non-colluding servers. In HERMES, vehicle keys and booking details are kept private, as each server holds only a share of the secret data. The system optimizes MPC protocols by using AES-CBC-MAC for Boolean circuits and HtMAC for arithmetic circuits, minimizing communication rounds and computational overhead. This system allows for rapid AT generation in ∼30.30ms, managing up to 546 operation per second, while providing the scalability needed for real-world applications, such as rental companies overseeing 1000 vehicles.

6.4.2 Privacy in Mobility Infrastructures. As can be observed in Table 4, most privacy-preserving solutions for infrastructure-based vehicle services align with distributed settings, involving interactions between vehicles, RSUs, servers, and blockchain networks. These approaches are particularly relevant for preserving privacy as vehicle data moves through various infrastructure layers, such as toll systems, parking facilities, and traffic management platforms.

One relevant example is TollsOnly, a privacy risk reduction model proposed by Karim and Rawat [56]. The model addresses the need for secure and controlled sharing of electronic toll transponder data with smart city infrastructure planners, to help manage traffic congestion while preserving driver's location privacy. TollsOnly employs FHE to perform computations on encrypted toll data. In addition, a blockchain-based mechanism grants users control over how and when their encrypted data is shared with authorized entities.

Parking services in a distributed setting involve interactions between vehicles, parking providers, and decentralized units such as RSUs to securely manage and process parking data while preserving driver privacy. Zhang et al. [138] propose a blockchain-based smart parking scheme called BSDP to protect the privacy of Vehicular Sensor Network (VSN) participants and provide reliable data aggregation. The scheme employs the Paillier Cryptosystem with Threshold Decryption (PCTD) to securely encrypt and aggregate location and driving speed data from various VSN participants. Two adjacent RSUs collaborate to perform privacy-preserving data aggregation. Secure Hidden Vector Encryption (SHVE) is employed to handle encrypted location queries. BSDP aggregates data in under 150ms when 100 vehicles and parking requests in 2.5ms per driver.

Another blockchain-based approach for parking was proposed by Amiri et al. [6]. They leverage PIR to enable drivers to privately retrieve parking offers from a consortium blockchain, using Reed-Solomon codes to generate coded queries. Their evaluations show that PIR incurs low communication overhead with ∼3.5KB and ∼1ms computation for parking reservation, making it practical for real-world deployment. However, the complexity of PIR schemes generally increases with the number of nodes, which could impact scalability in very large networks.

With a similar concern, to protect the location privacy of drivers during the parking space detection and matching process, Li et al. [67] introduced PriParkRec. It utilizes OPRF and PSI to enable drivers to match available parking spaces provided by a semi-honest parking service provider without revealing their exact location. Anonymous credentials allow users to authenticate without disclosing their identities, while AHE ensures confidentiality during aggregated data operations.

6.4.3 Privacy in Vehicular Data Analysis. Many recent work address scalable vehicular data analysis through a distributed paradigm, largely to support privacy-preserving machine learning. In particular, Chen et al. [22] propose a Decentralized Privacy-preserving Deep Learning (DPDL) model for VANETs that aims to reduce network congestion and provide low-latency services. This decentralized approach shifts data processing from central cloud servers to Edge Computing (EC) nodes. The transportation data is encrypted using FHE before being input into local DPDL models on each EC node for training. Evaluation results indicate low communication latency, rising from 287.2ms to 823.6ms as the number of vehicles scales from 25 to 150.

Liu et al. [70] addressed real-time lane-changing trajectory prediction in VANETs based on SSS. Vehicles collect driving data and distribute it in secret-shared form to multiple RSUs, which collaboratively train an Adaboost [144] algorithm. Secure sub-protocols allow RSUs to jointly compute model updates, error rates, and trajectory predictions.

Li et al. [65] focus on addressing the limitations related to resource overhead in cloud-assisted fog computing, that involves multiple interactions between the cloud service center and the fog nodes, which can cause delays and increase resource overhead. They employ SSS to enable user gradients to split into multiple secret shares and distribute them among fog nodes. Specifically,

the (T, N) threshold property prevents collusion among up to $T - 1$ fog nodes and supports up to $N - T$ fog nodes, where N represents the number of fog nodes, and T stands for the threshold value. Their work distinguishes itself by enabling computation across an unlimited number of nodes N, offering greater scalability than other MPC methods that are typically limited to 2–4 nodes.

Hu et al. [49] propose DSSFL, a DFL-based data-sharing scheme for the IoV, integrating SSS and HE. In this approach, vehicles fragment their local model parameters using SSS, distributing these encrypted fragments to multiple RSUs. The use of HE (specifically, the CKKS scheme) allows RSUs to perform secure aggregation on these encrypted fragments. The results are then sent back to vehicles, which use Lagrange interpolation to recover the global model securely. Although HE adds computational overhead, the model still achieves a high accuracy of approximately 86% due to efficient data handling and secure aggregation methods. DSSFL uses SSS with a polynomial degree of 5, requiring at least 6 out of 10 RSUs for model reconstruction. Each vehicle sends 10 encrypted fragments per round. Model training converges in ∼9 minutes over 20 training rounds.

Li et al. [66] present a FL framework for autonomous vehicles based on HE and ZKPs to protect model updates from both semi-honest servers and potentially malicious vehicles. HE enables vehicles to share encrypted model updates securely without disclosing raw data, while ZKP ensures anonymous identity verification. This dual approach improves model accuracy and reduces training loss, but it faces latency challenges in high-mobility environments that could benefit from further optimization for real-time performance. A common limitation in privacy-preserving FL schemes is the challenge of handling new users and user dropouts [16, 122]. Kong et al. [61] propose a privacy-preserving aggregation scheme for FL in vehicular fog computing. Their approach combines SSS with a homomorphic threshold encryption scheme to ensure that client data remains private during model aggregation. SSS enables the system to tolerate user dropouts by establishing a minimum threshold for the number of user shares required for aggregation.

Beyond general solutions for privacy-preserving machine learning and FL, several works focus on concrete applications for smart and autonomous vehicles. Xiong et al. [119] propose an edge-assisted framework for privacy-preserving object classification. In this ASS-based approach, a vehicle splits an image into shares for two non-colluding edge servers, which cooperatively process them with a deep learning model. The same authors in [118] introduce a refined lightweight ASS-based scheme with enhanced security using chaotic map encryption and proposing a multi-party extension to tolerate offline servers. Bi et al. [14] extend the approach to full object detection with their P2OD framework, which implements a secure equivalent of Faster R-CNN to privately compute both object features and their bounding boxes. These works show that it is possible to offload intensive computer vision tasks from vehicles to edge servers in a privacy-preserving manner.

Kong et al. [60] propose a privacy-preserving scheme based on HE and DP for continuous data collection in vehicular fog to implement predictive maintenance, aiming to detect the anomalies of vehicles and offer early warnings in ITSs. In this scheme, the Paillier cryptosystem is used to encrypt individual sensory data pieces, facilitating the secure aggregation of multiple data reports directly at the fog nodes before sending these encrypted data to the cloud server. DP is applied by adding noise to each aggregated result, making it difficult to infer individual data points.

Gyawali et al. [40] proposes a privacy-preserving misbehavior detection system in VANETS. In this work, vehicles evaluate messages from neighboring vehicles and send weighted, encrypted feedback scores to the Local Authority (LA), utilizing a modified ElGamal cryptosystem. The LA aggregates these encrypted scores without accessing the individual values and then forwards the aggregated result to the Trusted Authority (TA). The TA decrypts this result to update the vehicle reputation scores. The authors emphasize that in contrast to the Paillier cryptosystem, which causes considerable delays, the lightweight and efficient ElGamal-based encryption, with additive homomorphic properties, is better suited for misbehavior detection systems. Additionally,

implementing batch verification in a bilinear system further reduces delays to 8.23ms per encrypted feedback at the vehicle-side and 7.61ms for decryption and verification.

