计算机科学
COMPUTER SCIENCE

车联网边缘服务场景下的隐私保护计算:技术基础与研究进展综述

李佳惠, 李英龙, 陈铁明

引用本文

李佳惠, 李英龙, 陈铁明. 车联网边缘服务场景下的隐私保护计算:技术基础与研究进展综述[J]. 计算机科学, 2026, 53(1): 298-322.

LI Jiahui, LI Yinglong, CHEN Tieming. Privacy-preserving Computation in Edge Service Scenario of Internet of Vehicles:A Review ofTechnical Basis and Research Progress [J]. Computer Science, 2026, 53(1): 298-322.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

面向5G城市交通的轻量级安全认证和密钥更新方案

Lightweight Secure Authentication and Key Update Scheme for 5G Urban Transportation

计算机科学, 2025, 52(12): 331-338. https://doi.org/10.11896/jsjkx.241100093

一种对时延敏感的去中心化联邦学习算法

Decentralized Federated Learning Algorithm Sensitive to Delay

计算机科学, 2025, 52(12): 314-320. https://doi.org/10.11896/jsjkx.241100085

解决联邦学习Non-IID问题的基础模型方法综述

Research on Foundation Model Methods for Addressing Non-IID Issues in Federated Learning

计算机科学, 2025, 52(12): 302-313. https://doi.org/10.11896/jsjkx.241200056

面向图垂直联邦学习的对抗攻击方法

Adversarial Attack on Vertical Graph Federated Learning

计算机科学, 2025, 52(11A): 241200220-10. https://doi.org/10.11896/jsjkx.241200220

基于知识蒸馏的联邦学习后门攻击方法

Backdoor Attack Method for Federated Learning Based on Knowledge Distillation

计算机科学, 2025, 52(11): 434-443. https://doi.org/10.11896/jsjkx.250100146

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250200113

车联网边缘服务场景下的隐私保护计算:技术基础与研究进展综述

李佳惠[1]　李英龙[1]　陈铁明[1,2]
1 浙江工业大学计算机科学与技术学院、软件学院　杭州 310023
2 浙江工业大学地理信息学院　杭州 310014
(211122120082@zjut.edu.cn)

摘　要　随着智能汽车、边缘计算与无线通信技术的深度融合,“车-路-云”协同的智能车联网边缘服务体系快速发展,通过实时数据处理优化了交通效率与驾驶安全性。然而,开放边缘网络环境下海量车辆感知数据(如位置轨迹、驾驶行为)的交互与计算,面临窃听攻击和推理攻击等隐私泄露风险。虽然现有的隐私保护方案逐步增强了隐私保护效果,但车联网边缘环境下的动态拓扑与资源受限等特性,使得隐私保护强度与服务性能存在矛盾。隐私保护计算作为一种有效的隐私保护手段,对于维护用户的个人权益以及促进车联网产业的可持续发展具有重要意义,已成为保障车联网服务的关键研究领域之一。首先,概述了车联网边缘服务架构,并分析了其中潜在的隐私泄露风险。然后,根据隐私保护计算技术的不同机制,分类探讨了基于数据变换、安全多方计算、联邦学习和可信执行环境技术的车联网隐私保护计算方法。在此基础上,从隐私泄露风险、数据效用、开销和可扩展性4个关键评价维度出发,对隐私保护计算技术在车联网中的实际应用进行了系统性的分析与比较,可以更清晰地了解不同隐私保护计算方法在车联网中的优势、局限性和适用场景。此外,还阐述了相应的优化策略,为未来的研究和实践提供参考和指导。最后,探讨了未来车联网隐私保护计算的研究切入点和问题的解决思路。

关键词:车联网;边缘服务;隐私保护计算;差分隐私;模糊泛化;安全多方计算;联邦学习;可信执行环境
中图分类号　TP391

Privacy-preserving Computation in Edge Service Scenario of Internet of Vehicles:A Review of Technical Basis and Research Progress

LI Jiahui[1],LI Yinglong[1] and CHEN Tieming[1,2]
1 College of Computer Science and Technology,Zhejiang University of Technology,Hangzhou 310023,China
2 College of Geoinformatics,Zhejiang University of Technology,Hangzhou 310014,China

Abstract　With the deep integration of intelligent vehicles,edge computing,and wireless communication technologies,the “vehicle-road-cloud” collaborative intelligent IoV edge service system is rapidly developing,optimizing traffic efficiency and driving safety through real-time data processing. However,the interaction and computation of massive vehicle perception data(such as location trajectories and driving behaviors) in an open edge network environment face privacy leakage risks such as eavesdropping attacks and inference attacks. Although the existing privacy protection schemes have gradually enhanced the effect of privacy protection,the characteristics of dynamic topology and resource constraints in the edge environment of the IoV create a conflict between the strength of privacy protection and service performance. Privacy-preserving computation,as an effective means of privacy protection,is of significant importance for safeguarding users' personal rights and promoting the sustainable development of the IoV industry,and has become one of the key research areas for ensuring the services in the IoV. Initially,it outlines the edge service architecture of IoV and analyzes the potential privacy leakage risks within it. Subsequently,based on the different mechanisms of privacy-preserving computation technologies,it categorizes and discusses the privacy-preserving computation methods for IoV based on data transformation,secure multi-party computation,federated learning,and trusted execution environment technologies. On this basis,a systematic analysis and comparison of these privacy-preserving computation methods are conducted from four key evaluation dimensions:privacy leakage risk,data utility,overhead,and scalability,along with corresponding optimization strategies. Finally,the challenges faced by privacy-preserving computation technologies for IoV edge services and future research directions are discussed.

到稿日期:2025-02-27　返修日期:2025-05-24
基金项目:国家自然科学基金重点项目(U22B2028);浙江省自然科学基金探索/重大项目(LY23F020022,LD22F020002)
This work was supported by the National Natural Science Foundation of China(U22B2028) and Natural Science Foundation of Zhejiang Province,China(LY23F020022,LD22F020002).
通信作者:李英龙(liyinglong@zjut.edu.cn)

Keywords Internet of vehicles, Edge services, Privacy-preserving computation, Differential privacy, Fuzzy generalization, Secure multi-party computation, Federated learning, Trusted execution environment

1 引言

车联网(Internet of Vehicles, IoV)概念源于物联网(Internet of Things, IoT)，它以行驶中的车辆作为信息感知对象，借助新一代信息通信技术，实现车辆到万物(Vehicle to Everything, V2X, X包括车辆、路侧单元、行人等多维度)的实时信息交互[1]，成为智能交通与自动驾驶系统的核心组成部分。当前，全球车联网市场正处于高速扩张期，中国商用车车联网市场预计2025年将达到806亿元。这一增长，得益于新能源汽车的普及和政策扶持(如《新能源汽车产业发展规划(2021－2035年)》《交通强国建设纲要》)。

随着边缘计算(Edge Computing, EC)和云计算在车联网中的角色和功能的不断拓展和相互作用[2-3]，车联网服务面临越来越多的潜在风险，其中隐私泄露风险尤为严峻[4]。尽管车联网边缘计算通过将传统的云计算任务下沉至边缘侧，能够降低对中心服务器的依赖，为解决隐私保护和计算效率问题提供了一条有效途径[5]，但是在车联网开放、动态的运行环境下，如何兼顾数据全生命周期的隐私保护与智能边缘服务性能的需求面临着诸多挑战。

传统的隐私保护方案通常依赖于加密、身份认证和匿名等技术手段[6]，难以满足实时而可靠的车联网边缘服务要求[7]。以匿名技术为例，匿名通信虽然能够保护用户的身份隐私，但可能会给恶意用户的冒充攻击留下可乘之机，因此通常需要结合匿名认证机制进行使用，以确保通信过程的安全性和用户身份的真实性[8]。此外，数据匿名化并传输给第三方后，也无法控制数据使用者使用，且容易受到链接攻击和差分攻击。相比之下，隐私保护计算则是一种针对数据生命周期各个阶段的隐私保护技术，能够保证数据在不暴露其具体内容的前提下被充分利用[9]，涵盖了数据变换、秘密分享、安全多方计算、联邦学习及可信执行环境等多种技术。然而，在车联网边缘服务架构中，部署隐私保护计算技术仍面临诸多复杂挑战，特别是在多种网络和服务平台互联互通的环境下，隐私攻击呈现多途径、强隐蔽性和高防控复杂度的特点，这极大地增加了隐私保护的难度。

从车联网服务场景来看，车联网边缘环境中的终端设备众多[10]，数据来源广、规模大，且车联网设备具有动态移动性、硬件异构性、通信能力弱、不可信任等特点[11]。这种大规模、动态变化的车联网环境对隐私保护计算技术提出了更高的要求，尤其是在可扩展性方面。对于实时性要求较高的服务[12]，如自动驾驶辅助，可能需要选择计算效率较高的隐私保护计算技术，以确保数据处理的及时性。因此，如何选择和运用合适的、可扩展的隐私保护计算技术，以保障数据在采集、存储和计算等过程中的隐私性，成为亟待解决的难题。

从数据效用角度来看，隐私保护计算技术可能会对数据质量和可用性产生负面影响。在车联网边缘服务中，服务提供方希望收集到可用的原始车联网数据，而用户却要求其敏感数据得到保护。这种隐私保护能力与数据效用之间的矛盾，是在应用隐私保护计算技术时必须面对的问题。例如，差分隐私技术通过引入噪声，虽然降低了数据泄露的风险，但也降低了数据精度。因此，在不同的服务需求下，选择既能满足数据所有者的隐私保护要求，又能最大程度地保证边缘服务的数据效用需求的隐私保护计算技术[13]，是一大挑战。

从通信与计算资源角度来讲，车联网中的车辆和设备通常具有有限的通信和计算资源，而部分隐私保护计算技术需要大量的计算和通信开销，这可能会对车联网中的设备造成沉重的负担[14]。例如，联邦学习需要参与节点(包括车辆、边缘服务器等)之间的通信以共享模型参数，这可能会消耗大量的通信资源。此外，频繁的通信还会增加数据被攻击或窃取的可能性。再者，隐私保护计算技术的应用方式和效果也会对车联网边缘服务质量产生不同程度的影响。因此，如何平衡隐私保护开销和车联网资源是一个挑战。

1.1 相关综述

当前已有不少与车联网直接或间接关联的隐私保护计算研究综述，它们各有侧重。例如，Ghosal等[15]在2020年的工作仅限于对称密码学。Huang等[16]分析了基于密码学和基于信任的方案，并较为详细地阐述了身份和位置隐私保护方案，但对数据共享的讨论相对较少。Lu等[17]对5G V2X服务的信任、安全和隐私问题及关键策略进行了自上而下的探讨，但未比较各方案的开销。2022年，Moya等[18]介绍了IoV在5G和6G以外的安全和隐私方面的问题，探讨了网络软件化、区块链、人工智能/机器学习、物理层安全等技术在6G中的未来前景。Sedar等[19]从主动与被动防御的安全机制分类出发，探讨了人工智能和机器学习的安全潜力。Deng等[20]基于车联网的体系结构以及车联网隐私保护的保护对象，对各方案进行了分析。Liu等[21]聚焦车联网隐私保护数据聚合。2023年，Zhang等[22]面向边缘智能，从联邦学习技术角度进行分析展望。2024年，Haddaji等[23]基于IoV中的安全和隐私漏洞进行讨论分析。Abidi等[24]特别关注应用程序上下文中使用的信任管理模型的要求。Li等[25]从不可链接性、假名性、匿名性、不可检测性、不可观察性几个方面对车联网隐私保护解决方案进行分析与总结。而对于车联网边缘服务而言，数据效用、计算开销、通信开销同样值得关注。

尽管已有大量研究对车联网、隐私保护技术进行了探讨，但现有综述尚未对隐私保护计算技术在车联网中的应用进行全面概述。此外，在对各项技术的优势、不足及优化路线的比较分析方面，仍存在进一步完善的空间，特别是车联网服务涉及到的性能问题。

1.2 本文贡献

本文从车联网边缘网络环境下的隐私泄露风险威胁角度出发，为理解隐私保护计算技术的必要性做铺垫，之后对隐私保护计算技术的优点及主流技术进行了简要介绍，接着阐述了车联网边缘服务融合隐私保护计算所面临的挑战及目标，并着重对已有相关研究（截至 2025 年 2 月在线公开的）中具有代表性的方法进行了对比分析。

1.3 文章结构

本文第 1 章介绍与车联网隐私保护计算相关的综述研究工作，通过分析现有综述研究的不足，指出了本文工作的重要性和必要性；第 2 章对车联网边缘架构及服务中存在的隐私安全问题进行探讨，并明确了隐私保护计算的优势以及车联网边缘隐私保护计算方案设计的目标和原则；第 3—6 章依据第 2.2.2 节的主要研究方向，从数据机密性、数据效用、开销、可扩展性角度对车联网实际应用中各隐私保护计算的研究工作进行了综述及比较分析，并深入探讨了在车联网场景下实施隐私保护计算时所面临的挑战；第 7 章提出了可能的未来研究方向和解决方案。

2 车联网边缘服务及隐私保护计算

在进行车联网边缘隐私保护计算相关技术的综述调研之前，本章先介绍车联网边缘服务架构及隐私保护计算方面的背景知识，以便读者更好地理解隐私保护计算在车联网边缘服务中的关键作用。

2.1 车联网边缘服务及隐私泄露风险

2.1.1 车联网边缘服务

车联网边缘服务是车联网架构的关键组成部分。边缘服务涵盖多种服务类型，包括交通信息服务（如实时交通信息推送、车辆状态查询等）[26]、道路安全服务（如碰撞预警、车道驾驶辅助等）和通行效率服务（如交通流量优化、智能停车引导等）[13]。这些服务对智能交通和智慧城市管理有着重要的经济价值和社会效益，可显著提升道路效率、驾驶安全和驾驶体验。然而，由此产生的海量车联网数据采集、存储、传输和融合不仅从负面影响了边缘服务质量的实时性，也增加了隐私泄露风险。车联网边缘服务架构通过利用边缘计算技术，将计算和存储资源部署在靠近车辆和用户的边缘节点，如路侧单元（Road Side Unit，RSU）或基站上，使得车辆与车联网智能服务融合得更加紧密[27]，从而在降低延迟响应和增强隐私保护等方面发挥了积极作用[28]。

车联网边缘服务架构可划分为感知控制层、网络传输层以及综合应用层（见图 1）。其中，感知控制层由车内传感器、路网感知器组成，它们通过协同感知将采集的数据反馈给配备智能车载系统的车辆；网络传输层基于 V2X 通信方式，实现服务接入、数据交互等功能；综合应用层则根据用户不同的需求提供相应的软件、平台，通过对资源的计算分析和合理分配，为用户提供精准的车联网服务。