6.4.4 Privacy in Dynamic Traffic Management and V2X Communications. Energy storage sharing involves challenges in maintaining the privacy of clients' energy demands. To address these issues, Wang et al. [113] propose a solution combining blockchain and SSS, enabling secure service scheduling without revealing individual users' demands. Users share their individual energy demands in a secret-shared way and generate ZKPs to verify the consistency of their commitments before calculating the energy storage service schedule and agreeing on payments. They then submit these payments to the ledger with proofs, execute the service, and request settlement, with the operator verifying transactions through signed receipts on the ledger.

Ying et al. [128] propose PrivacySignal to address the vulnerability in traffic control systems where the transmission of vehicle data, such as location and speed, potentially leads to privacy breaches. In this system, vehicles divide their location and speed data into secret shares that are processed by RSUs. To demonstrate the feasibility of PrivacySignal in the multi-party setting, the authors assert that its sub-protocols, such as secure addition, multiplication, and comparison, are MPC- compatible, Indeed, indicating the system's potential for scaling to more RSUs in practical implementations. PrivacySignal incurs a runtime overhead ranging from 0.003s to 0.672s and a communication overhead between 4.9KB and 45.8KB across its secure sub-protocols, by employing ASS protocols, making it suitable for real-time applications. Recently, Adelipour et al. [2] proposed another approach to traffic signal control systems to enable secure green time durations, i.e., the time intervals during which specific traffic lights remain green, in urban networks. To achieve this, they use SSS to distribute real-time traffic data across multiple shares, allowing semi-honest servers to jointly compute green time signals without accessing the raw data.

6.4.5 Summary. In this section, we reviewed applications of HE and MPC in distributed settings. These implementations typically leverage multiple computing nodes to process data closer to the source. The solutions aim to support large dynamic vehicle fleets and address diverse use cases, from scalable location-based services to real-time data analysis. We observe increasing adoption of hybrid approaches combining multiple privacy-preserving technologies. While distributed architectures offer improved scalability compared to traditional client-server models, they introduce additional complexity and require careful privacy analysis.

7 TAKEAWAYS AND DISCUSSION

In this section, we review the applicability of MPC and HE in the automotive domain, based on the analysis in the previous Section 6, and highlight several challenges in applying these technologies.

7.1 Primitives

We observe that both MPC and HE are widely applied to secure computing scenarios in the automotive domain, and are useful across a variety of use cases. MPC and HE are sometimes employed interchangeably within the same use cases, offering similar, though not identical, privacy guarantees and resource requirements. For instance, ride-sharing and vehicular crowdsourcing scenarios show applications of both HE and MPC-based solutions.

In particular, AHE and SHE are frequently adopted across ride-sharing, platooning, and crowdsourcing applications, utilizing privacy-preserving arithmetic operations. While FHE theoretically supports more complex operations, it is currently less suited for multi-client collaborative scenarios, as it typically requires data to be encrypted under the same key. Multi-key FHE schemes provide a promising alternative by enabling computations on data encrypted by different parties with their individual keys [79]. However, many such schemes are limited to working over single-bit

ciphertexts and may not be suitable for encrypting large datasets [135]. A notable challenge for AHE and SHE-based solutions is the increased size of encrypted messages, which leads to higher computational and bandwidth demands. Nonetheless, several reviewed optimized approaches like hybrid PSI and SHE schemes [41], and ciphertext-packing techniques [20] help reduce the payload sizes, reducing the computational and communication overhead when handling large-scale systems.

MPC approaches also demonstrate their utility in the automotive domain, particularly those based on Secret Sharing (SS). SS-based non-linear computation requires more communication rounds compared to HE and GC-based approaches. However, they are advantageous for linear computations, having relatively low costs during the input-independent computation in the online phase [145]. These approaches prove particularly effective in outsourced settings, such as Federated Learning [61, 66] and vehicular crowdsourcing [134], where clients can upload their privacy-sensitive data to external servers for computation, enabling clients to remain offline between iterations and reducing computational overhead. In non-outsourced scenarios such as EV charging [52, 113], speed advisory [71], ride-sharing [57] and vehicle sharing [104, 105], secret sharing can be employed to protect sensitive information, while clients need to be online during data exchange process.

In contrast, there are only a few GC-based MPC approaches to privacy issues in the automotive domain. For instance, we can see several GC-based solutions for vehicle localization and ride-sharing scenarios. In the localization use case [53], we can see the comparison-based nonlinear functions can be efficiently implemented in a two-party setting utilizing GC. However, considering the large number of clients in ride-sharing, GC protocols incur high communication and computation overhead. For instance, Luo et al. [75] used GC to lightweight the distance comparison computation between rider and driver; however, it is not practical for real-world ride-sharing applications.

We observe that several papers utilize PSI in distinct automotive scenarios with matching as main function: parking [67], ride-sharing[4, 41, 57, 86, 141], profile matching [114], and POIs [143]. The intersection of multiple sets can be calculated iteratively by performing pairwise intersections. Extending the two-party PSI protocol to a multi-party setting in certain automotive use cases may not be straightforward. However, there are several works on Multi-Party PSI (MPSI) [10, 140]. Although MPSI comes with higher communication overhead and complexity, it reduces the limitations of PSI among a larger group of participants [78]. Despite the limitations of both techniques, considering the trade-offs, MPSI might be a new research direction for automotive scenarios such as ride-sharing or spatial crowdsourcing.

Our study shows that both MPC and HE are effective for implementing privacy-preserving aggregation of sensitive vehicular data. In particular, integrating MPC with FL enables model training on client data without exposing individual model parameters. In an FL setup, the communication of model updates can be done via MPC, which enhances the privacy of the system. Similarly, HE can also be a suitable choice for privacy-preserving aggregation in respective scenarios. HE efficiently supports the arithmetic addition, which aligns well with the frequent requirement in vehicular data analysis and FL to compute aggregated averages based on the client's data.

Our analysis reveals limited adoption of MPC and HE in client-to-client settings, such as in V2V/V2X contexts, primarily due to the requirements for dynamic, real-time communication. Recent developments in efficient two-party MPC protocols [33, 73] offer promising solutions to enhance the applicability of these use cases. In contrast, we observe an increasing number of works addressing scalable and distributed settings. These complex scenarios often require not only privacy-preserving computation but also verification of client inputs, achieved through PVSS [100] as demonstrated in [23], or through MPC protocols with authenticated inputs [28]. For server-side vehicular data analysis applications, additional privacy measures for protecting computation outputs become relevant, such as combining MPC and HE with differential privacy techniques [106, 113].

7.2 Performance

Given the diversity of system settings, protocols, and evaluation metrics, a direct performance comparison across all surveyed papers is not straightforward. The surveyed papers span a wide spectrum, from highly performant, lightweight systems to computation or communication-heavy systems, which makes it challenging to draw generalized performance evaluations.

Direct comparisons are possible for specific applications such as ride-sharing. For example, in the client-to-server setting, the SHE-based ORide [90] approach shows high computation overhead from 0.2s to ∼114s for different algorithms on the server side. This overhead was later reduced to 37.13s in PRIS [43] using AHE and bilinear pairing. SRide [5] introduces a more efficient two-stage approach with 0.519s for match computation (SHE-based SS) and 0.005s for equality testing, requiring 62KB and 31KB of communication for riders and drivers, respectively, with 1000 drivers. More recent works further improve efficiency: pRide2 [75] achieves 0.0051s rider-side and 9.1s server-side runtime with only 256 bytes of communication per user; EPRide [130] reaches ∼0.0006s client-side runtime and 8.67MB server-side communication for 2000 taxis; PGRide [133] supports group matching with ∼1.25s server runtime and less than 3.2 MB communication for 2000 drivers; and PSRide [131] enables dynamic scheduling with ∼1.5s server runtime and 2.3 MB communication for 6000 taxis. P^2Ride [74] replaces GC with non-interactive PEQT, reducing rider-side computation from 58.6s to 0.47s and driver-side from 60.1s to 4.7s, with 784 bytes and 9.8KB communication, respectively. In contrast, client-to-client protocols show worse performance. The PrivatePool [41] exhibits high runtime with trajectory size (0.022s for 32 segments to 96.78s for 1024), whereas TOPPool [86] reduces this to less than 0.31s. Aïvodji et al. [5] report runtimes between 0.48–0.67s for PSI-based matching. Overall, client-to-server solutions offer better scalability and lower per-client latency, while client-to-client approaches are better suited for small-scale setups.

Although the ride-sharing shows a clear trend towards efficiency, applications that involve large-scale or data-intensive computations still exhibit significant performance overheads. For example, end-to-end object classification by Xiong et al. [118] requires over 20s and 327 MB of communication, while the object detection task by Bi et al. [14] takes 190s and over 6 GB for a single detection. Similarly, the HPRoP algorithm for route planning requires ∼23.55s to compute a complete route, a notable latency despite being an improvement over prior work.

Overall, our analysis shows that MPC and HE are feasible in scenarios that do not require continuous real-time updates and can tolerate moderate latency. In addition, recent protocol optimizations and hybrid approaches have reduced overheads and improved scalability, particularly in client–to–server and distributed settings. However, MPC and HE likely remain infeasible in use cases with large numbers of clients, frequent real-time interactions, and complex system design.

7.3 Datasets

We observe that several surveyed works evaluate their solutions on real-world datasets while others use simulated data only (see Table 4). We also observe that only a few works perform an evaluation on relatively large datasets containing hundreds of thousands of records or more [41, 66, 74, 90, 94, 142]. We believe that only the evaluation on real-world datasets (recently surveyed in [8, 72]) can validate the applicability of the solutions, while the large-scale evaluation can prepare the solutions for deployment in large national fleets. The release of new large-scale datasets, and unified evaluation benchmarks for HE and MPC based on them, would provide great value for privacy research in automotive applications, as authors could evaluate their works in realistic settings.

7.4 Security Model

We find that most MPC and HE works in our paper assume a semi-honest security model, where participating parties honestly follow a protocol. However, in practical applications, real-world threats often come from malicious attackers. Therefore, it is important to study the performance of protocols that offer protection against actively malicious adversaries. Several works (see Table 4) demonstrate the applicability of malicious security models in the automotive domain. Protocols designed under the assumption of semi-honest adversaries can often be modified to protect against malicious adversaries. However, this modification significantly increases cost, often to levels impractical for real-world applications. Overall, the extension of MPC to larger-scale applications remains a challenge, particularly under a fully malicious security model [29].

8 FUTURE DIRECTIONS

Although extensive research has already addressed many challenges related to privacy issues in the automotive domain, there are still several key research problems that need further exploration. We highlight several key areas below to inspire future directions.

Unaddressed Use Cases. Our analysis in Sections 5-6 reveals several privacy-sensitive automotive use cases that remain unaddressed by either MPC or HE, including traffic anomaly detection, road profile estimation, vehicle emission control, etc. Addressing these use cases is a clear opportunity for future work. Furthermore, we observe that several use cases leverage HE but not MPC, such as predictive maintenance, misbehavior detection, platooning, etc. Similarly, some use cases employ MPC but lack HE-based solutions, e.g., querying points of interest, localization, EV charging, etc. Given that MPC and HE can be applied interchangeably in many scenarios, exploring alternative implementations of existing solutions using the other technology, and comparing their respective requirements and guarantees, could offer valuable insights for automotive applications.

Baseline Implementations. The surveyed research works typically propose comprehensive solutions addressing multiple requirements for specific use cases. For instance, numerous ride-sharing solutions are proposed, each with different complexity levels and privacy guarantees. However, the field often lacks baseline implementations of fundamental MPC and HE protocols for common automotive scenarios. Proof-of-concept implementations, evaluated on sample data, would enable systematic evaluation of various approaches. Such implementation would help researchers assess how different requirements (e.g., moving from semi-honest to malicious security models) affect system performance, and determine the applicability of technologies in corresponding use cases.

Real-World Datasets and Benchmarks. Existing works mostly evaluate their approaches to simulated vehicular data. We need publicly available real-world datasets to improve the accuracy and applicability of privacy-preserving solutions in real-world automotive scenarios. Similarly, one of the future directions can be focusing on establishing standard benchmarks with unified datasets and metrics, allowing for the comparison of performance and scalability across privacy-preserving solutions for similar automotive use cases and settings.

Security Model. The security model in privacy-preserving approaches needs to be strengthened to ensure robust solutions by moving from semi-honest to malicious security in practical applications. Recent advances in MPC demonstrate that malicious security can be achieved efficiently using techniques such as authenticated secret sharing (e.g., SPDZ-style IT-MACs) and optimized preprocessing protocols (e.g., MASCOT) [31]. Applying and benchmarking maliciously secure MPC protocols in privacy-sensitive vehicular use cases remains an open and promising direction.

Dynamic Data. Most existing approaches omit client dropouts and focus on static vehicular data processing. The development of flexible, dynamic datasets and solutions that can cope with dynamic users might be a future research direction that needs to be addressed.

Broader Exploration of Use Cases and Privacy-Preserving Technologies. In Section 5, our work specifically reviewed automotive use cases that were explicitly identified as privacy-sensitive or implemented privacy-preserving solutions to analyze the applicability of HE and MPC in those. Future research could expand this scope to systematically analyze a broader range of automotive use cases, identify *new* privacy-sensitive use cases, and study suitable solutions. Finally, while our work concentrated on MPC and HE, similar systematic analysis could be conducted for other PETs, such as DP, anonymization techniques, zero-knowledge proofs, or a combination of those.

Alignment with Privacy Regulations. A promising future direction includes aligning solutions with privacy regulations such as GDPR and CCPA. We find that only eight works surveyed in Section 6 discuss the relation to such frameworks: some suggest their solutions help minimize data disclosure to ensure compliance [41, 86]; others highlight that regulations complicate use case adoption without such solutions [71, 123], or serve as a general motivation for applying PETs in considered scenarios [2, 56, 113, 137]. Future work can include a detailed legal assessment of the proposed schemes. Recent analysis shows MPC's classification as a GDPR-compliant anonymization technique depends on the deployment setting, such as the legal relationship between the parties computing on the secret shares [12]. Future research can evaluate which automotive settings (e.g., specific client-to-client or distributed configurations) best align with such regulations. Furthermore, research could explore how complementary technologies, such as applying differential privacy to computation outputs, can enhance both the technical privacy guarantees and the solution's legal standing.

Application to Existing Automotive Standards. Most surveyed papers frame their solutions in the V2X or CAVs context; however, they rarely align with established automotive standards such as ISO/SAE 21434, AUTOSAR, or IEEE 802.11p. Some works reference these standards and incorporate related simulation parameters such as message size, latency, or communication range [22, 24, 50, 53, 66, 139]. Others mention standards such as IEEE 802.11p or AUTOSAR only at a conceptual level, without integrating them into the system architecture or evaluation [21, 40, 59, 76]. Future research direction should align proposed solutions with these regulations and evaluate them on automotive hardware (e.g., ECUs, embedded SoCs) under realistic network conditions.

Formal Analysis. We observe that the surveyed works offer different levels of security analysis. Some works provide formal, simulation-based or game-based proofs (e.g., [41, 57]). Other works (e.g.,[5, 53]) argue for their security based on the security of their underlying cryptographic primitives without providing a formal proof for the complete system. Vulnerabilities (e.g., [62, 82, 112]) found in some schemes (see Section 6.3.1) further demonstrate the need for a rigorous security analysis. A key direction for future research is therefore to perform comprehensive security analysis for proposed solutions. For use cases with multiple privacy-preserving solutions, such as ride-sharing or vehicular crowdsourcing, it would be beneficial to perform a *comparative* analysis of the guarantees offered by different approaches. Strengthening the formal analysis will improve trust and facilitate the adoption of PETs in the automotive domain.

Recent Advancements in PETs. Finally, we point out several developments in the fields of PETs, outside the automotive domain, that can be transferrable to vehicular applications.