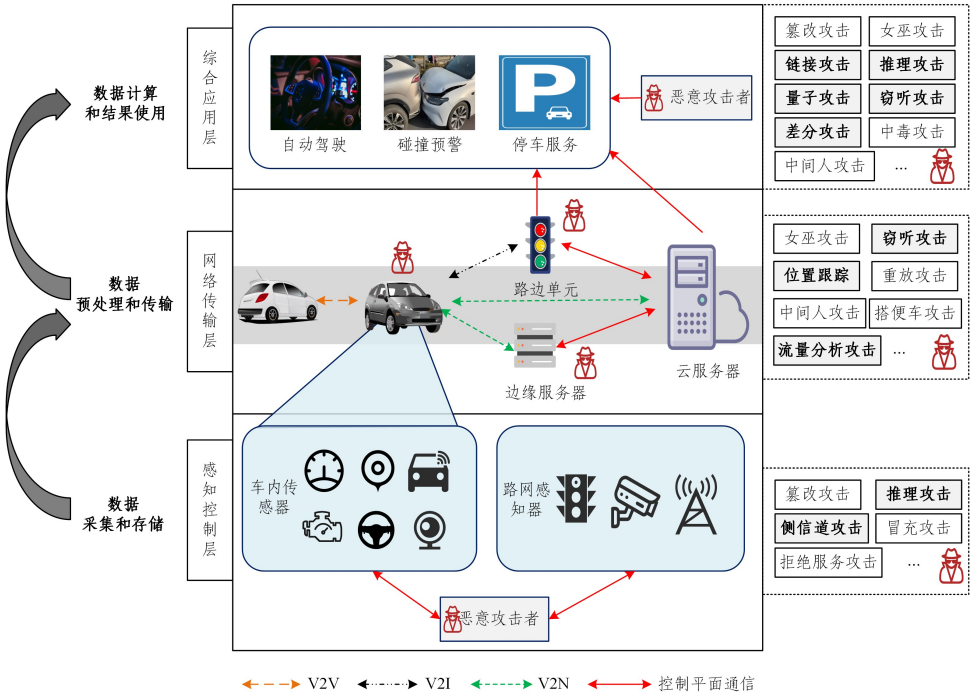


图 1 车联网边缘服务隐私泄露风险

Fig. 1 Risk of privacy leakage of IoV edge services

2.1.2 车联网隐私泄露风险

车联网可被看成一个大数据驱动的边缘移动网络[29]，一辆智能网联汽车每天能产生 TB 级的海量数据[30]。这些数据不仅包含丰富的车辆运行信息，还涵盖了大量与用户个人相关的敏感数据，如驾乘人员的面部数据、声音数据，以及位置信息、驾驶习惯等数据。这些数据具有数据规模大、时效性强、精度高、多样性、涉及隐私等特点，若直接明文存储、传输，可能导致隐私泄漏和滥用[30]。车联网实现隐私保护的前提是明确要保护的隐私数据目标，因此，本文根据国内关于车联网数据安全和隐

私保护的要求文件[1),2)]，整理了当前车联网敏感性数据类型与隐私泄露风险等级（见表1）。鉴于车联网敏感性数据类型具有多样性，须针对隐私泄露风险等级的不同选择合适的隐私保护计算技术。对于高敏感数据，如车辆控制指令，应采用隐私保护能力强的技术，例如结合同态加密和可信执行环境，确保指令在加密状态下执行。对于低敏感数据，如交通拥堵情况数据，可通过模糊泛化这类轻量的技术实现高效脱敏。

表1 车联网敏感性数据类型与隐私泄露风险分级

Table 1 Sensitive data type and privacy leakage risk classificationin IoV

数据方	数据种类	数据示例	隐私泄露风险等级
车辆自身	基础属性数据	车辆的车牌号、品牌型号等	低
		车辆的车架号、发动机号、标识等	中
		与车辆设计相关的核心数据	高
	车辆工况数据	车内空调、车辆一定时间内的平均行驶速度、年行驶里程等	低
		挡位使用和变化情况、在特定时间和特定路线内的停车次数或制动次数等	中
		基于某个或多个数据可唯一标识或识别出特定品牌车辆核心属性的数据	高
环境	环境感知数据	道路情况、交通拥堵情况、行驶周边可能的公共服务的位置信息、天气情况等	低
		邻近车辆的物理位置、行驶速度等；与车-行人通信相关的临近行人的位置信息、行人的行驶速度等	中
		相邻车辆一定时间内的出行路线、位置、停车信息等，或驾驶员的身体健康状况等	高
服务提供方	车控数据	倒车辅助中倒车提示声音、与车联网远程监控相关的一般读取类数据等	低
		仪表盘提醒指令；远程锁车、远程鸣笛等远程启动或制动车辆等相关指令	中
		自动泊车确认指令；通过车联网服务平台对多辆汽车进行远程操控的相关指令	高
用户	应用服务数据	天气预报推送；前方拥堵提醒、交通事故实时提醒等；与车载娱乐系统相关的记录、相关的娱乐系统使用行为数据	低
		多媒体数据；车辆碰撞预警数据等；与驾驶行为密切相关的车辆行为数据等	中
		语音服务的通话和视频记录等；车辆远程监控数据；基于车辆行为数据等分析出的车主某些个人喜好、行为习惯类数据；基于车辆自身状态和环境感知数据等分析识别出的车辆核心参数数据等	高
	用户个人信息	与已识别或者可识别的车主、驾驶人、乘车人、车外人员等有关的各种信息，不包括匿名化处理后的信息	低
		重要敏感区域的地理信息、人员流量等，以及车辆流量、物流等反映经济运行情况的数据，包含人脸信息、车牌信息等的车外视频、图像数据	中
		可能导致个人受到歧视或人身财产受到严重危害的信息，如车辆行踪轨迹、音频、视频和生物识别特征等信息	高

此外，由于车联网边缘与云端结合的特殊架构及开放特性，隐私攻击具有多入口、高隐蔽、难预防的特点，用户面临多层次、多方面的攻击威胁（见图1）。具体而言，在感知控制层，攻击者可通过物理接触或者无线电波等方式对车联网设备进行攻击，窃取驾驶习惯、车辆健康状态等敏感信息。例如，2022年丰田汽车旗下零部件制造商日本电装遭到网络攻击[31]；2024年，大众Cariad[32]因配置错误，导致80万辆电动汽车数据泄露，这些数据包括车辆的精确位置（精度达10 cm）、驾驶员信息等，甚至包括部分德国政要车辆和警方巡逻车辆的信息。在网络传输层，攻击者可通过欺骗行为，拦截、窃取或篡改通信信息。例如，2023年美国汽车配件零售商巨头AutoZone[33]称遭受了Clop MOVEit文件传输网络攻击，造成大量数据泄露。在综合应用层，攻击者可通过背景知识以及数据集的输出结果，推理出本不该泄露的敏感信息。例如，特斯拉声称哨兵模式所记录的数据只离线存储在车内USB设备中，车主和特斯拉均不能远程在线查看，但实际存在系统漏洞，有隐私泄露的风险。上述现实事件的发生，更凸显了保护车联网数据隐私的紧迫性。

为全面地说明隐私泄露风险，本文依照攻击者危害隐私的方式、风险来源、严重程度对车联网存在的典型攻击进行总结，如表2所列[34-43]。如果攻击严重影响车联网系统的运行性能或侵犯隐私，则攻击的严重性将被推断为高。

表2 车联网直接或间接导致隐私泄露的攻击及其特征

Table 2 Attacks directly or indirectly causing privacy leakage in IoV and their characteristics

威胁目标	攻击名称	危害隐私的方式	风险来源	严重程度
数据可用性	中毒攻击[35]	间接	内部	高
数据机密性	推理攻击[35]	直接	内部，外部	中
	流量分析攻击[38]		内部，外部	低
	位置跟踪[14]，窃听攻击[39]，差分攻击[40]		内部	高
	链接攻击[39]，量子攻击[41]，侧信道攻击[42]		外部	高
数据完整性	篡改攻击[15]，重放攻击[39]	间接	内部	中
数据真实性	中间人攻击[39]	间接	内部	高
	串通攻击[39]		内部	中高
	女巫攻击[41]		内部	高
	冒充攻击[43]		内部，外部	高

2.2 车联网边缘隐私保护计算

作为一种结合了密码学、人工智能等学科的技术集合，隐

1) 《汽车数据安全管理若干规定（试行）》. https://www.gov.cn/zhengce/zhengceku/2021－09/12/content_5640023.htm，2021，8，16

2) 中国通信标准化协会. 车联网信息服务数据安全技术要求：YD/T 3751-2020. https://std.samr.gov.cn/hb/search/stdHBDetailed?id＝AFC9FE3F29D8B96EE05397BE0A0AFF12，2020，8，31

私保护计算能够在保护数据隐私性的同时对数据进行计算、分析和处理，保障数据在采集、存储、处理、发布等全生命周期中的“可用不可见”[9]。在复杂的车联网边缘环境中，隐私保护计算的作用和价值尤为显著。车联网涉及到车辆、用户、服务提供商等多个参与方，数据的交互频繁且广泛。在车联网场景中，隐私保护计算可以使各参与方在不暴露各自敏感数据的前提下进行数据共享和联合计算。以交通流量分析为例，不同的车辆可以通过安全多方计算技术将加密后的位置信息和行驶速度等数据进行共享，从而实现对交通状况的准确评估，而各方的具体数据内容不会被泄露。

2.2.1 服务需求与评估维度

车联网边缘服务的实时性、动态性与异构性特征，对车联网隐私保护计算方案提出了多维度要求。

在服务场景隐私需求层面，车联网边缘隐私保护计算方案需适配 3 类典型场景。1）信息服务类。在这类服务场景中，数据隐私性要求因服务类型而异。交通信息服务主要涉及交通规则、交通路况等公开性信息，但对于车辆位置则需要进行隐私保护[44]。生活服务信息服务在使用时会推送天气信息、新闻资讯等公共信息，但对于涉及推送周边的服务则需要注意隐私保护。在数据效用方面，交通信息服务对数据时效性和准确性要求较高，生活服务信息服务也需精准且与用户相关。在效率方面，交通信息服务要高效收集、处理和分发信息，生活服务信息服务应及时推送周边信息并快速响应查询。2）安全服务类。此类服务场景对数据隐私性要求较高。碰撞预警、车道驾驶辅助等主动安全服务中，车辆传感器会采集轨迹、位置等隐私数据，因此需要对其进行隐私处理。被动安全服务，如在交通事故发生后，发送车辆位置和车内人员情况给救援机构，也要确保数据在传输时的安全性和完整性。在数据效用方面，主动安全服务对数据的准确性和实时性要求极高[26]，被动安全服务强调数据的完整性和可靠性。在效率方面，主动安全服务和被动安全服务都需要快速处理和响应数据。3）效率服务类。此类服务场景对数据隐私性的要求也是因服务类型而异。例如，安排车辆运行路线及出租车调度等调度服务，可能会涉及用户行程等隐私数据，因此需要隐私保护[13]；通过分析车辆行驶数据，给驾驶员提供节能驾驶建议的节能服务[26]，可能会涉及到与用户驾驶习惯相关的数据，因此也需要进行一定的隐私保护。此类服务对数据效用和服务效率要求不高。

在数据生命周期隐私保护方面，数据采集与存储、数据预处理与传输以及数据计算与结果使用这 3 个阶段具有各自独特的应用场景和隐私需求，隐私保护措施应针对不同阶段的特点予以设计。1）在数据采集与存储阶段，由于车辆数据来源广泛且格式不一，如何在分布式存储条件下确保各存储节点的数据隐私成为首要挑战。此外，由于数据在采集过程中常常以原始形式存在，其敏感信息较为集中，因此保护措施必须充分考虑数据格式与来源的异构性。2）在数据预处理与传输阶段，车联网边缘服务通常要求数据在极短时间内从采集端传输至边缘节点进行实时处理[45]。复杂且动态的通信环境，使得数据在传输过程中极易遭受窃听、篡改等攻击。如何在确保传输效率和实时性的同时对数据进行有效的隐私防护，是这一阶段亟待解决的问题。3）在数据计算与结果使用阶段，多方数据共享及协同计算对隐私保护的要求更高，既需要充分利用数据进行智能决策，又要防止敏感信息被过度暴露。此阶段要求采用的隐私保护计算技术既能保证计算结果的准确性，又能严格控制数据泄露风险，同时兼顾系统的计算与通信资源限制。

针对上述多元化的车联网边缘服务需求和隐私需求，车联网边缘隐私保护计算方案应该从以下 4 个维度进行评估。

1）隐私泄露风险：数据安全三要素包括可用性、机密性和完整性[8]。其中，机密性是指保证信息不被非授权访问，非授权用户即使得到信息，也无法知晓信息内容[46]。隐私攻击的最终目标则是破坏系统的机密性，推断和获取系统非主动暴露的隐私信息。对于隐私泄露风险，本文根据参考文献中给出的理论分析、攻击实验等分析手段予以评估。

2）数据效用：数据效用是从数据的使用者角度出发，关注数据是否能够满足用户的需求，以解决实际问题，即衡量数据的使用价值和效果。这可以从数据以及服务两个层面来衡量[47]。常用的度量指标有熵、平均绝对误差（Mean Absolute Error，MAE）、均方根误差（Root Mean Square Error，RMSE）、均方误差（Mean Square Error，MSE）、平均相对误差（Mean Relative Error，MRE）、假阴性率（False Negative Rate，FNR）和假阳性率（False Positive Rate，FPR）等。

3）开销：由于边缘设备的计算和存储能力有限，边缘服务的质量（如能否获得高效、稳定的数据处理）也应受到关注[11]。隐私保护计算方案在保证隐私的情况下，应尽可能减少计算和存储的开销。因此，隐私保护计算方案的性能评估应综合考虑计算开销、通信开销等因素。

4）可扩展性：在设计隐私保护计算方案时，需要考虑方案的兼容性、适用范围和资源管理等因素。一个优秀的隐私保护计算方案，应该在面对不断增长的车联网服务需求或规模时，能够有效地扩展和适应变化，而不影响效率[48]。

2.2.2 主要研究方向

本文基于隐私保护计算技术机制的差异，从计算过程涉及的数据采集和存储（S1）、数据预处理和传输（S2）、数据计算和结果使用（S3）这 3 个阶段出发，将现有的车联网边缘隐私保护计算方法归纳为以下 4 类。

1）基于数据变换的隐私保护计算。本路线适用于 S1，S2，S3 阶段。其核心机制在于对真实数据进行泛化或随机扰动处理，以降低数据的敏感性，实现数据去隐私。本路线的优势在于无需复杂的计算资源，部署简单，特别适合于对实时性要求较高的场景。例如，模糊泛化技术适用于对数据精度要求不高、以趋势分析为目标的服务，如城市交通流量统计和拥堵预测。差分隐私技术适用于对数据精度要求较高、需兼顾个体隐私保护的服务，如实时路况分析与个性化导航。此类场景要求数据在脱敏后仍能维持数据关联性，同时允许单次查询的绝对精度存在可控损失。然而，这些技术是通过牺牲数据精度来实现隐私保护的，因此在实际使用中需要权衡数据效用和隐私保护强度（即脱敏强度）[49]，例如根据服务隐私需求定制隐私保护程度。具体的研究进展及分析见第 3 章。