Significant work has been done on improving MPC and HE with hybrid protocols for deep learning applications. Specifically, combining different cryptographic primitives, such as HE for linear operations and SS or GCs for non-linear functions, can significantly reduce computation

and communication overhead compared to single-primitive solutions [35, 145]. The vehicular data analysis papers we surveyed mainly rely on a single primitive. Future work can explore adapting these hybrid approaches for vehicular use cases, such as trajectory prediction, object classification, or predictive maintenance. Furthermore, the choice of MPC protocol should align with automotive network characteristics. As discussed in recent works [31, 85], SS-based approaches are better suited for low-latency settings such as edge-based local area network (LAN). In contrast, GC protocols and non-interactive HE-based protocols are often more appropriate for wide area networks (WANs).

Beyond protocol design, the field is advancing with the development of usable compilers and frameworks (such as CrypTen, EzPC, MP-SPDZ) that abstract cryptographic complexity and automatically translate high-level code and DL interfaces into optimized MPC protocols [58, 85]. These advancements can simplify and accelerate adoption in vehicular applications.

Finally, research in secure aggregation for FL has evolved to include integrity and verification mechanisms, and ensure robustness against malicious participants [77]. In addition, complementary research explores secure FL architectures in distributed settings such as IoT networks [44, 47], software defined networks [45] and wireless sensor networks [46]. These works may offer transferable insights to collaborative vehicular applications such as FL-based navigation, misbehavior detection, object classification, and predictive maintenance.

9 CONCLUSION

In this paper, we offer a thorough analysis of current MPC and HE applications in the automotive domain. First, we identified and categorized a set of privacy-sensitive use cases relevant to modern automotive architectures and setups. The privacy use cases they examine mainly focus on privacy in the contexts of location-based services, mobility infrastructure, vehicular data analysis, and dynamic traffic management. Second, we studied existing works applying MPC and HE to the selected privacy-related use cases in detail. Based on our comprehensive analysis, existing MPC and HE applications in privacy-sensitive automotive scenarios offer promising directions for research and development toward privacy-preserving, deployable, and scalable computing approaches in the automotive domain. Finally, we highlight areas for future research in this field.

REFERENCES

[1] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti. 2018. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)* 51, 4 (2018), 1–35.

[2] Saeed Adelipour, Enayatollah Amiri Darreh Razgahi, and Mohammad Haeri. 2025. Vulnerability Mitigation of Urban Traffic Control Against Cyberattacks Using Secure Multi-Party Computation. *IEEE Transactions on Intelligent Transportation Systems* 26 (2025), 4568–4578.

[3] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. 2004. Order preserving encryption for numeric data. In *Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data* (Paris, France) *(SIGMOD '04)*. Association for Computing Machinery, New York, NY, USA, 563–574.

[4] Ulrich Matchi Aïvodji, Sébastien Gambs, Marie-José Huguet, and Marc-Olivier Killijian. 2016. Meeting points in ridesharing: A privacy-preserving approach. *Transportation Research Part C: Emerging Technologies* 72 (2016), 239–253.

[5] Ulrich Matchi Aïvodji, Kévin Huguenin, Marie-José Huguet, and Marc-Olivier Killijian. 2018. SRide: A Privacy-Preserving Ridesharing System. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (Stockholm, Sweden) *(WiSec '18)*. Association for Computing Machinery, New York, NY, USA, 40–50.

[6] Wesam Al Amiri, Mohamed Baza, Karim A. Banawan, Mohamed Mahmoud, Waleed S. Alasmary, and Kemal Akkaya. 2019. Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval. *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)* (2019), 1–6.

[7] Md Momin Al Aziz, Md Nazmus Sadat, Dima Alhadidi, Shuang Wang, Xiaoqian Jiang, Cheryl L Brown, and Noman Mohammed. 2019. Privacy-preserving techniques of genomic data—a survey. *Briefings in bioinformatics* 20, 3 (2019), 887–895.

[8] Bifta Sama Bari, Deepak Puthal, and Kumar Yelamarthi. 2025. Datasets in Vehicular Communication Systems: A Review of Current Trends and Future Prospects. *SN Comput. Sci.* 6 (2025), 210.

[9] Pablo Andrés Barbecho Bautista, Luis Felipe Urquiza-Aguiar, and Mónica Aguilar-Igartua. 2022. Privacy-Aware Vehicle Emissions Control System for Traffic Light Intersections. *Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks* (2022).

[10] Aslı Bay, Zekeriya Erkin, Jaap-Henk Hoepman, Simona Samardjiska, and Jelle Vos. 2022. Practical Multi-Party Private Set Intersection Protocols. *IEEE Transactions on Information Forensics and Security* 17 (2022), 1–15.

[11] D. Beaver, S. Micali, and P. Rogaway. 1990. The round complexity of secure protocols. In *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing* (Baltimore, MD, USA) *(STOC '90)*. Association for Computing Machinery, New York, NY, USA, 503–513.

[12] Sebastian Becker, Christoph Bösch, Benjamin Hettwer, Thomas Hoeren, Merlin Rombach, Sven Trieflinger, and Hossein Yalame. 2025. Multi-Party Computation in Corporate Data Processing: Legal and Technical Insights. *IACR Cryptol. ePrint Arch.* 2025 (2025), 463. https://api.semanticscholar.org/CorpusID:276962245

[13] Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Pedro Miguel S'anchez S'anchez, Sergio L'opez Bernal, Gérôme Bovet, Manuel Gil Pérez, Gregorio Mart'inez P'erez, and Alberto Huertas Celdr'an. 2022. Decentralized Federated Learning: Fundamentals, State of the Art, Frameworks, Trends, and Challenges. *IEEE Communications Surveys & Tutorials* 25 (2022), 2983–3013.

[14] Renwan Bi, Jinbo Xiong, Youliang Tian, Qi Li, and Kim-Kwang Raymond Choo. 2023. Achieving Lightweight and Privacy-Preserving Object Detection for Connected Autonomous Vehicles. *IEEE Internet of Things Journal* 10 (2023), 2314–2329.

[15] G. R. Blakley. 1979. Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*. 313–318.

[16] Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, and Karn Seth. 2016. Practical Secure Aggregation for Federated Learning on User-Held Data.

[17] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. 2005. Evaluating 2-DNF Formulas on Ciphertexts. In *Proceedings of the Second International Conference on Theory of Cryptography* (Cambridge, MA) *(TCC'05)*. Springer-Verlag, Berlin, Heidelberg, 325–341.

[18] Elette Boyle, Nishanth Chandran, Niv Gilboa, Divya Gupta, Yuval Ishai, Nishant Kumar, and Mayank Rathee. 2020. Function Secret Sharing for Mixed-Mode and Fixed-Point Secure Computation. *IACR Cryptol. ePrint Arch.* 2020 (2020), 1392.

[19] Zvika Brakerski. 2012. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. In *Advances in Cryptology – CRYPTO 2012*, Reihaneh Safavi-Naini and Ran Canetti (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 868–886.

[20] Zvika Brakerski, Craig Gentry, and Shai Halevi. 2013. Packed Ciphertexts in LWE-Based Homomorphic Encryption. In *International Conference on Theory and Practice of Public Key Cryptography*.

[21] Fu cai Zhou, Qiyu Wu, Pengfei Wu, Jian Xu, and Da Feng. 2024. Privacy-preserving and verifiable data aggregation for Internet of Vehicles. *Comput. Commun.* 218 (2024), 198–208.

[22] Jianguo Chen, Kenli Li, and Philip S. Yu. 2022. Privacy-Preserving Deep Learning Model for Decentralized VANETs Using Fully Homomorphic Encryption and Blockchain. *IEEE Transactions on Intelligent Transportation Systems* 23, 8 (2022), 11633–11642.

[23] Jin-Hua Chen, Min-Rong Chen, Guo-Qiang Zeng, and Jia-Si Weng. 2021. BDFL: A Byzantine-Fault-Tolerance Decentralized Federated Learning Method for Autonomous Vehicle. *IEEE Transactions on Vehicular Technology* 70, 9 (2021), 8639–8652.

[24] Hongyuan Cheng, Xianchao Zhang, Jingkang Yang, and Yining Liu. 2023. PPRT: Privacy Preserving and Reliable Trust-Aware Platoon Recommendation Scheme in IoV. *IEEE Systems Journal* 17, 3 (2023), 4922–4933.