2）基于安全多方计算（Secure Multi-Party Computation，MPC/SMPC）的隐私保护计算。本路线适用于 S2 和 S3 阶段。车联网的开放性意味着会存在不可信第三方，该路线以

密码学为基础，能够在数据加密状态下进行多方联合计算、检索等处理，使得输入数据、中间结果不会暴露，只输出最终结果。在多车或多边协同任务中，当各参与方不愿将数据以明文形式共享时，安全多方计算技术优势明显。以多车联合路径优化为例，多辆汽车可在不暴露各自行驶起点、终点及偏好信息的情况下，通过安全多方计算共同规划出最优行驶路径，避免交通拥堵并提高出行效率。然而，在密文上执行计算的方式会给车联网边缘服务场景带来一定的通信和计算成本，因此在实际使用中需要权衡隐私保护和开销，以提升其可扩展性。具体的研究进展及分析见第 4 章。

3）基于联邦学习（Federated Learning，FL）的隐私保护计算。本路线适用于 S2 和 S3 阶段。该路线基于数据分离思想，实现了一种分布式计算框架，使得参与方无需直接共享原始数据，只需输出本地基于原始数据计算的中间结果。其优势在于能够整合来自不同车辆和路侧单元的数据，充分利用边缘设备的计算资源，减少数据传输量，特别适合车联网场景下的协同训练任务，例如多车协同自动驾驶[50]、驾驶风格识别。然而，该技术依赖于边缘节点的算力与数据分布一致性，对数据偏斜和节点异构性较为敏感。此外，目前已有研究表明，联邦学习中间参数的梯度信息仍存在反演攻击风险[51]，且频繁的模型更新交互会带来显著的通信开销。因此，在实际使用中需要权衡隐私、模型精度以及开销和效率问题。具体的研究进展及分析见第 5 章。

4）基于可信执行环境（Trusted Execution Environment，TEE）的隐私保护计算。本路线适用于 S1，S2，S3 阶段。其核心机制是依托硬件隔离技术（如 Intel SGX）提供内存加密和代码完整性保护，从而确保敏感数据在全生命周期内的安全性。可信执行环境的硬件级安全保障和高兼容性，使得各参与方能够在不可信的计算环境中隔离执行隐私敏感任务。相较于同态加密等纯软件方案，TEE 仅需少量计算开销即可实现高等级安全防护，特别适合车联网边缘设备资源受限的场景。然而，其依赖特定硬件支持，存在侧信道攻击风险。由于这方面的研究工作较少，本文在第 6 章专注于分析已有通用技术在车联网中的适配度以及存在的问题。

图 2 展示了数据变换、安全多方计算、联邦学习、可信执行环境这几种主流技术在车联网边缘环境下可应用的阶段。这些技术在实现机制、隐私保护能力、性能开销及适用场景方面存在较大差异。为帮助读者快速了解各技术路线的核心，对这几类隐私保护计算方法的原理、优势、相关研究工作以及存在的挑战进行总结，如表 3 所列。后续将结合车联网边缘计算的动态性和异构性特征，详细分析各技术的实际部署策略及其优化方向。

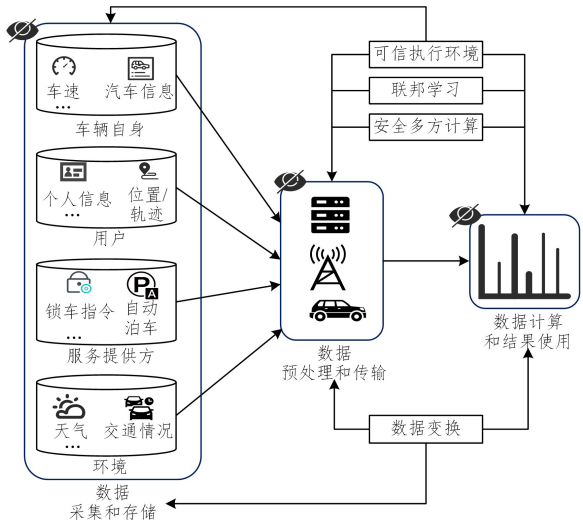


图 2 主流隐私保护计算技术在车联网边缘环境下的应用

Fig. 2 Application of mainstream privacy-preserving computation technology in the edge environment of IoV

表 3 车联网边缘隐私保护计算技术路线总结

Table 3 Summary of privacy-preserving computation technology for the IoV

技术路线		原理	特点	隐私保护能力	优势	可应用的阶段	适用场景	研究工作	挑战
基于数据变换	模糊泛化	通过模糊化等步骤，模糊描述原始敏感数据	使用近似推理来表示和处理不确定性、模糊性	中	简单、开销低；可以根据服务隐私需求定制隐私保护程度	S1，S2，S3	对数据精度要求不高、以趋势分析为目标的服务，例如交通流量统计和拥堵预测	FuzzyCom[52]、Fuzzy-Follow[53]、个性化停车隐私[54]、FuzzyTop[55]	隐私与数据效用的平衡、隐私开销与车联网资源的平衡
	中心差分隐私								
	本地差分隐私	对数据进行扰动	扰动对象可以是数据集的统计信息或各用户的原始数据项				对数据精度要求较高、需兼顾个体隐私保护的服务，例如实时路况分析与个性化导航	VDTP[56]，ODPRL[57]，DPTD[58]	
								TNC 车辆调度方案[13]、PLPP[47]、DPLP[59]	
基于安全多方计算	秘密分享	将敏感数据拆分为多个分发给参与者	只有足够数量的、不同类型的秘密分片组合在一起时，才能还原秘密	中高	考虑了不可信第三方；密文传输、密文计算	S2，S3	多车或多边协同任务，当各参与方不愿将数据以明文形式共享时，例如多车联合路径优化	PrivacySignal[44]、MPC-CSAS[60]、轨迹预测[61]、隐私保护真相发现[62]	隐私开销与车联网资源的平衡；量子攻击、内部对抗性攻击；多方协同兼容
	同态加密	先加密明文，再执行密文间的计算	能够直接对密文进行运算					Psafety[14]，ERDSS[63]，PPVF[64]	
	零知识证明	参与方之间通过交换问题和答案，来证明某些事情或论断的真实性	不暴露秘密信息					Eco-CSAC[26]、匿名认证方案[65]、Vehicloak[66]	

（续表）

技术路线	原理	特点	隐私保护能力	优势	可应用的阶段	适用场景	研究工作	挑战
基于联邦学习	本地训练模型，中心聚合各参数，更新全局模型，再发送回各参与方进行本地更新	原始数据不流出，计算过程中仅传递处理后的中间数据	中	易开发实现；性能较高；分布式架构可降低计算和存储开销	S2，S3	车联网场景下的协同训练，例如如多车协同自动驾驶、驾驶风格识别	扰动训练数据[67]、SecProbe[68]、三元联邦学习[69]、改进的 FedLoc[70]、FEEL[71]、EPPFL[72]、FedLSTM[73]、SEAR[74]数据聚合[75]	隐私、模型精度以及开销和效率的平衡问题
基于可信执行环境	通过隔离技术，为使用者创造了一个安全可信的执行空间	数据及代码不流出，集中计算	中高	支持多层次、高计算复杂度的算法逻辑；密文传输、明文计算	S1，S2，S3	不可信的计算环境，对隐私保护能力要求高，例如车辆控制指令、固件更新	QuaEva[42]、SEAR[74]、Cerberus[76]、信任管理[77]	多方协同兼容

3 基于数据变换的隐私保护计算方法

数据变换是一类通过特定技术手段对原始数据进行修改或转换的技术，可以降低数据被用于识别个体或推断敏感信息的风险，同时尽可能保留数据的可用性。本章介绍的基于数据变换的隐私保护计算方法具有实现简单、开销低的特点，适用于隐私性要求较高、数据效用要求一般、效率要求较高的场景。该路线不要求数据所有者完全信任服务提供商，其核心是在原始车辆数据的基础上进行泛化及添加噪声等处理，以解决数据流出时的隐私问题。此外，这类技术还可以根据服务隐私需求定制隐私保护程度。模糊泛化和差分隐私是数据变换技术中最具代表性的两种方法。

3.1 基于模糊泛化的隐私保护计算

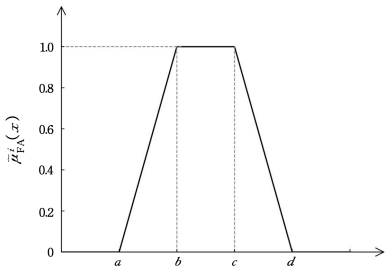
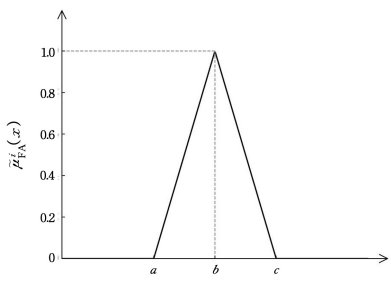
3.1.1 模糊泛化

模糊（Fuzzy）泛化是一种基于模糊集合理论的数据泛化方法[78]，其核心机理是通过隶属度函数将原始数据映射至模糊语义空间，在降低数据粒度的同时，维持其统计分布与关联特征。这样做既能实现隐私保护，又能在一定程度上维持数据的基本结构和分布特征。模糊集合（Fuzzy Set，FS）和隶属函数（Membership Function，MF）是模糊集合理论中最重要的两个概念。模糊集合通过定义隶属度$\widetilde{\mu}_{FA}^{i}(x)$，描述数据点$x$对集合$FA$的隶属程度，隶属度越接近于1，表示该元素属于该集合的程度越高。这种描述方式比简单的二元分类（属于或不属于某个类别）更加灵活，可以应对车联网数据的复杂性和非线性特点[79-80]，并具有更好的可解释性。该技术尤其适用于车联网边缘计算场景，其轻量化特征可有效缓解资源受限设备的计算压力。

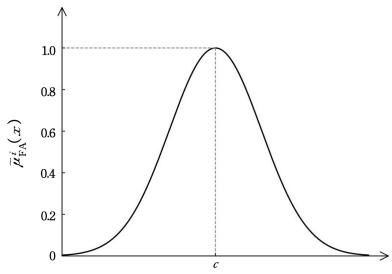
下面介绍模糊泛化的实现步骤。1）定义模糊集合：针对特定的车联网边缘智能服务，为每一维敏感数据的论域定义若干个模糊集合。2）设置隶属度函数：根据边缘智能服务的场景和需求，为每个模糊集合设置合适的隶属度函数。表4列出了梯形、三角形以及高斯型隶属函数的数学表达式。3）划分模糊区间：根据多个隶属度函数的交点划分论域，得到若干个模糊区间，每个模糊区间对应一个模糊集合的语义信息。4）数据泛化：根据不同模糊集合的语义信息定义模糊区间的泛化表示（语言变量、二进制编码等），使用泛化表示代替原始数据即可完成模糊泛化。

表4 常见隶属函数

Table 4 Common membership functions

隶属度函数	数学表示	示例
梯形	$f(x,a,b,c,d)=\begin{cases}0, & x\leqslant a\\ \dfrac{x-a}{b-a}, & a\leqslant x\leqslant b\\ 1, & b\leqslant x\leqslant c\\ \dfrac{d-x}{d-c}, & c\leqslant x\leqslant d\\ 0, & x\geqslant d\end{cases}$	
三角形	$f(x,a,b,c)=\begin{cases}0, & x\leqslant a\\ \dfrac{x-a}{b-a}, & a\leqslant x\leqslant b\\ \dfrac{c-x}{c-b}, & b\leqslant x\leqslant c\\ 0, & x\geqslant c\end{cases}$	

（续表）

隶属度函数	数学表示	示例
高斯型	$f(x,\sigma,c)=\mathrm{e}^{-\frac{(x-c)^2}{2\sigma^2}}$	

3.1.2 车联网边缘服务中的模糊泛化实现

车联网边缘设备通常具有计算能力弱、存储空间有限的特点。模糊泛化技术通过轻量级的模糊化处理，能够在不显著增加资源开销的情况下，使得方案能够满足车联网边缘信息检索服务的效率和实时性能的要求，进而提高服务质量[81-82]。

在交通信息服务类中，模糊泛化常用于对轨迹数据和交通情况进行处理。Li 等[52]将原始轨迹数据转换为车辆侧的模糊字符串，再将最长公共字符串技术与霍夫曼编码和 RLE 编码（fast-fuzzyCom）相结合，进一步压缩模糊轨迹字符串信息，其信息损失小于其他基准测试方法，实现了理想的压缩比、压缩时间以及它们之间的平衡。Chen 等[53]提出了基于动态不确定交通状况的隐私感知智能跟车方案，首先将位置、速度等敏感数据转换为模糊信息，再将模糊后的信息转换为模糊状态转换矩阵，并利用模糊多阶马尔可夫方法预测前车的制动行为，最终在实现 90.4% 预测准确率的同时，显著降低了通信成本和计算复杂度，实现了轻量级的实时跟车决策。

虽然模糊泛化技术通过降低数据精度而非完全加密的方式保护隐私，能够在保证数据可用性的同时减少计算和通信开销[53]，但是在某些对数据精度要求较高的车联网应用场景，这种方法可能会带来不利影响。传统模糊泛化技术通常依赖静态隶属函数，其设计和选择主要基于专家经验，存在较强的主观性和局限性。这种静态设计难以适应车联网动态多变的环境，尤其在突发交通事件或高动态场景下，可能增加预测误差，限制了技术的实际应用效果。此外，不同类型的数据具有各异的分布特征和变化规律，不同应用场景对隶属函数的需求各异，而现有方法缺乏自适应调整能力，难以满足多样化的实际需求。因此，实现隶属函数的动态优化和自适应选择，成为提升模糊泛化技术在车联网中的适用性的关键。

部分研究根据实时变化的数据分布特征，提出动态调整隶属函数参数，从而提升模糊泛化技术在动态环境中的适应性和准确性。为满足交通拥堵情况评估服务的实时性需求，Liu 等[83]通过动态多模型自适应指数平滑预测交通车速、交通量密度和道路饱和度，依据历史预测误差，计算各模型的最优平滑系数与权重，实现对指标的精准预测。预测值作为梯形隶属度函数的输入，随交通状况实时变化。对于权重的确定，基于自适应 CRITIC 方法[84]，先对原始数据进行标准化处理：$K_i=\frac{k_i-k_{i\min}}{k_{i\max}-k_{\min}}$ 计算指标标准差 S_i 和线性相关系数 $R_{ii'}$，再根据 $W_i=\frac{C_i}{\sum_{i=1}^{g}C_i}$ 确定权重，其中 $C_i=S_i\sum_{i'=1}^{g}(1-R_{ii'})$。该方法使权重能反映指标间的实时关系，与动态变化的预测值共同作用，实现隶属度函数的动态调整。值得关注的是，神经模糊网络的兴起为自适应隶属函数学习提供了范式[5]。

此外，模糊泛化技术也可以依据不同的用户偏好进行相应的泛化，以实现个性化隐私保护。例如，文献[54]将模糊规则和 SkyLine 相结合进行决策，实现了实时停车推荐，推荐的平均准确率为 91.2% 左右，并且该方案的实时性好，平均数据传输率约为对比方法的 1/3，响应时间短。Chen 等[55]利用直觉模糊集，通过模糊隶属函数对停车数据的距离、空余车位数、停车费用等属性进行模糊化处理，再根据用户偏好设置权重，加权计算各停车场的综合得分，最终依据得分排序确定前 k 个最优推荐，有效保护了停车数据的隐私。

基于模糊泛化的隐私保护计算方案之间的对比分析如表 5 所列。

表 5 基于模糊泛化的隐私保护计算方案

Table 5 Privacy-preserving computation schemes based on fuzzy generalization

研究工作	隐私数据	隐私泄露风险	隶属函数	数据效用	开销	可扩展性
fuzzyCom[52]	位置/轨迹	中/能抵御窃听攻击以及对网关端的攻击	梯形	中高	低	高
FuzzyFollow[53]	位置、速度等	中/能抵御嗅探攻击	梯形、高斯	中	低	高
个性化停车隐私[54]	停车场的数量、停车价格和用户的偏好	中/能抵御窃听攻击	梯形、三角形	中	中	高
FuzzyTop[55]	停车数据	中/能抵御窃听攻击和妥协攻击	高斯	高	中	高

3.2 基于差分隐私的隐私保护计算

3.2.1 差分隐私

差分隐私（Differential Privacy，DP）是一种典型的噪声添加技术，其核心思想是通过各种随机化机制（如拉普拉斯、高斯、指数等），在数据发布或输出过程中添加噪声，使得敏感数据失真，从而在实现对数据集中个体隐私脱敏的同时，保留数据集整体的统计学信息[85]。差分隐私的数学定义如下：设随机化机制 $M(\cdot)$，$Range(M)$ 为 $M(\cdot)$ 所有可能的输出构

成的集合。对于任意相邻的输入数据集 D 和 D'（D 和 D' 只相差一条数据记录），以及 $Range(M)$ 的任何子集 S_M，有：

$$\Pr[M(D)\in S_M]\leqslant e^{\varepsilon}\cdot\Pr[M(D')\in S_M]+\delta$$

则称随机化机制 $M(\cdot)$ 满足 (ε,δ)-DP（$\varepsilon>0,\delta>0$）。若 $\delta=0$，则 $M(\cdot)$ 是 ε-DP（$\varepsilon>0$）的。在该定义中，使用 ε 和 δ 两个参数来描述概率差距，用于确定添加噪声的大小。其中，ε 被称为隐私预算（Privacy Budget），是用来控制随机化机制 $M(\cdot)$ 在两个相邻数据集上获得相同输出的概率比值。ε 值越小，隐私保护能力越强，但有用的信息就越少。δ 被称为失败概率。该定义也可以理解为该机制至少能以 $1-\delta$ 的概率满足 ε-DP。

差分隐私能够抵抗攻击者基于背景知识的攻击和利用统计查询的差分攻击[40]，是保护各种数据类型的事实标准[86]，其优点是可以通过数学方法控制隐私损失量，提供形式化的隐私保证。

3.2.2 车联网边缘服务中的差分隐私实现

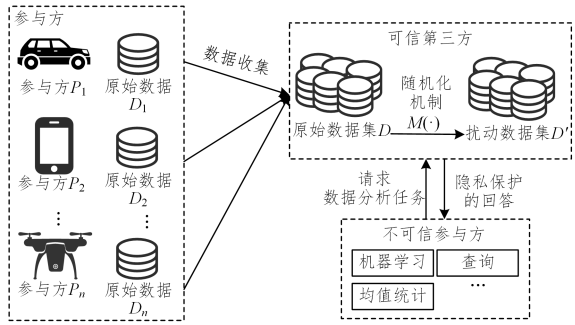
在车联网中，差分隐私技术可以广泛应用于自动驾驶、智能交通管理、停车推荐等多个场景。例如，在自动驾驶系统中，车辆需要频繁地共享实时的道路信息、位置和速度数据。差分隐私技术通过为这些数据加入噪声，能够保证即使数据被外部访问，也无法推断出单辆车的具体位置或驾驶行为。而在车联网边缘服务中实现差分隐私，需要综合考虑隐私保护要求、数据处理效率和数据精确度等因素，来决定最适合的噪声添加位置、随机化机制以及隐私预算等差分隐私属性。

1）噪声添加的位置

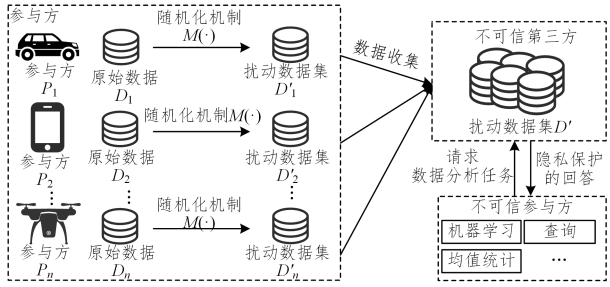
噪声可以添加在采集的原始数据、中间计算结果和输出结果上。根据第三方是否可信，也可以选择是否由用户在本地对数据添加噪声，即选择中心差分隐私（Central Differential Privacy，CDP）还是本地差分隐私（Local Differential Privacy，LDP）。

CDP 要求数据所有者将原始数据发送到一个第三方服务器，由该服务器对数据进行统一的扰动处理。CDP 具有较高精度和较低实现成本的特点，适用于第三方可信的场景，例如交通管理平台。其在车联网环境下的应用模型如图 3(a)所示。

在实际应用中，CDP 假设的可信数据中心较难实现，如果第三方是恶意的，仍会泄露用户的敏感信息。LDP 将数据隐私化的工作从服务器转移到用户端，允许数据所有者对其敏感信息进行本地化扰动处理，接着将已经处理过的数据发送给第三方，避免了不可信第三方造成的数据泄露问题[87]。在这个过程中，用户被赋予了一定的数据控制权，可以自行决定隐私保护的级别。其在车联网环境下的应用模型如图3(b)所示。Wei 等[59]在将位置信息提交给不受信任的空间众包（Spatial Crowdsourcing，SC）服务器之前，将工作者和任务的精确位置分割成具有噪声的多级网格，保护了空间众包中工作者和任务的位置隐私，同时实现了高数据效用的任务分配，工作者保护过程中的数据效用分别为 88.28% 和 93.25%，任务保护过程中的所有数据效用均超过 90%。



(a)CDP



(b)LDP

图 3 DP 在车联网中的应用示意图

Fig. 3 Application diagram of DP in IoV

2）采用的随机化机制

随机化机制与查询函数 $f(D)$ 紧密相关。在车联网环境中，车辆数据多为连续型数据，例如车辆的速度、轨迹等。而对于数值型查询（如计算数据集的均值、总和等统计量），一般对连续型输出结果采用加性噪声（拉普拉斯机制）[88]，对离散型输出结果采用指数机制。轨迹数据是一个时间序列数据，通常包含多个数据点，每个数据点都包括位置、时间以及其他属性，因此在添加噪声时，需要考虑它的时空特征。Liu 等[56]提出了一种基于差分隐私的细粒度车辆轨迹数据清洗框架，以生成包括位置、速度和时间戳等属性在内的完整数据。该框架分为 3 个阶段，阶段一使用属性车辆 ID、位置和计数对概率输出进行采样，阶段二对要与车辆 ID 和位置关联的移动值进行采样，阶段三对要与车辆 ID、位置和移动值关联的时间戳进行采样。为了进一步提高三阶段采样的输出效用，该方案对车辆轨迹插值，通过近似估计填补不同时间的缺失值。然而，该方案的总体概率差距有限，且计算复杂度为 $O(n^2)$。基于边缘计算的车联网中，数据庞大且类型复杂，在处理高维车辆数据时，通信开销会呈线性或指数增长。对于复杂数据类型，可以使用树型结构、图结构等结构化格式表示[86]。

3）添加噪声量的大小

敏感度（Sensitivity）Δf 是指删除数据集中任一记录对查询结果造成的最大改变，是决定加入噪声量大小的关键。敏感度越大，则需要添加的噪声就越多。以拉普拉斯机制为例，对一个可以输出结果为数值型的函数 $f(D)$ 加入服从拉普拉斯分布 $Lap\left(\frac{\Delta f}{\varepsilon}\right)$ 的噪声，使得查询结果满足 ε-DP，可以表示为 $F(x)=f(x)+Lap\left(\frac{\Delta f}{\varepsilon}\right)$。其中，敏感度 Δf 为：

$$\Delta f=\max_{D,D';d(D,D')\leqslant 1}|f(D)-f(D')|$$

车辆位置数据是车联网中最常见的数据之一[89]。ε-地理不可区分性[90]是将差分隐私的思想引入LBS中，其数学定义为：一个机制K满足由参数ε决定的地理不可区分性，当且仅当位置集X中任意两个位置点x，x'满足：

$$K(x)(z)\leqslant e^{\varepsilon d(x,x')}K(x')(z),\forall x,x'\in X,z\subseteq Z$$

其中，K是一个用于选择报告值的概率函数；$K(x)(z)$是当用户位置为x时，$z\subseteq Z$的概率；$d(\cdot,\cdot)$表示两个位置之间的欧氏距离；X是可能的位置集合，Z是一组重新报告的值。

Andres等[90]通过在用户位置添加受控随机噪声来实现ε-地理不可区分性，能够在释放近似信息的同时提供所需的LBS服务。然而，这种处理方式为所有位置提供了统一的隐私保证，会降低查询答案在位置分析中的效用。Zhang等[13]将基于差分隐私的地理不可区分性方案与风险规避两阶段数据驱动的优化方法结合，实现了用户位置隐私和交通网络公司收益的平衡，数据标准差的值随着历史数据的增加而减小。

为了避免出现保护不足或者过度保护的情况，需要解决隐私预算的分配问题。Chen等[57]将强化学习与差分隐私结合，动态优化车辆轨迹上每个位置的隐私预算分配，能够更好地平衡地理位置混淆和语义位置安全，在4个数据集上的数据效用损失稳定在331.3，482.5，285.2，384.4左右。然而，该方案需要收集一定的数据，因此初始阶段的效率低下。Cai等[58]根据时间戳，将轨迹空间划分为多个平面，再通过先聚类后泛化的方法重新形成新轨迹，有效解决了时间维度导致的数据分布稀疏和全局敏感度高的问题。此外，该学者还提出基于马尔可夫转移概率来预测偶数层中的节点数，该方法节省了近一半的隐私预算，并提高了数据可用性，在RMSE、查询误差、频繁模式挖掘3个指标上表现良好。然而，该方法中的轨迹长度是固定的，因此需要进一步扩展以解决动态轨迹数据的问题。Xu等[47]综合考虑轨迹泄漏、攻击策略、服务质量以及用户隐私偏好等因素，通过建立效率和隐私影响的归一化决策矩阵，计算有效的驾驶路线。同时，通过定义敏感距离指标来量化不同服务请求位置的隐私需求，实现了位置隐私和服务质量平衡的最优解，用户的收益提高了14.6%～23.24%，且MAE小于对比方案。然而，该方案未解决车辆行驶速度、加速度、行驶方向等属性对隐私泄露的影响，且时间复杂度为$O(n^2)$。

基于差分隐私的隐私保护计算方案之间的对比分析如表6所列。

表6 基于差分隐私的隐私保护计算方案

Table 6 Privacy-preserving computation schemes based on DP

研究工作		隐私数据	隐私泄露风险	参数设置		数据效用	开销	可扩展性
				随机化机制	噪声量大小			
噪声添加位置	VDTP[56]	轨迹	中/数学定义分析，无法从输出中识别此类车辆是否包含在数据集中	拉普拉斯	(ε,δ)-DP，ε为0.05～0.65	中高	中低	中高
	ODPRL[57]	语义位置	中低/实验分析，语义风险很小	拉普拉斯	ε-DP，ε为0.1～1	中	中	中
	DPTD[58]	轨迹	中/引文证明，后处理不会导致隐私泄露	拉普拉斯	ε-DP，ε为0.1～2.0	中高	中	中
基于LDP	DPLP[59]	位置、任务	中/理论分析，不受信任SC服务器无法知道任何任务和工作程序的确切位置	拉普拉斯	ε-DP，ε为0.1～1	中高	中	中高
	PLPP[47]	位置	中/理论分析，用户在享受LBS提供的服务的同时不会泄露自己的隐私	拉普拉斯	ε-DP，ε为1～12	中高	中	中
	车辆调度方案[13]	位置	中/基于地理不可区分性，攻击者无法区分输入的真实位置	高维拉普拉斯	$\varepsilon-DP$，ε为1，1.5	中高	—	中

4 基于安全多方计算的隐私保护计算方法

本章介绍的路线考虑了不可信第三方，能够支持密文传输、明文计算，在对隐私性要求和数据效用要求较高、对效率要求一般的场景中具有一定的应用价值。但是，部分基于密码学的隐私保护计算方案会存在计算效率较低、计算和通信开销大等问题。因此，在车联网边缘服务领域，需要设计出高效的轻量级方法，以实现隐私开销与车联网资源的平衡。

4.1 安全多方计算

安全多方计算(MPC/SMPC)是指在不信任对方及第三方的情况下，多个参与方通过事先约定的密码学协议进行交互，共同计算模型或目标函数。各参与方的输入不可见，计算后仅能得到自己的计算结果，而无法得知其他参与方的输入和输出。安全多方计算不依赖硬件，支持多节点协作，能够在车辆与周边设备(如其他车辆或边缘节点)之间实现安全数据交互，隐私保护能力强，且计算结果准确可靠。因此，SMPC被广泛用于解决在多方共享和计算数据时产生的隐私问题[91]。

SMPC是一种计算模式，只要是涉及多个参与方的密码学任务都可以看作一个安全多方计算任务。SMPC的实现需要依赖多个底层密码学协议或框架，如秘密分享(Secret Sharing，SS)、同态加密(Homomorphic Encryption，HE)和零知识证明(Zero Knowledge Proof，ZKP)、隐私集合求交(Private Set Intersection，PSI)等[92]。

4.2 基于秘密分享的安全多方计算

秘密分享的核心思想是将敏感数据(秘密)s拆分为n个分片分发给参与者，当有$t(1\leqslant t\leqslant n)$个不同类型的秘密分片组合在一起时，才能还原秘密[93]。在秘密分发阶段，有基于位运算和基于线性代数两种分片生成方式[48]。基于位运算的方法通过位操作生成分片，适用于资源受限的环境。而基