[25] Yudan Cheng, Jianfeng Ma, Zhiquan Liu, Yongdong Wu, Kaimin Wei, and Caiqin Dong. 2023. A Lightweight Privacy Preservation Scheme With Efficient Reputation Management for Mobile Crowdsensing in Vehicular Networks. *IEEE Transactions on Dependable and Secure Computing* 20 (2023), 1771–1788.

[26] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. 2017. Homomorphic Encryption for Arithmetic of Approximate Numbers. In *International Conference on the Theory and Application of Cryptology and Information Security*.

[27] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. 1995. Private information retrieval. *Proceedings of IEEE 36th Annual Foundations of Computer Science* (1995), 41–50.

[28] Moumita Dutta, Chaya Ganesh, Sikhar Patranabis, and Nitin Singh. 2022. Compute, but Verify: Efficient Multiparty Computation over Authenticated Inputs. *IACR Cryptol. ePrint Arch.* 2022 (2022), 1648.

[29] David Evans, Vladimir Kolesnikov, and Mike Rosulek. 2018. A Pragmatic Introduction to Secure Multi-Party Computation. *Foundations and Trends in Privacy and Security* 2, 2-3 (2018), 70–246.

[30] Junfeng Fan and Frederik Vercauteren. 2012. Somewhat Practical Fully Homomorphic Encryption. Cryptology ePrint Archive, Paper 2012/144.

[31] Dengguo Feng and Kang Yang. 2022. Concretely efficient secure multi-party computation protocols: survey and more. *Secur. Saf.* 1 (2022), 2021001.

[32] Michael J. Freedman, Kobbi Nissim, and Benny Pinkas. 2004. Efficient Private Matching and Set Intersection. In *International Conference on the Theory and Application of Cryptographic Techniques*.

[33] Offir Friedman, Avichai Marmor, Dolev Mutzari, Omer Sadika, Yehonatan C. Scaly, Yuval Spiizer, and Avishay Yanai. 2024. 2PC-MPC: Emulating Two Party ECDSA in Large-Scale MPC. *IACR Cryptol. ePrint Arch.* 2024 (2024), 253.

[34] Andreas Fuchs, Dustin Kern, Christoph Krauß, and Maria Zhdanova. 2020. TrustEV: trustworthy electric vehicle charging and billing. *Proceedings of the 35th Annual ACM Symposium on Applied Computing* (2020).

[35] Idoia Gamiz, Cristina Regueiro, Oscar Lage, Eduardo Jacob, and Jasone Astorga. 2024. Challenges and future research directions in secure multi-party computation for resource-constrained devices and large-scale computations. *Int. J. Inf. Sec.* 24 (2024), 27.

[36] Huan Gao, Zhaojian Li, and Yongqiang Wang. 2022. Privacy-Preserving Collaborative Estimation for Networked Vehicles With Application to Collaborative Road Profile Estimation. *IEEE Transactions on Intelligent Transportation Systems* 23 (2022), 17301–17311.

[37] Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. 2010. A Simple BGN-Type Cryptosystem from LWE. *IACR Cryptol. ePrint Arch.* 2010 (2010), 182.

[38] Oded Goldreich. 1998. Secure multi-party computation. *Manuscript. Preliminary version* 78, 110 (1998), 1–108.

[39] Yunguo Guan, Rongxing Lu, Yandong Zheng, Jun Shao, and Guiyi Wei. 2020. Achieving Privacy-Preserving Vehicle Selection for Effective Content Dissemination in Smart Cities. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference* (2020), 1–6.

[40] Sohan Gyawali, Yi Qian, and Rose Qingyang Hu. 2021. A Privacy-Preserving Misbehavior Detection System in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology* 70, 6 (2021), 6147–6158.

[41] Per Hallgren, Claudio Orlandi, and Andrei Sabelfeld. 2017. PrivatePool: Privacy-Preserving Ridesharing. In *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. IEEE, Santa Barbara, CA, USA, 276–291.

[42] Muhammad Hataba, Ahmed Sherif, Mohamed Mahmoud, Mohamed Abdallah, and Waleed Alasmary. 2022. Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey. *IEEE Open Journal of the Communications Society* 3 (2022), 811–829.

[43] Yuanyuan He, Jianbing Ni, Xinyu Wang, Ben Niu, Fenghua Li, and Xuemin Shen. 2018. Privacy-Preserving Partner Selection for Ride-Sharing Services. *IEEE Transactions on Vehicular Technology* 67, 7 (2018), 5994–6005.

[44] Zakaria Abou El Houda, Bouziane Brik, Adlen Ksentini, Lyes Khoukhi, and Mohsen Guizani. 2022. When Federated Learning Meets Game Theory: A Cooperative Framework to Secure IIoT Applications on Edge Computing. *IEEE Transactions on Industrial Informatics* 18 (2022), 7988–7997.

[45] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and Lyes Khoukhi. 2023. MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain. *IEEE Transactions on Network Science and Engineering* 10 (2023), 1985–2001.

[46] Zakaria Abou El Houda, Hajar Moudoud, and Bouziane Brik. 2024. Federated Deep Reinforcement Learning for Efficient Jamming Attack Mitigation in O-RAN. *IEEE Transactions on Vehicular Technology* 73 (2024), 9334–9343.

[47] Zakaria Abou El Houda, Hajar Moudoud, Bouziane Brik, and Lyes Khoukhi. 2023. Securing Federated Learning through Blockchain and Explainable AI for Robust Intrusion Detection in IoT Networks. *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (2023), 1–6.

[48] Zakaria Abou El Houda, Hajar Moudoud, Bouziane Brik, and Lyes Khoukhi. 2024. Blockchain-Enabled Federated Learning for Enhanced Collaborative Intrusion Detection in Vehicular Edge Computing. *IEEE Transactions on Intelligent Transportation Systems* 25 (2024), 7661–7672.

[49] Xiaoya Hu, Ruiqin Li, Licheng Wang, Yuqiao Ning, and Kaoru Ota. 2023. A Data Sharing Scheme Based on Federated Learning in IoV. *IEEE Transactions on Vehicular Technology* 72, 9 (2023), 11644–11656.

[50] Yan hua Liang, Yining Liu, and Brij Bhooshan Gupta. 2022. PPRP: Preserving-Privacy Route Planning Scheme in VANETs. *ACM Transactions on Internet Technology* 22 (2022), 1 – 18.

[51] Junxin Huang, Yuchuan Luo, Shaojing Fu, Ming Xu, and Bowen Hu. 2021. pRide: Privacy-Preserving Online Ride Hailing Matching System With Prediction. *IEEE Transactions on Vehicular Technology* 70 (2021), 7413–7425.

[52] Xiang Huo and Mingxi Liu. 2022. Distributed privacy-preserving electric vehicle charging control based on secret sharing. *Electric Power Systems Research* 211 (2022), 108357.

[53] Siam Umar Hussain and Farinaz Koushanfar. 2018. P3: Privacy Preserving Positioning for Smart Automotive Systems. *ACM Trans. Des. Autom. Electron. Syst.* 23, 6, Article 79 (Nov 2018), 19 pages.

[54] Hongbo Jiang, Jie Li, Ping Zhao, Fanzi Zeng, Zhu Xiao, and Arun Iyengar. 2021. Location Privacy-preserving Mechanisms in Location-based Services. *ACM Computing Surveys (CSUR)* 54 (2021), 1 – 36.

[55] Frank Kargl, Arik Friedman, and Roksana Boreli. 2013. Differential privacy in intelligent transportation systems. In *Wireless Network Security*.

[56] Hassan Karim and Danda B. Rawat. 2022. TollsOnly Please—Homomorphic Encryption for Toll Transponder Privacy in Internet of Vehicles. *IEEE Internet of Things Journal* 9, 4 (2022), 2627–2636.

[57] Banashri Karmakar, Shyam Murthy, Arpita Patra, and Protik Paul. 2024. QuickPool: Privacy-Preserving Ride-Sharing Service. *IACR Cryptol. ePrint Arch.* 2024 (2024), 1109.

[58] Marcel Keller. 2020. MP-SPDZ: A Versatile Framework for Multi-Party Computation. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*.