于线性代数的方法则利用多项式插值或矩阵运算生成分片，具有更高的灵活性和可扩展性。秘密分享的通信量与通信轮次成正比，尤其对线性操作具有较高的效率。

秘密分享可用于车联网边缘环境中动态数据共享的轻量化实现。在自动驾驶编队服务场景中，Liu 等[60]将速度-排放量映射进行拆分，其中一些保存在本地，另一些与其他车辆交换，以实现隐私保护。该方案模型收敛的最优推荐速度非常接近原始优化问题的真实最优值。此外，该方案的实验表明，车辆之间共享信息的大小为 152 Byte，对于具有一般硬件配置的车辆和基站，通信和计算时间大约为 0，数据共享和聚合过程在 5 ms 内完成。虽然该方案的实时性好，但秘密拆分过程涉及大量的数值计算和数据处理操作，随着参与方数量的增加，大量的秘密份额数据在网络中传输，极易造成网络拥塞，数据传输延迟会显著增加，甚至可能出现丢包现象。这对于对实时性要求极高的车联网应用，如自动驾驶车辆间的协同驾驶来说，严重威胁到了系统的可靠性和安全性。

对于复杂计算任务的隐私保护问题，现有学者大多基于计算任务设计协议，以提高执行效率。Ying 等[44]针对智能交通管理中的动态信号控制服务场景中通勤者的隐私问题，设计了一系列基于加法秘密分享(Additive Secret Sharing，ASS)的轻量级安全计算子协议，以秘密值的形式完成交通信号控制的子操作。Liu 等[61]提出用于车联网轨迹预测的秘密分享多方计算方案，设计了 4 个交互协议，即 $SecLog(\cdot)$，$SecExp(\cdot)$，$SecRec(\cdot)$和 $SecCmp(\cdot)$，用于计算非线性对数、指数、倒数和比较函数。这些协议基于 ASS，通过随机数保护数据隐私，使 AdaBoost 集成学习算法能够在多个路侧单元间分布式部署。实验表明，当参与者为 2 个、弱分类器为 16 个时，处理单个测试数据的模拟运行时间约为 257 ms，具有较低的延迟。真相发现，是提高移动群智感知感知数据准确性的一种方法。然而，隐私泄露和数据滥用问题，打击了用户参与传感任务的积极性，而现有的隐私保护真相发现解决方案通常存在计算效率低、用户与服务器交互频繁等问题。为此，Peng 等[62]提出了一种基于安全多方计算的隐私保护真相发现方案。用户将感知数据拆分为 3 个分片，分别将其上传至独立服务器 S_1，S_2，S_3，利用 ASS 确保单个服务器无法还原原始数据。服务器间基于 Sharemind 框架执行安全计算协议。实验表明，在高负载场景下，该方案的执行时间增长缓慢，在大量用户和任务场景下表现更优；无论是正常场景还是大量任务场景，相较于其他方案，其通信成本增长缓慢，当任务数量达到 500 时，通信成本仅为 12.008 kB/用户。

4.3 基于同态加密的安全多方计算

同态加密(Homomorphic Encryption，HE)作为一种支持密文计算的密码学技术，具有加法同态性和乘法同态性，即可以利用加法和乘法构造任意的计算方法对进行运算，其计算得到的结果与在明文状态下用同一方法计算的结果一致。基于同态加密的方案架构更为简单，能够直接对密文数据进行分析、检索、运算，从而避免数据在进行分布式处理时的加解密过程，提高了数据处理的效率。

同态加密分为全同态加密(Fully Homomorphic Encryption，FHE)和部分同态加密(Partial Homomorphic Encryption，PHE)两种类型。FHE 的安全性保证更高，适用于复杂的计算任务，但其计算开销较大，难以满足实时性要求。相比之下，PHE 构造简单，计算效率较高，适用于线性计算任务。Paillier 加密是常见的 PHE 算法。

Paillier 加密是一种概率公钥加密算法，该算法的安全性基于复合残差类的难题。针对数据存储阶段的车辆隐私问题，Wang 等[63]利用 Paillier 加密的同态属性，可以在加密的数据上执行排序和相关性评分的计算，从而实现对加密数据的检索。该方案能够实现用户访问控制的细粒度管理、结果可验证、搜索精度高的效果，但未考虑到车载网络数据的动态更新和删除问题，其搜索开销会随着查询关键词数量的增加而呈线性增长。车辆反馈报告涉及到身份、位置、行驶路线等隐私信息，因此 Cheng 等[64]提出每辆车都使用 Paillier 加密对个人反馈进行加密，并将其提交给 RSU，有效保护了车辆反馈隐私。实验表明，在通信领域车辆数量增加的情况下，该方案具有较低的消息丢失率。然而，该方案必须基于证书机构和云服务提供商的密钥是安全的前提。

车联网边缘服务中的复杂计算任务(如实时数据分析)往往涉及非线性操作，而基于 FHE 的方案则会面临计算复杂度大、内存占用多以及计算非线性函数时效率较低的问题。Yu 等[14]提出了两种使用 HE 的安全轨迹相似度计算算法，实现了为用户规划约定的加密路径和测量带有噪声的加密轨迹的偏差。在 30%的噪声率下，当计划路径长度为 $m=2^{11}$ 和 $\alpha=52$ 时，FNR 和 FPR 分别保持在 0%和 3%左右，数据效用高。此外，作者设计了密文压缩算法和安全比较协议来提高效率。在路径规划阶段，用户端的计算成本约为 26 ms，通信成本约为 90 kB；在监控阶段，用户的计算成本约为 13 ms。然而，该方案未解决加密轨迹的时空相似性问题，限制了其对更复杂的异常加密轨迹的识别能力。

4.4 基于零知识证明的安全多方计算

零知识证明是密码学中的一种技术，可以让证明者在不暴露秘密信息的情况下，向验证者证明某些事情或论断的真实性。根据证明者和验证者之间的交互次数，零知识证明可以分为交互式和非交互式。在实际的车联网应用中，若多注重通信效率，可以使用非交互式零知识证明(Non-Interactive Zero-Knowledge，NIZK)[26]。

V2V 消息的真实性和完整性对于安全至关重要，零知识证明可以在不泄露消息内容的情况下，验证消息的真实性。在车联网中，零知识证明的主要应用场景包括身份认证和数据验证。在身份认证场景中，需要验证某种属性(如用户身份或权限)，确保参与者在计算过程中保持身份的真实性。Jiang 等[65]针对车辆认证过程中存在隐私泄露的问题，使用基于点阵的零知识证明方案实现车辆的匿名认证，能够在不损害车辆隐私的前提下显著提高验证效率。认证方案的计算成本为 7.08 ms。然而，由于车联网中设备众多，尤其是在车辆高速移动、网络环境不稳定的情况下，车辆之间以及车辆与基础设施之间需要多次验证消息，这可能会显著增加数据的处理时间，进而影响系统的实时性。而非交互式零知识证明则可以避免这种复杂的交互过程。Li 等[26]使用 Fiat-Shamir 变换将交互式 ZKP 协议转换为非交互的，并将其引入到联盟

链的架构中，实现了车辆合法身份的验证，保证了服务信任和数据内容隐私。实验表明，该方案能够使各车避免碰撞并遵守道路速度限制，同时使各车队的总能耗最小，当一个车队的车辆数为 100 时，基站验证来自车辆的签名和密码文本的时间开销约为 53.2 ms。在数据验证场景中，车辆需要验证某些数据是否满足特定条件（如速度限制、位置真实性等）。Guo 等[66]将假名和群签名引入智能合约，基于简洁非交互式零知识证明（zero-knowledge Succinct Non-interactive Argument of Knowledge，zk-SNARK），隐藏了发送方和接收方之间的直接关系，在保护车辆的位置和身份隐私的同时，确保了应付金额的正确性和位置的真实性。实验表明，该方案 zk-SNARK 的性能只受到站点数量的轻微影响。

几类基于安全多方计算的隐私保护计算方案之间的对比分析如表 7 所列。

表 7　基于安全多方计算的隐私保护计算方案

Table 7　Privacy-preserving computation schemes based on SMPC

研究方向	研究工作	隐私数据	隐私泄露风险	数据效用	开销	可扩展性
秘密分享	MPC-CSAS[60]	车的原始排放成本函数	中/举例分析，可以实现隐私保护计算	高	低	中高
	PrivacySigna[44]	车辆的速度、位置等状态信息	中低/理论分析，在半诚实模型中是安全的	高	低	中高
	轨迹预测[61]	轨迹数据	低/理论分析，在半诚实模型中是安全的	高	中低	中高
	隐私保护真相发现[62]	感知数据	低/理论分析，在半诚实模型中是安全的	高	中低	中高
同态加密	ERDSS[63]	外包数据、索引以及语义	中低/理论分析，没有算法能比过安全实验	高	中	中
	PPVF[64]	反馈	低/理论分析，可以实现反馈的保密性，能抵御冒充、重放和篡改等攻击	高	中低	中
	Psafety[14]	位置	中低/理论分析，在半诚实模型中是安全的，当存在恶意用户时也是安全的	高	中	中高
零知识证明	匿名认证方案[65]	身份、位置	中低/理论分析，能抵御中间人攻击、重放攻击、冒充攻击	高	低	中高
	Eco-CSAC[26]	内容	中低/理论分析，能抵御女巫攻击、篡改攻击、冒充攻击	高	中	中
	Vehicloak[66]	位置、身份	中/理论分析，能保证数据真实性、正确性	高	中	中

4.5　车联网安全多方计算的隐私保护优化

基于数学难题构建的密码学方案在量子计算环境下易受攻击，抗量子计算密码学成为保障车联网隐私安全的重要研究方向。Mohanty 等[94]提出了一种基于量子密码学的阈值 PSI 的协议，可确保拼车服务中的隐私安全。Sutradhar 等[95]针对这一场景中的车辆通信问题，提出了一种量子加密协议，其能够抵御窃听攻击、重放攻击和中间人攻击，适用于高速公路车辆通信场景。这些方案虽能提供极高的安全性，但量子设备的部署成本高，且对通信环境要求严格，限制了其大规模的应用。

此外，基于密码学的技术对来自内部人员的对抗性攻击防护不足。例如，秘密分享依赖第三方服务器进行秘密分发，会存在单点故障、恶意敌手等额外的安全风险。而信任管理[96]和激励机制[97]可以作为密码学方案的补充，从而可以基于博弈论减少不诚实的节点，或降低节点由于自私或恶意发出不可信信息的可能性。Miao 等[81]基于车辆的行为数据，利用模糊理论评估每辆车的可信度。Li 等[98]针对车辆数据提供者的隐私问题，提出基于部分排序的信任管理方案以及由 Wasserstein 生成对抗网络和差分隐私联合设计出轨迹隐私保护方案，在完全可信的无人机协助下，实现了对数据提供者的精准评估和信任管理，选择排名靠前的车辆进行数据采集。Chen 等[77]进一步设计出去中心化信任管理系统，结合区块链和 TEE，降低了单点故障风险。这些方案在保护隐私的同时，提高了系统的安全性和可扩展性，但可能引入额外的计算和通信开销。Jiang 等[99]提出一种基于进化博弈论的动态激励模型，用于解决数据共享场景中的访问控制和公平激励分配问题。被缓存命中的车辆通过向边缘节点发送凭证，来证明已将缓存内容传输到请求车辆，参与合作行为的车辆节点因此获得更大的收益，从而鼓励车辆积极参与车对车通信，抑制恶意和贪婪节点的自私行为。

4.6　车联网安全多方计算的性能优化

尽管安全多方计算在车联网隐私保护中展现出强大的隐私性优势，但其实际部署仍面临显著的计算和通信开销问题。安全多方计算技术需要多个参与方频繁地交换加密信息，这导致通信带宽需求增加和延迟升高，从而在实时性要求严格的车联网应用中影响系统的响应速度和性能。为了降低安全多方计算的计算和通信开销，研究者提出了多种优化策略，主要集中在混合加密方案以及通信优化技术上。

混合加密方案结合了对称加密和非对称加密的优点，通过对不同的数据采用不同的加密方式，既保证了隐私保护的强度，又有效降低了计算复杂度。例如，对大规模数据的传输和处理，可以使用对称加密，因其计算效率高且适合大规模数据。而对小数据量和敏感数据的交换，例如用户身份、车速信息等，可以使用同态加密这种非对称加密，以确保数据隐私。这种混合加密方式能够在保证隐私的同时显著减少计算和通信开销，提高安全多方计算在车联网应用中的可行性。

安全多方计算的多轮交互特性，导致通信量随参与方数量呈线性或指数增长。通信优化技术通过减少通信轮次和降低单次通信量，来减少通信开销。通过将在线阶段的计算转换为本地计算和离线计算，以及设计并行机制将不相互依赖的操作进行并行计算，来减少通信轮次。减少单次通信量，可以通过优化底层操作，减少每次交互所需的通信量来实现。根据计算的不同，使用不同大小的域或环表示中间数据，以减少单次通信量。此外，密文压缩与批处理技术也可有效降低通信量。例如，应用 Huffman 编码与批量聚合技术，减少通信轮次和传输数据量。

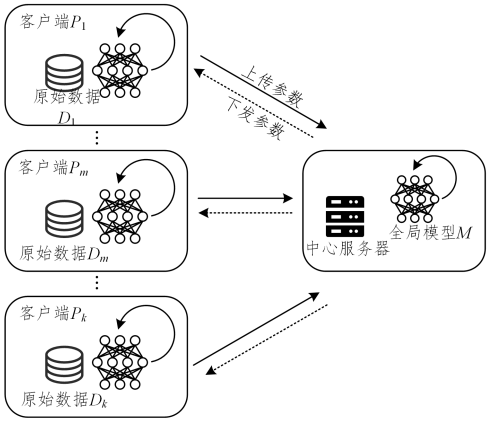
随着硬件加速技术的不断发展，将 ARM TrustZone 这类可信执行环境技术应用于车载设备，成为优化安全多方计算性能的又一有效途径[91]。其并行化模运算能力，可以显著加快同态加密等复杂操作的执行速度。同时，将高负载运算合理卸载至边缘服务器进行处理，车载设备仅负责接收并验证计算结果，这一举措极大地减轻了车载计算压力，显著提升了系统的整体运行效率。

5 基于联邦学习的隐私保护计算方法

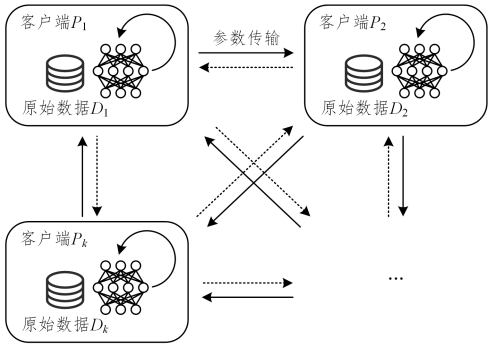
本章介绍的路线易于开发实现且具有较高性能，适用于隐私性、数据效用和效率均要求较高的分布式场景。该路线虽然避免了原始数据的直接传输，但车联网的应用场景中，终端车辆节点具有异构性，设备资源也有限，加之联邦学习本身的隐私和性能问题，往往需要结合其他技术，以提升联邦学习在规模大且分布广的移动车联网场景中的适用性。