[59] Qinglei Kong, Rongxing Lu, Maode Ma, and Haiyong Bao. 2017. Achieve Location Privacy-Preserving Range Query in Vehicular Sensing. *Sensors* 17, 8 (2017), 16 pages. https://www.mdpi.com/1424-8220/17/8/1829

[60] Qinglei Kong, Rongxing Lu, Feng Yin, and Shuguang Cui. 2021. Privacy-Preserving Continuous Data Collection for Predictive Maintenance in Vehicular Fog-Cloud. *IEEE Transactions on Intelligent Transportation Systems* 22, 8 (2021), 5060–5070.

[61] Qinglei Kong, Feng Yin, Rongxing Lu, Beibei Li, Xiaohong Wang, Shuguang Cui, and Ping Zhang. 2021. Privacy-Preserving Aggregation for Federated Learning-Based Navigation in Vehicular Fog. *IEEE Transactions on Industrial Informatics* 17, 12 (2021), 8453–8463.

[62] Deepak Kumaraswamy, Shyam Murthy, and Srinivas Vivek. 2021. Revisiting Driver Anonymity in ORide. *ArXiv* abs/2101.06419 (2021).

[63] Runchuan Li, Zhiquan Liu, Yong Ma, Yunni Xia, Yudan Cheng, Lin Wan, and Jianfeng Ma. 2023. RPPM: A Reputation-Based and Privacy-Preserving Platoon Management Scheme in Vehicular Networks. *IEEE Transactions on Intelligent Transportation Systems* (2023), 1–14.

[64] Xiaoguo Li, Bowen Zhao, Guomin Yang, Tao Xiang, Jian Weng, and Robert H. Deng. 2023. A Survey of Secure Computation Using Trusted Execution Environments. (2023). arXiv:2302.12150 [cs.CR]

[65] Yiran Li, Hongwei Li, Guowen Xu, Tao Xiang, and Rongxing Lu. 2022. Practical Privacy-Preserving Federated Learning in Vehicular Fog Computing. *IEEE Transactions on Vehicular Technology* 71, 5 (2022), 4692–4705.

[66] Yijing Li, Xiaofeng Tao, Xuefei Zhang, Junjie Liu, and Jin Xu. 2021. Privacy-Preserved Federated Learning for Autonomous Driving. *IEEE Transactions on Intelligent Transportation Systems* 23 (2021), 8423–8434.

[67] Zengpeng Li, Mamoun Alazab, Sahil Garg, and M. Shamim Hossain. 2021. PriParkRec: Privacy-Preserving Decentralized Parking Recommendation Service. *IEEE Transactions on Vehicular Technology* 70, 5 (2021), 4037–4050.

[68] Hsiao-Ying Lin and Wen-Guey Tzeng. 2005. An Efficient Solution to the Millionaires' Problem Based on Homomorphic Encryption. *IACR Cryptol. ePrint Arch.* 2005 (2005), 43.

[69] Yehuda Lindell and Benny Pinkas. 2011. Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. *Journal of Cryptology* 25 (2011), 680–722.

[70] Dengzhi Liu, Geng Yu, Yongdong Ding, Zhaoman Zhong, and Chen Wang. 2024. Privacy Preserving Multi-Party Computation With Secret Sharing for Trajectory Prediction in VANETs. *IEEE Transactions on Vehicular Technology* 73 (2024), 18666–18677.

[71] Mingming Liu, Long Cheng, Yingqi Gu, Ying Wang, Qingzhi Liu, and Noel E. O'Connor. 2022. MPC-CSAS: Multi-Party Computation for Real-Time Privacy-Preserving Speed Advisory Systems. *IEEE Transactions on Intelligent Transportation Systems* 23, 6 (2022), 5887–5893.

[72] Mingyu Liu, Ekim Yurtsever, Jonathan Fossaert, Xingcheng Zhou, Walter Zimmer, Yuning Cui, Bare Luka Žagar, and Alois Knoll. 2024. A Survey on Autonomous Driving Datasets: Statistics, Annotation Quality, and a Future Outlook. *IEEE Transactions on Intelligent Vehicles* 9 (2024), 7138–7164.

[73] Yibiao Lu, Bingsheng Zhang, and Kui Ren. 2024. Maliciously Secure MPC From Semi-Honest 2PC in the Server-Aided Model. *IEEE Transactions on Dependable and Secure Computing* 21 (2024), 3109–3125.

[74] Yuchuan Luo, Shaojing Fu, Xiaohua Jia, Ming Xu, and Yingwen Chen. 2023. P2Ride: Practical and Privacy-Preserving Ride-Matching Scheme for Ridesharing. *IEEE Transactions on Intelligent Transportation Systems* 24, 3 (2023), 3584–3593.

[75] Yuchuan Luo, Xiaohua Jia, Shaojing Fu, and Ming Xu. 2019. pRide: Privacy-Preserving Ride Matching Over Road Networks for Online Ride-Hailing Service. *IEEE Transactions on Information Forensics and Security* 14, 7 (2019), 1791–1802.

[76] Naercio Magaia, Carlos Borrego, Paulo Rogério Pereira, and Miguel Correia. 2018. ePRIVO: An Enhanced PRIvacy-preserVing Opportunistic Routing Protocol for Vehicular Delay-Tolerant Networks. *IEEE Transactions on Vehicular Technology* 67, 11 (2018), 11154–11168.

[77] Mohamad Mansouri, Melek Önen, Wafa Ben Jaballah, and Mauro Conti. 2023. SoK: Secure Aggregation Based on Cryptographic Schemes for Federated Learning. *Proc. Priv. Enhancing Technol.* 2023 (2023), 140–157.

[78] Daniel Morales, Isaac Agudo, and Javier Lopez. 2023. Private set intersection: A systematic literature review. *Computer Science Review* 49 (2023), 100567.

[79] Pratyay Mukherjee and Daniel Wichs. 2016. Two Round Multiparty Computation via Multi-key FHE. In *Advances in Cryptology – EUROCRYPT 2016*, Marc Fischlin and Jean-Sébastien Coron (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 735–763.

[80] Pravin Mundhe, Shekhar Verma, and S. Venkatesan. 2021. A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Computer Science Review* 41 (2021), 100411.

[81] Shyam Murthy and Srinivas Vivek. 2022. Driver Locations Harvesting Attack on pRide. In *International Conference on Network and System Security*.

[82] Shyam Murthy and Srinivas Vivek. 2022. Passive Triangulation Attack on ORide. *ArXiv* abs/2208.12216 (2022).

[83] Mohamed Nabeel, Stefan Appel, Elisa Bertino, and Alejandro P. Buchmann. 2013. Privacy Preserving Context Aware Publish Subscribe Systems. In *International Conference on Network and System Security*.

[84] Boel Nelson and Tomas Olovsson. 2017. Introducing Differential Privacy to the Automotive Domain: Opportunities and Challenges. *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)* (2017), 1–7.

[85] Lucien K. L. Ng and Sherman S. M. Chow. 2023. SoK: Cryptographic Neural-Network Computation. *2023 IEEE Symposium on Security and Privacy (SP)* (2023), 497–514.

[86] Elena Pagnin, Gunnar Gunnarsson, Pedram Talebi, Claudio Orlandi, and Andrei Sabelfeld. 2019. TOPPool: Time-aware Optimized Privacy-Preserving Ridesharing. *Proceedings on Privacy Enhancing Technologies* 2019 (2019), 93–111.

[87] Pascal Paillier. 1999. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *International Conference on the Theory and Application of Cryptographic Techniques*.

[88] Tao Peng, Wentao Zhong, Guojun Wang, Entao Luo, Shui Yu, Yining Liu, Yi Yang, and Xuyun Zhang. 2024. Privacy-Preserving Truth Discovery Based on Secure Multi-Party Computation in Vehicle-Based Mobile Crowdsensing. *IEEE Transactions on Intelligent Transportation Systems* 25 (2024), 7767–7779.

[89] Mert D. Pesé, Xiaoying Pu, and Kang G. Shin. 2020. SPy: Car Steering Reveals Your Trip Route! *Proceedings on Privacy Enhancing Technologies* 2020 (2020), 155 – 174.