5.1 联邦学习

联邦学习(Federated Learning，FL)的核心思想在于将原始数据在本地存储和计算的数据分离，使得参与方能够在不共享原始数据的情况下进行数据分析和模型训练[100]，其本质上是一种分布式机器学习。常见的联邦学习架构为客户端-服务器架构，当没有中心服务器时，联邦学习采用端对端架构(见图 4)。



(a)客户端-服务器架构



(b)端对端架构

图 4 常见的联邦学习架构

Fig. 4 Common FL architecture

在车联网边缘服务架构中，移动设备、基站或边缘服务器等具有一定的计算和存储资源，可以充当中间聚合节点。因此，客户端-服务器架构与车联网边缘服务架构具有良好的适配性[10]，本文着重介绍在此架构下的联邦学习。

设有 k 个客户端$\{P_1, P_2, \cdots, P_k\}$，它们的本地数据分别表示为$\{D_1, D_2, \cdots, D_k\}$。传统的集中式机器学习先将所有数据集汇聚到服务器端，并将其合并为 $D=D_1 \cup D_2 \cup \cdots \cup D_k$ 进行训练，得到模型M_{SUM}。而联邦学习则允许各客户端(终端设备等)使用其本地原始数据训练本地模型，并将这些本地模型聚合，以协同训练全局模型M_{FED}。在客户端-服务器架构下，联邦学习的具体步骤如下。1)模型初始化。中心服务器初始化全局模型参数 w。2)下发全局模型。中心服务器选取 m 个终端参与联邦学习，将全局模型结构和参数发送给这 m 个客户端。3)本地模型训练。客户端 P_k 获得全局模型后，利用本地收集的私有数据进行模型训练，并更新本地模型。参数向量 $\boldsymbol{w}^k$ 对数据集 D_k 中的实例(x_i, y_i)产生的损失函数为 $f(\boldsymbol{w}^k, x_i, y_i)$，其反映了模型输出和真实训练标签之间的差异。联邦学习的模型学习过程是求解最优模型 $\boldsymbol{w}$，以使全局损失函数最小化。与机器学习一样，联邦学习的核心任务同样包括分类和回归两类问题[70]，针对不同任务特性，需采用不同的损失函数。4)上传本地模型。客户端将训练好的模型更新参数 $\boldsymbol{w}_{t+1}^k$ 上传到中心服务器。5)聚合、更新。中心服务器收集客户端上传的本地参数，执行聚合算法，更新全局模型。联邦平均算法(Federated Averaging Algorithm，FedAvg)[100]是最常用的模型聚合算法之一。该算法将各客户端本地训练好的模型参数进行加权平均。迭代执行步骤 2)—步骤 5)，直至全局模型收敛或训练终止。训练完成后，根据需要选择是否将最终模型发布，以供服务请求者使用。

5.2 车联网联邦学习面临的挑战

在车联网中使用联邦学习，能够通过避免直接共享用户数据来保护隐私，利用车联网中分布的设备资源来提高资源利用率，通过学习更新模型适应不断变化的数据和环境。虽然 Lin 等[50]针对车辆列队行驶系统的网络攻击与隐私问题，提出了一种基于联邦学习的分布式异常检测框架，其通过混合攻击模拟与去中心化检测机制，显著提升了协同驾驶系统的安全性与隐私保护能力，但是，如图 5 中的加粗标识所示，车联网固有的开放性、异构性和动态性仍会影响联邦学习的实际应用效果。

首先，隐私泄漏呈现技术升级态势。车联网边缘场景的开放性导致联邦学习参与节点易遭受攻击，不可靠节点(车辆或边缘服务器)可通过投毒攻击等恶意手段破坏全局模型训练效果，甚至诱导隐私泄露。此外，目前已有研究表明，联邦学习中间参数的传输和更新仍然面临梯度反演等攻击[101]。攻击者不仅可以通过梯度还原原始数据，还能根据中间参数推断掌握的记录内容是否来自某个特定参与者[35]。Geiping 等[102]的研究进一步证明，从参数梯度的知识中可以重建高分辨率的图像，即使对于经过训练的深度网络来说，这种隐私的打破也是可能的。

其次，终端异构性与动态网络环境形成双重制约。车联网的终端设备数量众多且分布广泛，设备间存在显著的硬件异构性和计算能力差异，这使得各节点在参与本地模型训练

时表现不一致，容易导致全局模型更新出现数据偏斜和收敛缓慢问题。此外，车辆高度的移动性，会导致网络环境变化频繁。网络连接的不稳定和带宽波动，会使得模型参数在频繁上传和同步过程中面临较高的通信开销和延迟风险。

再者，信任管理和激励机制尚不完善。车联网允许车辆与附近的车辆进行通信。但是，当这些相邻车辆彼此不熟悉时，在它们之间建立完全信任变得具有挑战性[62]。当网络中存在恶意车辆时，问题会变得尤为严重。这些恶意车辆可能会故意进行攻击，从而导致隐私泄露。此外，车辆终端的自利性（如担心数据泄露或能耗增加）会导致参与意愿不足[103]。因此，如何将隐私保护计算技术与性能优化方法结合到车联网场景下的联邦学习，以取得模型精度、效率成本以及隐私安全之间的平衡，是此路线的一大挑战。

目前，学术界主要从隐私保护、客户端选择、聚合更新以及模型训练角度，来应对车联网边缘场景下联邦学习的隐私、模型精度以及开销和效率问题，具体如表 8 所列。

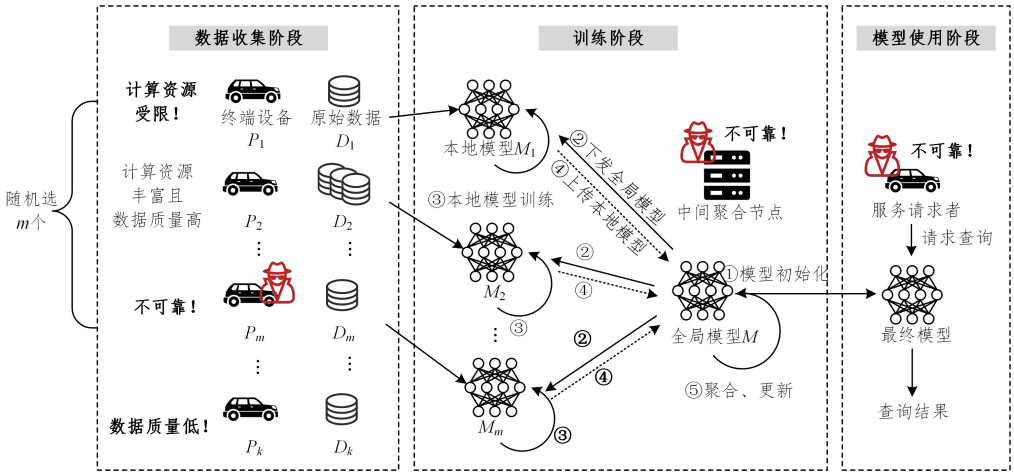


图 5 车联网边缘联邦学习架构

Fig. 5 FL architecture in the edge environment of IoV

表 8 车联网联邦学习优化技术

Table 8 FL optimization technology in the IoV

技术角度	方法	特点	隐私	模型精度	开销和效率
隐私保护	密码学[70]	对模型精度损失小	√		
	差分隐私[67]	轻量；需要平衡模型精度和隐私	√		√
	可信硬件[74]	将模型及数据汇聚到可信环境中	√		√
客户端选择	随机选择[100]	实现简单，但无法针对不同参与方的数据特点进行优化			√
	客户端评估	评估数据质量[68]		√	√
		评估存储、计算和通信资源[10]			√
		信任机制，减轻不可靠参与方的负面影响[36]	√	√	
	激励机制	根据参与方贡献给予相应激励[104]		√	√
	参与方选择率[105]	根据数据属性集和动态环境使用固定比率；使用离群点检测			√
聚合更新	聚合方式[106]	同步[107]；需等待所有参与方完成上传			√
		异步[108]；随时聚合更新			√
	调整聚合的次数及频率[109]	以更少的迭代次数实现相同的模型精度			√
模型训练	压缩[110]	模型压缩，剪枝、蒸馏[111]、稀疏化等	√		√
		梯度压缩，裁剪等	√		√
		数据压缩，模糊泛化等	√		√
	计算卸载[5]、边缘缓存等[11]	借助多设备[5]			√
	联邦学习框架分层分级[112]	设计联邦架构			√

5.3 车联网联邦学习的隐私保护优化

目前，学术界已经提出了许多将联邦学习与其他技术结合所形成的不同维度的工作，以保护训练数据、中间参数或输出结果隐私[113]，如同态加密、差分隐私、可信执行环境。

引入差分隐私的联邦学习方法具有明显的轻量级优势，并且可以在训练数据、梯度参数、模型训练的目标函数或输出结果上添加噪声扰动。在车辆层面使用差分隐私可以更好地保护数据在传输和存储期间的隐私，但会导致数据机密性与可用性的平衡问题更加困难。Batool 等[67]利用拉普拉斯机制在车辆的训练数据中添加噪声后计算模型参数 $W=\frac{1}{n}\sum_{i=1}^{n}w_i^{dp}$，服务器聚合客户端的模型参数后在平均值中加入噪声 $W=\frac{1}{n}\sum_{i=1}^{n}w_i^{+}\eta$。该方法在 10 次迭代内实现了较高的模型准确性，当 ε 为 0.5 时，本地和全局模型的平均精度分别为 81.53%和 87.3%。梯度扰动是将梯度裁剪到一定范围后添加满足差分隐私的噪声，对训练的目标函数没有要求，适用于大部分模型训练场景[114]。函数机制是在目标函数上添加扰动。由于函数机制对目标函数所添加的噪声量与数据维度、

数据集大小有关，在高维数据场景下会对目标函数引入过多噪声，因此与梯度扰动相比，函数机制不能直接用于车联网的联邦学习中。该机制需要将目标函数转换为关于模型权重的多项式形式，然后计算出多项式系数的敏感度，并对多项式系数添加满足 ε-DP 的拉普拉斯噪声。Zhao 等[68]在训练过程中使用函数机制扰动神经网络的目标函数，实现了 ε-DP，并利用指数机制聚合局部模型。该方案对不可靠的参与者具有鲁棒性，且模型精度接近传统集中式训练模型方案的精度。该方案虽然能够进一步避免共享模型参数导致的隐私泄露，但是不支持用户在训练过程中离线。函数机制不会对训练时的梯度结果做出任何限制或裁剪，因此模型可用性更高，但当参与方持有大量低质量或非独立同分布（Non-Independent Identically Distributed，Non-IID）数据时，会出现权重发散的问题[115]。即便联邦学习的过程中没有泄露参数，攻击者也可通过反复查询推测某条记录是否属于训练集或推测模型的具体参数。通过衡量函数的敏感度，在训练完成的模型参数上添加噪声，也可以为整个模型提供隐私保护。尽管通过压缩隐私预算及增加噪声规模能够达到更好的隐私保护效果，但是过多的噪声也会影响模型训练的准确性[68,116]。减少训练的迭代次数，以及降低每轮迭代所计算梯度的维度等方法，可以减轻噪声对模型精度的影响。Zhang 等[117]设计了自适应本地差分隐私机制，将较大的隐私预算分配给低抗攻击性的参数，并结合裁剪和随机化操作，以实现隐私-效用平衡。Li 等[69]则针对联邦学习中的成员推理攻击问题，提出动态调整隐私预算和噪声注入策略，为进一步降低通信开销，研究引入了 TernGrad 三元梯度量化技术。实验结果表明，当隐私预算系数 $C>1$ 时，模型准确率显著优于传统差分隐私方案，与无隐私保护场景的差距缩小至 2.1%～3.4%。在 MNIST，Cifar10，Cifar100 和 SVHN 数据集上，训练梯度的通信量分别减少了 93.33%，93.56%，93.60%和 93.74%。在 85%，90%，95%的压缩率下，模型准确率与未压缩场景的差异均小于 0.8%。

在联邦学习中引入密码学技术，让参与方之间传输加密的中间参数，可以保障用户数据和模型参数的隐私。Kong 等[70]利用同态阈值加密系统进行密钥的建立与更新，利用有界拉普拉斯机制和跳过列表保护本地模型更新，平衡了计算复杂度和隐私保护。用户加入和退出的计算复杂度分别为 $O(\boldsymbol{w})$ 和 $O\left(\boldsymbol{w}*\left\lceil\frac{n}{w}\right\rceil\right)$，在参与者波动时，计算效率也较高。Li 等[104]基于阈值 Paillier 加密系统，确保每个用户的梯度和每个梯度分量的可靠性不暴露给任何其他参与者。该方案中每个用户的计算复杂度为 $O(M+L)$，通信复杂度为 $O(L)$。实验表明，该方案的最终精度高于 SecProbe[68]，并且在获得相同精度时，所需的迭代次数少于 SecProbe。Li 等[72]构建了一个基于 Paillier 的通信协议，实现了中央服务器上安全的模型参数更新，保护了每个协作基站的真实更新。此外，同态加密不适用于层数深的机器学习模型，容易出现密文爆炸问题。秘密分享中，各个参与方基于秘密共享份额的本地计算和明文下的本地计算（如本地的矩阵乘法）的复杂度一致。Liu 等[118]提出了一个基于秘密分享和权重掩码的轻量级隐私保护协议，其可以在不损失模型精度的前提下保护梯度隐私，并且能够抵抗设备掉线和设备间的共谋攻击。另外，也可以引入其他密码学技术来保护模型隐私。Huang 等[73]设计了一种基于密文策略属性的加密机制来保护预测模型，但这种加密类型的技术通常面临参与方计算效率和模型安全性的权衡问题。实验表明，随着迭代次数的增加，预测模型的 MAE，MSE 和 RMSE 指标逐渐收敛，性能趋近于长短期记忆（Long Short-Term Memory，LSTM）模型，为隐私保护下的模型优化提供了理论依据。Xu 等[75]基于 shamir 秘密共享方案、pallier 同态加密方案和盲因子保护等方法设计的车联网数据聚合协议，可以保证模型参数的隐私性。

表 9 对比分析了车联网基于联邦学习的隐私保护优化工作。

表 9 车联网联邦学习的隐私保护优化

Table 9 Optimization of privacy protection for FL in IoV

研究工作	隐私泄露风险	策略特点	数据效用	开销	可扩展性
扰动训练数据[67]	中低/基于 LDP，能抵御差分攻击，在推理攻击和梯度泄露攻击下是安全的	扰动训练数据，拉普拉斯，ε-DP，ε 为 0.0001～2.0	中	中高	中高
SecProbe[68]	中低/基于 DP，能抵御差分攻击	扰动目标函数，拉普拉斯，ε-DP，ε 为 0.01～100	高	低	中高
三元联邦学习[69]	中低/理论分析，可防御成员推理攻击，每个用户的明文数据不会在交互下暴露给云服务器或其他用户	动态调整隐私预算和噪声注入策略；TernGrad 三元梯度量化	高	中	中高
改进的 FedLoc[70]	中/理论分析，能保护模型超参数	有界拉普拉斯，ε 为 0.05 和 0.1	高	中	中高
FEEL[71]	中低/基于同态加密的安全性	构建了基于 Paillier 的通信协议；设计了两种簇间学习和簇内学习算法	高	低	高
EPPFL[72]	中低/理论分析，每个用户的明文数据不会在交互下暴露给云服务器或其他用户	迭代执行“排除不相关部分”和“加权聚合”	中高	低	中高
FedLSTM[73]	中高/理论分析，模型及任务的信息不会被获取	基于密文策略属性的加密机制	高	低	高
数据聚合[75]	中低/基于同态加密、秘密共享等技术的安全性，能抵御 RSU 与车辆的合谋攻击，防止模型参数泄露	基于 shamir 秘密共享方案、pallier 同态加密方案和盲因子保护设计协议；设置动态训练时间窗口	高	低	高

5.4 车联网联邦学习的性能优化

上述将联邦学习与其他隐私保护技术结合的做法虽能够提高隐私保护的程度，但会给联邦学习方案引入额外的计算和通信开销，降低模型精度和算法效率。对车联网中基于联邦学习的隐私保护计算方案的性能优化，可从客户端选择、聚合更新以及模型训练这 3 个联邦学习的关键环节入手。

1）客户端选择

在车联网的实际应用场景中，数据分布（如数据样本分布、样本新鲜度等）、模型结构、系统边缘设备资源、参与意愿以及通信网络等方面存在差异[1]。这种异构性不仅会影响训练的准确性，甚至导致最终模型无用，还不利于提升训练的效率[1]。因此，在车联网边缘服务这种环境下，为联邦学习训练选择合适的参与方尤为重要[1]。

最简单的客户端选择方法是随机选择，由 Google 最早提出的联邦学习算法 FedAvg 就采用了该方法[100]。随机选择虽然可以保证公平性和均衡性，却无法针对不同客户端的数据特点进行优化，如可能导致数据质量更优的客户端未被机选中。

鉴于随机选择的局限性，部分研究采用客户端评估方法。该方法通过评估各客户端的数据分布、存储计算资源、可信度等情况，有针对性地选择更优客户端参与车联网的联邦学习。

车联网中设备众多，其在数据分布、资源和信任度等多方面都存在较大差异。各客户端生成和收集的数据通常为 Non-IID[71]。针对这一数据样本异构问题，常采用基于数据质量评估的客户端选择方法。Zhao 等[68]使用辅助验证数据计算每个参与者的效用分数，然后以特定概率接受参数。Hui 等[119]综合考虑了 Non-IID 度和数据冗余度，建立了数据重要性模型。Saputray 等[1]同时兼顾车辆的位置和数据质量。

针对存储和计算资源异构的问题，可以选择具有丰富资源的客户端进行联邦学习，以提高联邦学习的效率。例如，Guo 等[120]对服务器和客户端进行分组，能够显著缩短本地训练的等待时间，且不影响学习精度。Li 等[121]提出了一种考虑车辆选择和无线资源分配的任务驱动车辆联盟算法。Jai Vinita 等[122]考虑了车辆的计算能力和通信链路质量，根据可访问内存、数据记录、剩余能量以及链路强度等因素，在 RSU 和基站执行基于模糊逻辑的车辆选择技术，以加快全局更新。Zhang 等[123]针对车联网中车辆高速移动与动态信道导致的联邦学习性能挑战提出的方案，通过移动性感知的车辆选择、信道自适应的加权聚合及计算通信资源联合优化，在保证延迟与能耗约束下，显著提升了模型精度与训练效率。

针对车联网联邦学习训练过程中存在的不可靠参与方（半诚实但好奇的参与方、恶意参与方）[36]，如果没有建立起对参与方的信任机制，恶意参与方可以通过故意改变本地数据（数据中毒）或梯度上传（模型中毒）来发起攻击，导致模型精度降低，甚至是隐私泄露[124]。Zhou 等[36]通过整合基于对数的归一化机制以及基于声誉的加权聚合，限制了可疑梯度，放大了可信梯度。此外，在不同节点之间进行合理的网络选择，也是一种减少数据传输延迟和成本的方法。例如，Shinde 等[10]将 FL 网络选择问题建模为基于马尔可夫决策过程的顺序决策问题，从而降低了整体 FL 过程成本。

在隐私需求下，终端车辆节点参与联邦学习的主观意愿可能不足。为了激励终端车辆节点加入训练，须公平、合理地评估参与方的贡献，并给予其相应激励[125]，以提高模型的精度、收敛速度和泛化能力[126]。Li 等[104]考虑了诚实但好奇的边缘计算服务器和恶意车辆，提出了一种基于区块链和声誉的激励机制。Zhao 等[127]综合考虑本地数据规模、历史模型性能、时间约束和系统性能，提出了一种基于尽力而为（Best-effort）训练机制和多准则贡献评价方法的物联网客户选择机制。Li 等[128]提出了基于斯塔克尔伯格（Stackelberg）博弈的分层联邦学习激励机制。该方案将用户设备、无人机和基站之间的交互建模为斯塔克尔伯格博弈，通过调整参与方的效用，确定模型训练所需的最大数据量以及用户设备和无人机的数量，实现了博弈过程中参与者收益的最大化，提高了用户设备的质量和联邦学习模型的性能。鉴于车联网边缘场景在实际运行中存在与上述研究相似的需求，该方法或有借鉴意义。

上述的维度是如何选择合适的客户端，而参与方选择率为客户端选择提供了一个新的维度。目前的方法有两种：一种是根据数据属性集和动态环境使用固定比率，另一种是使用离群点检测[105]。例如，根据参与方的训练时间和通信时间，应用离群点检测技术来检测联邦学习的环境是否发生了变化，以便决定在不同轮次中选择多少客户端及选择通信渠道等[105]。

2）聚合更新

针对车联网这样的边缘服务场景，各参与方的计算能力、存储容量、网络带宽等方面资源有限，且车辆状态（位置、在线情况等）会动态变化，仅从客户端选择这一角度，难以保证联邦学习在车联网边缘服务场景下的整体性能。联邦学习的模型聚合方式会影响模型的精度及资源消耗。根据聚合更新方案的不同，可以分为同步联邦学习（Synchronized Federated Learning，SFL）和异步联邦学习（Asynchronous Federated Learning，AFL）两种（见图 6）。

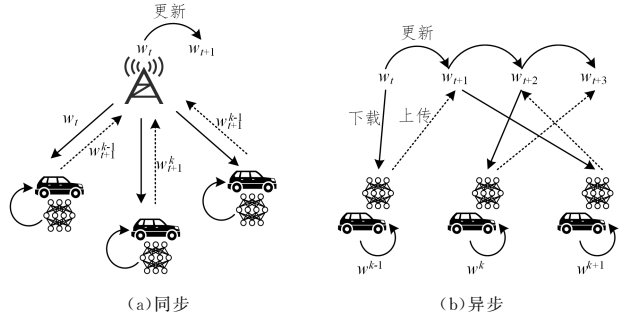


图 6 联邦学习模型的聚合方式

Fig. 6 FL model aggregation method

FedAvg 算法通过让参与方在本地多次执行随机梯度下降算法，实现了以更少的通信轮数训练出相同精度的模型，降低了通信开销。Wu 等[107]简化了 FedAvg 的聚合过程，将深度神经网络的层数作为通信轮数的阈值，提高了通信效率，并减少了中心控制器的计算资源消耗。同步联邦学习虽然易于实现，但需等待所有参与方完成上传，若存在训练速度慢或突

然离线的参与者时，可能会导致较长的通信延迟，甚至导致全局学习进度暂停[108]。而在高移动性且有异构设备的车联网场景下，不同设备间的可用性和训练速度是不同的，计算资源和电池时间是有限的，实现全局同步化颇具难度[84]。

异步联邦学习允许参与方按自身速率更新模型，无论其他参与方的训练进度如何，可随时聚合已经接收到的本地更新，缓解了客户端训练速度慢和数据质量不高的问题，加快了训练过程[129]。Wu 等[129]提出了基于 FedAvg 的半异步联邦平均协议，引入滞后容差参数，减轻了滞后、脱机、模型过时的影响。Mo 等[108]结合遗传算法构造了基于通信资源优化的 AFL 算法，通过减少单轮次联邦学习所需的通信资源来降低系统整体通信开销。然而，参与方之间的异步更新，可能会导致全局模型的不一致和收敛速度的下降，且会使得客户端更频繁地参与，造成潜在的资源浪费。因此，在训练过程中，须考虑充分利用每个客户端配额来最大程度地提高资源利用效率。

除了同步、异步的聚合方式外，聚合的次数及频率也会影响到联邦学习的性能。如果能够以更少的迭代次数实现最终的精度，那将促进联邦学习在车辆网络中的快速部署和应用，为车联网服务带来更高的效率、更优的性能和更好的用户体验。

3)模型训练

客户端的主要计算开销源于模型参数更新时的计算，主要的通信开销来源于模型传输时所需发送的数据。因此，可以对模型进行压缩(如知识蒸馏、剪枝[110]、稀疏化等)，以减小模型的规模，减少存储和通信资源的开销，同时降低模型参数泄露的风险。Shang 等[111]通过利用全局模型的知识来指导本地训练，以解决联邦分心驾驶检测中数据的 Non-IID 问题，并引入额外的注意力损失来微调聚合的全局模型，降低了训练的波动性。对梯度或数据进行压缩，如采用模糊泛化这种基于语义的优化策略，虽然减小了数据的规模，但会导致部分信息的丢失。

此外，还有研究通过计算卸载、边缘缓存等方式进行资源扩展[5]。无人机(Unmanned Aerial Vehicle，UAV)可作为中间聚合节点参与模型训练，减少用户设备与边缘基站之间的通信次数，提高通信效率，还能解决数据远程传送的高延迟和链路故障问题。Oualil 等[130]通过分散的区域 RSU 来增强本地模型，实现了更准确的个性化边缘缓存和替换决策。另外，有研究通过将联邦学习框架分层分级，在车辆端进行部分训练，根据客户端的计算能力分配不同大小的模型，减轻服务器的存储和计算负担；或筛选与用户之间距离短的数据处理计算节点，减少数据传输和延迟，降低服务器的通信负担。例如，Zhao 等[112]采用“客户端-边缘-云”架构动态优化共享模型和异步参数聚合算法自动调整每个边缘模型参数的混合权重。Li 等[12]面向车联网延迟敏感任务，提出多任务联邦学习框架，支持动态优先级调度与资源分配，并设计了基于匹配博弈的车辆联盟机制，显著提升了模型的收敛速度与网络稳定性。Zhang 等[113]提出鲁棒且具有隐私保护功能的联邦学习框架 RUPT-FL，其利用打包秘密共享、安全多方计算和同态加密技术，设计了多 RSU 辅助的模型上传方案，以及在双服务器模型下的身份无关共享重建和模型聚合协议。

6 基于可信执行环境的隐私保护计算方法

除了使用基于算法、软件的方法确保隐私性，还可以借助基于硬件的技术进一步实现更安全、高效的车联网边缘隐私保护。本路线的核心是通过软硬件隔离安全机制建立一个可信赖的执行环境，将关键数据和操作放在这个受保护的环境中进行，从而保证关键数据和代码的机密性[42]。本路线支持多层次、高计算复杂度的算法逻辑[131]，能够实现密文传输和明文计算；同时避免了额外的通信开销以及基于密码学的大量计算开销，适用于需要平衡实时性和隐私性的场景。但车联网领域的动态性、异构性，硬件安全漏洞(如侧信道攻击[132])，以及不同 TEE 构建技术的差异，会影响到数据的兼容性和互操作性。

6.1 可信执行环境

可信执行环境(Trusted Execution Environment，TEE)[133]是密码学和系统安全的结合，它通过软硬件隔离安全机制建立一个可信赖的执行环境，能够保证其内部加载程序和数据的机密性[76]。

常见的 TEE 方案构造一般基于硬件飞地(Enclave)计算模式，即把所有隐私数据相关的计算放入物理隔离的飞地中执行。完整的流程大致为 TEE 硬件设备注册、可信执行程序部署、可信执行程序调用 3 个步骤。Intel 的 SGX(Software Guard Extensions)[1)]是其中一种较为成熟的可信执行环境方案。SGX 不依赖于固件和软件的安全状态，而是在原有架构上增加了一组新的指令集和内存访问机制，在应用程序的地址空间中划分出一块受保护的区域，用于存放应用程序的敏感数据和代码，使得应用程序能够在 Enclave 中运行，并且只有位于 Enclave 内的代码才能访问 Enclave 的内存区域。在 SGX 中，每个 Enclave 都是相互隔离的，即使其中一个 Enclave 中存在恶意程序，也无法访问和危害其他 Enclave 的内容。

TrustZone[2)]是 ARM 提出的一种硬件强制隔离技术，在处理器层面上，它将一个 CPU 分成普通世界(Normal World)和安全世界(Secure World)两个不同权限的保护域，通过安全监视器调用指令通信。安全世界中的任务只能在单个处理器上执行，始终使用安全的小内核提供 TEE，机密数据可以在 TEE 中被存储和访问，并且安全世界中运行的程序可以正常访问普通世界中的资源。该方案适用于资源受限的边缘设备[131]。但由于其监控模式切换、安全外设管理等核心细节受知识产权保护，技术细节多体现于非公开的芯片设计文档或内部白皮书，而非学术论文，这导致独立研究者难以深入分析其安全机制。

6.2 现有方案的应用现状分析及存在的问题

Intel SGX 支持本地和远程认证机制，允许不同实体(如

1) https://www.intel.com/content/dam/develop/external/us/en/documents/329298-002-629101.pdf

2) https://developer.arm.com/documentation/PRD29-GENC-009492/c?lang=en

车辆、路侧单元、云端服务器）验证 Enclave 的完整性与运行环境的可信性。该机制可保障车联网边缘服务中的计算过程安全和数据安全，使验证者能够确认 Enclave 内的代码与数据未被篡改，且运行于受信任的环境。在联邦学习场景中，SGX 被用于保障模型参数安全。Zhao 等[74]利用 SGX 原语将模型上传到配备 SGX 的聚合服务器，保证了联邦学习的聚合隐私。然而，SGX 本身无法抵御侧信道攻击，再加上飞地可使用内存太小、用户态运行模式须频繁与不可信区域交互等问题，存在安全风险和系统开销。为缓解上述问题，Zhao 等[74]进一步提出行主数据存储和列主数据存储两种模式，通过优化数据访问路径来适配不同聚合算法，提升了联邦学习效率。

TEE 可为车辆身份信息、行驶记录等敏感数据提供隐私保护，能够支持复杂度高的算法，适用于车联网中对计算能力要求高的场景。Chen 等[77]结合 TEE 和多重签名技术，设计去中心化信任管理系统，利用 TEE 保护信任评估过程，利用多重签名增强区块链共识安全性。该方案通过分层架构实现并行处理，由基站的 TEE 集中执行安全敏感操作，从而减少对中心化服务器的依赖，并提升系统的整体效率。当 TEE 与其他隐私增强技术（如安全多方计算）结合时，可以进一步提升数据规模量级，增强数据隐私性并优化方案性能[77]。