[90] Anh Pham, Italo Dacosta, Guillaume Endignoux, Juan Ramon Troncoso Pastoriza, Kevin Huguenin, and Jean-Pierre Hubaux. 2017. ORide: A Privacy-Preserving yet Accountable Ride-Hailing Service. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, BC, 1235–1252.

[91] Benny Pinkas, T. Schneider, and Michael Zohner. 2014. Faster Private Set Intersection Based on OT Extension. In *USENIX Security Symposium*.

[92] Shiva Raj Pokhrel, Youyang Qu, Surya Nepal, and Surjit Singh. 2021. Privacy-Aware Autonomous Valet Parking: Towards Experience Driven Approach. *IEEE Transactions on Intelligent Transportation Systems* 22, 8 (2021), 5352–5363.

[93] Chenxi Qiu, Anna Squicciarini, Ce Pang, Ning Wang, and Ben Wu. 2022. Location Privacy Protection in Vehicle-Based Spatial Crowdsourcing via Geo-Indistinguishability. *IEEE Transactions on Mobile Computing* 21, 7 (2022), 2436–2450.

[94] Nicolas Quero, Aymen Boudguiga, Renaud Sirdey, and Nadir Karam. 2023. Towards Privacy-Preserving Platooning Services by means of Homomorphic Encryption. In *Symposium on Vehicle Security and Privacy (VehicleSec) 2023*. Internet Society, San Diego, CA, USA, 7 pages.

[95] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 26 (1978), 96–99.

[96] Hajira Saleem, Faisal Riaz, Leonardo Mostarda, Muaz A. Niazi, Ammar Rafiq, and Saqib Saeed. 2021. Steering Angle Prediction Techniques for Autonomous Ground Vehicles: A Review. *IEEE Access* 9 (2021), 78567–78585.

[97] Berry Schoenmakers. 1999. A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. In *Advances in Cryptology — CRYPTO' 99*, Michael Wiener (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 148–164.

[98] Adi Shamir. 1979. How to share a secret. *Commun. ACM* 22, 11 (Nov 1979), 612–613.

[99] Prinkle Sharma and Hong Liu. 2021. A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles. *IEEE Internet of Things Journal* 8, 6 (2021), 4991–4999.

[100] Markus Stadler. 1996. Publicly Verifiable Secret Sharing.

[101] Wei Sun and Kannan Srinivsan. 2023. Reminding Drivers of the Stalking Vehicles on the Road. *Proceedings Inaugural International Symposium on Vehicle Security & Privacy* (2023).

[102] Xiaoqiang Sun, F. Richard Yu, Peng Zhang, Weixin Xie, and Xiang Peng. 2020. A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks. *Sensors* 20, 15 (2020), 31 pages.

[103] Kartick Sutradhar, Beena G Pillai, Ruhul Amin, and Dayanand Lal Narayan. 2024. A survey on privacy-preserving authentication protocols for secure vehicular communication. *Comput. Commun.* 219 (2024), 1–18.

[104] Iraklis Symeonidis, Abdelrahaman Aly, Mustafa Asan Mustafa, Bart Mennink, Siemen Dhooghe, and Bart Preneel. 2017. SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision. In *Computer Security – ESORICS 2017*, Simon N. Foley, Dieter Gollmann, and Einar Snekkenes (Eds.). Springer International Publishing, Cham, 475–493.

[105] Iraklis Symeonidis, Dragos Rotaru, Mustafa A. Mustafa, Bart Mennink, Bart Preneel, and Panos Papadimitratos. 2022. HERMES: Scalable, Secure, and Privacy-Enhancing Vehicular Sharing-Access System. *IEEE Internet of Things Journal* 9, 1 (2022), 129–151.

[106] Arnaud Grivet Sébert, Renaud Sirdey, Oana Stan, and Cédric Gouy-Pailler. 2022. Protecting Data from all Parties: Combining FHE and DP in Federated Learning. arXiv:2205.04330 [cs.CR]

[107] Zheng Tan, Cheng Wang, Mengchu Zhou, and Luomeng Zhang. 2018. Private information retrieval in vehicular location-based services. *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (2018), 56–61.

[108] Francis Jerome Tiausas, K. Yasumoto, Jose Paolo Talusan, Hayato Yamana, Hirozumi Yamaguchi, Shameek Bhattacharjee, Abhishek Dubey, and Sajal K. Das. 2023. HPRoP: Hierarchical Privacy-preserving Route Planning for Smart Cities. *ACM Transactions on Cyber-Physical Systems* 7 (2023), 1 – 25.

[109] Aashma Uprety, Danda B. Rawat, and Jiang Li. 2021. Privacy Preserving Misbehavior Detection in IoV Using Federated Machine Learning. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, Las Vegas, NV, USA, 1–6.

[110] Meghana Vargheese and Srinivas Vivek. 2023. Attack on the Privacy-Preserving Carpooling Service TAROT. In *International Conferences on Information Science and System*.

[111] Visual Capitalist Team. 2023. Network Overload. https://www.visualcapitalist.com/network-overload/ Accessed: Aug 15, 2023.

[112] Srinivas Vivek. 2021. Attacks on a Privacy-Preserving Publish-Subscribe System and a Ride-Hailing Service. In *IMA Conference on Cryptography and Coding*.

[113] Nan Wang, Sid Chi-Kin Chau, and Yue Zhou. 2021. Privacy-Preserving Energy Storage Sharing with Blockchain. *Proceedings of the Twelfth ACM International Conference on Future Energy Systems* (2021).

[114] Xianmin Wang, Xiaohui Kuang, Jin Li, Jing Li, Xiaofeng Chen, and Zheli Liu. 2021. Oblivious Transfer for Privacy-Preserving in VANET's Feature Matching. *IEEE Transactions on Intelligent Transportation Systems* 22 (2021), 4359–4366.

[115] Ami Woo, Baris Fidan, and William W. Melek. 2018. Localization for Autonomous Driving. In *Handbook of Position Location: Theory, Practice, and Advances* (2nd ed.), Seyed A. (Reza) Zekavat and R. Michael Buehrer (Eds.). John Wiley & Sons, Ltd, Hoboken, NJ, USA, Chapter 29, 1051–1087.

[116] Songqi Wu, Jin Li, Fenghui Duan, Yueming Lu, Xu Zhang, and Jiefu Gan. 2021. The Survey on the development of Secure Multi-Party Computing in the blockchain. In *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*. 1–7.

[117] Yan Wu, Can Zhang, and Liehuang Zhu. 2023. Privacy-Preserving and Traceable Blockchain-Based Charging Payment Scheme for Electric Vehicles. *IEEE Internet of Things Journal* 10 (2023), 21254–21265.

[118] Jinbo Xiong, Renwan Bi, Youliang Tian, Ximeng Liu, and Dapeng Wu. 2022. Toward Lightweight, Privacy-Preserving Cooperative Object Classification for Connected Autonomous Vehicles. *IEEE Internet of Things Journal* 9, 4 (2022), 2787–2801.

[119] Jinbo Xiong, Renwan Bi, Mingfeng Zhao, Jingda Guo, and Qing Yang. 2020. Edge-Assisted Privacy-Preserving Raw Data Sharing Framework for Connected Autonomous Vehicles. *IEEE Wireless Communications* 27, 3 (2020), 24–30.

[120] Zuobin Xiong, Zhipeng Cai, Qilong Han, Arwa Alrawais, and Wei Li. 2021. ADGAN: Protect Your Location Privacy in Camera Data of Auto-Driving Vehicles. *IEEE Transactions on Industrial Informatics* 17, 9 (2021), 6200–6210.

[121] Zuobin Xiong, Wei Li, Qilong Han, and Zhipeng Cai. 2019. Privacy-Preserving Auto-Driving: A GAN-Based Approach to Protect Vehicular Camera Data. In *2019 IEEE International Conference on Data Mining (ICDM)*. IEEE, Beijing, China, 668–677.

[122] Guowen Xu, Hongwei Li, Sen Liu, Kan Yang, and Xiaodong Lin. 2020. VerifyNet: Secure and Verifiable Federated Learning. *IEEE Transactions on Information Forensics and Security* 15 (2020), 911–926.

[123] Qi Xu, Hui Zhu, Yandong Zheng, Jiaqi Zhao, Rongxing Lu, and Hui Li. 2022. An Efficient and Privacy-Preserving Route Matching Scheme for Carpooling Services. *IEEE Internet of Things Journal* 9 (2022), 19890–19902.

[124] Zihui Xu, Lei Wu, Chengyi Qin, Su Li, Songnian Zhang, and Rongxing Lu. 2023. PriTAEC: Privacy-Preserving Task Assignment Based on Oblivious Transfer and Edge Computing in VANET. *IEEE Transactions on Vehicular Technology* 72, 4 (2023), 4996–5009.

[125] Yang Yang, Xindi Huang, Ximeng Liu, Hongju Cheng, Jian Weng, Xiangyang Luo, and Victor Chang. 2019. A Comprehensive Survey on Secure Outsourced Computation and Its Applications. *IEEE Access* 7 (2019), 159426–159465.

[126] Andrew C. Yao. 1982. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)*. IEEE, Chicago, IL, USA, 160–164.

[127] Andrew Chi-Chih Yao. 1986. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (SFCS 1986)*. IEEE, Toronto, ON, Canada, 162–167.

[128] Zuobin Ying, Shuanglong Cao, Ximeng Liu, Zhuo Ma, Jianfeng Ma, and Robert H. Deng. 2022. PrivacySignal: Privacy-Preserving Traffic Signal Control for Intelligent Transportation System. *IEEE Transactions on Intelligent Transportation Systems* 23, 9 (2022), 16290–16303.

[129] Takahito Yoshizawa, Dave Singelée, Jan Tobias Mühlberg, Stéphane Delbruel, Amirhosein Taherkordi, Danny Hughes, and Bart Preneel. 2022. A Survey of Security and Privacy Issues in V2X Communication Systems. *Comput. Surveys* 55 (2022), 1 – 36.

[130] Haining Yu, Xiaohua Jia, Hongli Zhang, and Jiangang Shu. 2022. Efficient and Privacy-Preserving Ride Matching Using Exact Road Distance in Online Ride Hailing Services. *IEEE Transactions on Services Computing* 15 (2022), 1841–1854.

[131] Haining Yu, Xiaohua Jia, Hongli Zhang, Xiangzhan Yu, and Jiangang Shu. 2021. PSRide: Privacy-Preserving Shared Ride Matching for Online Ride Hailing Systems. *IEEE Transactions on Dependable and Secure Computing* 18, 3 (2021), 1425–1440.

[132] Haining Yu, Jiangang Shu, Xiaohua Jia, Hongli Zhang, and Xiangzhan Yu. 2019. lpRide: Lightweight and Privacy-Preserving Ride Matching Over Road Networks in Online Ride Hailing Systems. *IEEE Transactions on Vehicular Technology* 68 (2019), 10418–10428.

[133] Haining Yu, Hongli Zhang, Xiangzhan Yu, Xiaojiang Du, and Mohsen Guizani. 2021. PGRide: Privacy-Preserving Group Ridesharing Matching in Online Ride Hailing Services. *IEEE Internet of Things Journal* 8, 7 (2021), 5722–5735.

[134] Yantao Yu, Xiaoping Xue, Jingxiao Ma, Ellen Z. Zhang, Yunguo Guan, and Rongxing Lu. 2024. Efficient Privacy-Preserving Task Allocation With Secret Sharing for Vehicular Crowdsensing. *IEEE Internet of Things Journal* 11 (2024), 9473–9486.

[135] Minghao Yuan, Dongdong Wang, Feng Zhang, Shenqing Wang, Shan Ji, and Yongjun Ren. 2022. An Examination of Multi-Key Fully Homomorphic Encryption and Its Applications. *Mathematics* 10, 24 (2022), 20 pages.

[136] Farkhanda Zafar, Hasan Ali Khattak, Moayad Aloqaily, and Rasheed Hussain. 2022. Carpooling in Connected and Autonomous Vehicles: Current Solutions and Future Directions. *ACM Computing Surveys (CSUR)* 54 (2022), 1 – 36.

[137] Chuan Zhang, Liehuang Zhu, Jianbing Ni, Cheng Huang, and Xuemin Shen. 2020. Verifiable and Privacy-Preserving Traffic Flow Statistics for Advanced Traffic Management Systems. *IEEE Transactions on Vehicular Technology* 69, 9 (2020), 10336–10347.

[138] Can Zhang, Liehuang Zhu, and Chang Xu. 2023. BSDP: Blockchain-Based Smart Parking for Digital-Twin Empowered Vehicular Sensing Networks With Privacy Protection. *IEEE Transactions on Industrial Informatics* 19 (2023), 7237–7246.

[139] Chuan Zhang, Liehuang Zhu, Chang Xu, Kashif Sharif, Kai Ding, Ximeng Liu, Xiaojiang Du, and Mohsen Guizani. 2022. TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET. *IEEE Transactions on Services Computing* 15, 2 (2022), 806–818.

[140] En Zhang, Feng-Hao Liu, Qiqi Lai, Ganggang Jin, and Yu Li. 2019. Efficient Multi-Party Private Set Intersection Against Malicious Adversaries. *Proceedings of the 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop* (2019).

[141] Juyuan Zhang, Licheng Wang, Xiaoya Hu, Rui Li, and Shihui Zheng. 2023. Privacy-preserving Online Ride-hailing Service System Based on Taking the Intersection of Private sets of Points of Interest. *2023 International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS)* (2023), 107–117.

[142] Junwei Zhang, Fan Yang, Zhuo Ma, Zhuzhu Wang, Ximeng Liu, and Jianfeng Ma. 2021. A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems* 22, 4 (2021), 2299–2313.

[143] Lu Zhang, Wenhao Gao, Shukai Chen, Wei Ren, Kim-Kwang Raymond Choo, and Naixue N. Xiong. 2022. A Privacy-Preserving Proximity Testing Using Private Set Intersection for Vehicular Ad-Hoc Networks. *IEEE Transactions on Industrial Informatics* 18 (2022), 7373–7383.

[144] Pengbo Zhang and Zhixin Yang. 2018. A Novel AdaBoost Framework With Robust Threshold and Structural Optimization. *IEEE Transactions on Cybernetics* 48 (2018), 64–76.

[145] Qiao Zhang, Chunsheng Xin, and Hongyi Wu. 2021. Privacy-Preserving Deep Learning Based on Multiparty Secure Computation: A Survey. *IEEE Internet of Things Journal* 8 (2021), 10412–10429.

[146] Ping Zhao, Guanglin Zhang, Shaohua Wan, Gaoyang Liu, and Tariq Umer. 2019. A survey of local differential privacy for securing internet of vehicles. *The Journal of Supercomputing* 76 (2019), 8391 – 8412.

[147] Changli Zhou, Tian Wang, Hui Tian, Wenxian Jiang, and Zhijian Wang. 2020. A Top-K Query Scheme With Privacy Preservation for Intelligent Vehicle Network in Mobile IoT. *IEEE Access* 8 (2020), 81698–81710.

[148] Ian Zhou, Farzad Tofigh, Massimo Piccardi, Mehran Abolhasan, Daniel Robert Franklin, and Justin Lipman. 2024. Secure Multi-Party Computation for Machine Learning: A Survey. *IEEE Access* 12 (2024), 53881–53899.

[149] Jun Zhou, Shiying Chen, Kim-Kwang Raymond Choo, Zhenfu Cao, and Xiaolei Dong. 2021. EPNS: Efficient Privacy-Preserving Intelligent Traffic Navigation From Multiparty Delegated Computation in Cloud-Assisted VANETs. *IEEE Transactions on Mobile Computing* 22 (2021), 1491–1506. https://api.semanticscholar.org/CorpusID:239645137

[150] Liehuang Zhu, Meng Li, Zijian Zhang, and Zhan Qin. 2020. ASAP: An Anonymous Smart-Parking and Payment Scheme in Vehicular Networks. *IEEE Transactions on Dependable and Secure Computing* 17, 4 (2020), 703–715.