然而，在车联网边缘场景中，TEE 技术面临三重核心矛盾。1）硬件安全与动态拓扑的冲突。车联网节点的高移动性要求动态调整安全边界，而现有 TEE 方案（如 SGX）多依赖静态隔离策略，导致节点快速切换基站时的认证延迟激增。2）异构架构下的互操作困境。不同厂商采用异构 TEE 技术，导致数据交互效率低[4]。例如，TrustZone 的单处理器执行模式虽可确保安全世界的确定性调度，却制约了多任务并行处理能力，难以满足高并发场景的实时性需求。3）资源效率与隐私安全强度的权衡。TEE 的内存加密与上下文切换操作会消耗边缘设备资源，路侧单元部署 SGX 后，决策延迟增加，而轻量化方案虽能降低内存占用，却会牺牲计算能力。

7 挑战及未来展望

7.1 挑战

车联网边缘服务的快速发展催生了海量多模态数据的实时交互需求，但指数增长的数据规模与大规模部署的边缘节点，使得隐私数据的暴露面持续扩大。根据第 3－6 章的分析，当前隐私保护计算方案在车联网场景下的应用仍面临多重挑战。

1）动态拓扑与通信不确定下的隐私泄露风险加剧。车联网采用 V2X 通信架构，车辆与边缘节点间的通信链路易受干扰，车辆在高速移动中可能瞬间脱离原有边缘服务器的覆盖范围，须与邻近基站或路侧单元重新建立安全通道。这种动态性为窃听攻击和重放攻击等网络攻击手段提供了可乘之机。随着量子计算等先进技术的发展，单纯依靠某种特定的加密技术来保护隐私也可能面临被破解的风险。现有量子安全多方计算技术虽然可以为 V2X 中的数据传输和计算提供更高的隐私性保障，但其技术复杂性较高，难以在边缘设备有限的计算资源下实现高效的数据加密处理。基于可信执行环境的隐私保护计算技术虽能作为密码学方案的补充，但其部署成本高、对硬件供应商的依赖以及易受侧信道攻击的弱点限制了其应用。

2）终端自私性和激励机制不完善下的隐私保护与数据效用的失衡。车联网终端具有天然自私性，车辆可能为节省本地资源或避免隐私泄露风险，拒绝参与数据共享或联邦学习，导致整体服务质量下降。现有车联网中的激励机制难以平衡个体利益与集体效用，例如联邦学习中低算力车辆因需承担模型参数传输成本，普遍存在“搭便车”现象。这种自私性加剧了数据 Non-IID 程度，降低了模型泛化能力。另外，现有不同的车联网应用场景对数据精度要求不同，严格的隐私保护措施通常会导致数据可用性下降。尽管模糊泛化、差分隐私技术可以依据用户偏好调整数据粒度，但基于这些技术的方案服务场景的适配性有限，难以协调隐私保护和数据效用间的动态矛盾，从而无法在保证隐私保护的前提下充分挖掘数据的价值[47]。

3）终端异构性与资源约束下的性能瓶颈。理想的车联网边缘服务架构应具备快速处理终端设备收集的数据、在边缘节点进行实时分析和决策、实现不同设备和节点之间的数据高效共享的能力。然而，随着车联网终端设备的多样化和大规模化，多模态信息会更加广泛，车联网数据收集及处理的压力必然会增大。由于边缘设备的算力有限，现有隐私保护计算方案在计算性能、通信效率等方面的问题愈加突出，进而影响车联网服务的实时性和响应速度。此外，联邦学习这种分布式计算框架在有算力差异的异构边缘节点协同中面临通信开销与延迟问题，影响了模型聚合效率。此外，安全多方计算中的通信协议规范化、标准化不足，导致异构设备间互操作性差，进一步制约了处理效率。

4）车联网大规模部署下的可扩展性的局限。可扩展性反映了方案能否适应车联网规模扩大、需求变化、多方参与及隐私保护强化等要求，能否保障车联网的高效运行与持续发展。现有架构难以支撑千万级终端设备的动态接入与多模态数据（激光雷达、视觉等）的协同处理，会导致跨域数据共享时延激增。这对边缘计算架构的灵活性提出了更高的要求。例如，联邦学习在节点频繁加入/退出场景下，模型收敛速度下降，而区块链技术在边缘节点高密度接入时，网络吞吐量降低，形成新的性能瓶颈。这些系统性缺陷，暴露出当前架构在应对大规模多模态数据协同处理时的体系性不足。

7.2 可能的研究方向

7.2.1 隐私保护强度提升

挑战 1 的本质在于动态通信环境与攻击技术演进对隐私保护构成的双重挑战：一方面，V2X 通信架构的高流动性特征导致连接重构过程中出现安全真空区；另一方面，量子计算等新兴技术对传统加密体系形成代际冲击。这种“动态威胁＋技术代差”的叠加效应，使得现有隐私保护机制在响应速度、抗攻击性和资源适配性之间难以取得平衡。如何构建主动防御体系以适应动态威胁，如何通过技术融合突破数据共享的信任瓶颈，成为当前亟需解决的核心问题。

1）人工智能驱动的隐私攻击防御体系

车辆等边缘设备所产生的大量实时动态数据为攻击者提

供了数据关联性、整合分析和隐私挖掘的潜在机会。针对这种多样化的攻击形式以及涉及大量多模态数据的情况，需要聚焦 AI 赋能的动态防御体系构建[134]，监测车联网中的隐私漏洞，并相应地实施保护措施。

第 3—6 章提到的隐私保护计算方法，是建立在已知要保护的数据目标上的。但从现实来讲，在设计隐私保护计算方案时，难以全面地考虑到所有敏感数据。目前，已有部分学者从隐私识别入手[135]，以提高隐私保护计算方案的泛化性。未来，可以进一步研究通过使用自然语言处理（Natural Language Processing，NLP）、大语言模型（Large Language Model，LLM）等 AI 技术构建模型或算法，自学习国际上关于隐私保护的法律法规，并广泛调研用户隐私保护需求，构建动态的车联网隐私数据知识库[136]。在隐私风险评估领域，LLM 强大的语言理解能力，能够对文本数据中的隐私信息进行深度剖析与精准识别[137]。此外，针对车联网边缘服务场景中的隐私保护需求，可使用生成对抗网络、变分自编码器等深度学习模型合成具有相似特征的非敏感数据[138-139]，或基于循环神经网络、长短期记忆网络构建自学习、自适应的深度学习监测方案，实时、动态地监测车联网用户隐私信息，并动态调整隐私保护策略。

2）联邦学习与区块链的结合

区块链通过智能合约实现节点授权与任务分发[140]，确保联邦学习参数传输的透明性与不可篡改性，而联邦学习则通过分布式计算保留数据本地化优势，两者结合的核心价值在于，通过技术互补性解决分布式学习中的信任缺失、模型篡改及跨域协同问题，从而更能实现数据“采集可溯、计算可信、流通可控”的全周期治理，化解传统车联网边缘服务架构中的隐私泄露与单点故障风险[141]。

针对车联网动态场景下的恶意节点伪装与投毒攻击风险，设计基于区块链的联邦学习准入机制。在数据采集阶段，区块链可通过哈希链式结构记录数据来源与权属信息。在任务分发阶段，采用轻量级区块链构建优先级队列。针对数据机密性与存储开销，可构建链上、链下混合存储模型，将关键参数（如聚合后的模型权重哈希值）写入区块链，确保不可篡改，将非敏感数据（如训练样本统计信息）分布式存储。在数据交易阶段，区块链可通过链上确权（用户授权数据使用权通过智能合约记录，明确数据所有权与使用边界）、审计追踪（区块链完整记录数据交易全流程，监管机构可通过哈希值快速定位违规操作），有助于数据价值流通。在数据计算处理上，区块链则负责记录计算过程和结果，保证数据的可追溯性和可信度。

7.2.2 车联网架构下的隐私-数据效用平衡

挑战 2 的本质在于现有方案未能实现“用户需求-隐私保护-数据价值”的三维协同：一方面，用户隐私偏好具有动态性和异质性，例如对位置敏感而对驾驶行为容忍度高，但现有方案缺乏对个性化需求的精细化建模；另一方面，数据效用依赖准确性、完整性等多维度指标，但隐私保护强度的调整缺乏动态量化标准支撑。为此，亟需从用户行为洞察、个性化隐私服务、动态量化标准 3 个维度重构隐私-效用协同优化框架。

1）重视用户参与和个性化隐私需求

用户的隐私保护需求因人而异，部分用户可能由于缺乏对智能网联汽车、车联网服务等新兴事物的认知，而低估数据共享的隐私风险。此外，驾驶安全、隐私风险提示方式、先前的驾驶经验以及个性化的隐私偏好等因素，也会影响用户对隐私风险、数据分享利弊以及数据共享的决策[142]。为了建立可持续的用户关系并提高用户满意度，未来车联网隐私保护计算应更加重视用户参与和个性化需求。而个性化隐私服务的实现需要根据不同服务的特点和需求选择合适的隐私保护计算方法，为此，需要加强对用户偏好的研究和理解，采用更加先进的数据分析和机器学习技术，实时、准确地捕捉用户偏好的变化。例如，利用传感器数据和用户行为数据，通过深度学习算法来推断用户的实时偏好，从而为数据处理提供更加精准的依据。同时，建立用户偏好反馈机制，从而不断优化数据处理策略。

2）建立通用的隐私保护效果与数据可用性的量化及衡量标准

虽然已有学者基于参与用户与服务方各自成本收益的动态策略选取过程，构建了斯塔克尔伯格模型[128]，旨在通过博弈均衡获取最优的隐私设置策略，但要想根据不同的应用场景和需求灵活地控制隐私数据的精度范围，仍需要建立通用的隐私保护效果与数据可用性的量化及衡量标准，对车联网边缘数据的准确性、完整性、时效性等进行全面评估，并积极构建动态的数据隐私保护策略，根据用户的隐私偏好、数据的敏感程度和应用场景，动态调整隐私保护的级别，实现隐私保护与数据可用性的最佳平衡。

7.2.3 轻量化基础技术瓶颈突破

挑战 1，3，4 综合起来的本质在于物理层资源约束与协议复杂性的双重挤压：一方面，车辆和边缘设备受限于计算、存储与能耗约束；另一方面，安全多方计算的计算复杂度与通信开销难以适配动态通信场景。为此，亟需设计轻量化的隐私保护计算方法，通过算法优化与资源分配实现隐私与效率的动态平衡。

1）设计高效的轻量级隐私保护计算新方法

车辆和边缘设备的计算和存储资源有限，同态加密等密码学技术虽然能够实现较高的安全性，但它们通常需要进行较多的计算和存储操作，这会导致系统性能下降，从而对其他必要的车联网功能和应用产生影响。为了平衡保护隐私的开销与有限的边缘服务资源，一方面，可以通过改造现有的隐私保护计算方法，使之更加轻量化和高效化，以减少技术本身所带来的资源消耗，如可利用模型剪枝、量化以及知识蒸馏等技术开发轻量级方案；另一方面，则需要探索新颖的隐私保护计算技术，以最大限度地减少计算开销，提高效率，如结合算法优化与硬件加速实现计算性能的提升。

2）利用人工智能技术高效分配资源

车联网边缘服务对车辆的移动性和资源占用率非常敏感。不同的应用程序对隐私保护和服务质量（包括延迟、能耗、计算负载等）的要求程度不同[81]。车联网边缘服务架构作为层次型分布式结构，应充分利用分布式的特性，利用车联网边缘计算和协同计算的能力，将隐私保护

计算任务从中心服务器转移到车辆或边缘设备上进行处理，以减少数据传输和集中计算的需求，降低隐私泄露的风险，提高计算效率和加快响应速度，进而利于满足车联网规模扩大和需求变化的要求。但边缘计算涉及分布式数据处理，需要在多个节点之间进行协调和协作，这可能会增加数据处理的时间和复杂度，降低数据处理的效率和共享的灵活性，此外，不同节点的计算能力和存储资源可能不同[5]，也可能导致整体的实时响应时间增加。为此，可以利用人工智能技术自动高效地识别终端节点的特征，高效地组织和分配计算和存储资源。

7.2.4 “芯片-算法-标准”的全域生态协同

挑战3，4综合起来的本质在于破解车联网隐私保护计算的生态割裂困境：一方面，隐私保护计算技术的研究多集中在单一层面，如芯片层的硬件隔离技术、算法层的加密算法优化等，跨层协同的研究不足；另一方面，车联网行业需求的多样性使得现有技术难以满足实际应用场景的需求。为此，须构建覆盖芯片层、算法层、标准层的全栈协同体系，实现技术方案与产业需求的精准对齐。

不同的车辆技术和通信协议之间存在差异，基于软件开发的隐私保护计算方案存在兼容性问题，不同方案的数据格式、API接口等方面存在差异，导致难以在实际应用中实现互操作性。因此，需要构建多方协同兼容的隐私保护计算技术。跨域数据互操作性标准的制定，能够降低多参与方协作的门槛。而车联网的数据共享离不开通信协议。设计标准化的具有隐私保护的通信协议，可以简化设备之间的集成和交互，确保车联网异构设备之间的兼容性和互操作性，促进车辆和基础设施之间安全的数据交换。

针对车联网边缘动态接入场景的算力需求，也可联合车企、芯片商与算法团队开发定制化的车规级隐私保护计算芯片。该芯片须集成轻量加密引擎与联邦学习加速器，以适应动态接入场景中的算力需求，支持动态参数同步，实现算力密度提升。此外，须同步构建分层安全验证体系，在硬件层隔离敏感计算任务，在协议层集成V2X通信安全模块，在算法层预置噪声注入引擎。

结束语 本文系统梳理了车联网边缘服务场景下隐私保护计算的技术演进与研究进展。从隐私泄露风险、数据效用、开销与可扩展性4个维度出发，对基于数据变换、安全多方计算、联邦学习及可信执行环境的技术方案进行了全面评述，揭示了其在动态拓扑适配、多模态数据处理及资源受限场景下的性能边界与适用性差异。针对现有方案在隐私保护强度、隐私-数据效用协同优化、轻量化及跨域互操作性方面的不足，提出了AI驱动的动态隐私分配机制、车规级隐私计算芯片设计等关键方向。通过上述方向，车联网隐私保护计算技术有望实现从“理论可行”到“场景适配”的跨越，为智能交通系统的安全可信部署提供核心支撑。本文的框架梳理与技术展望，旨在为智能交通系统的隐私保护体系构建提供系统性参考，助力车联网产业的可持续发展。

参 考 文 献

[1] SAPUTRAY M，HOANG D T，NGUYEN D N，et al. Dynamic federated learning-based economic framework for internet-of-vehicles[J]. IEEE Transactions on Mobile Computing，2023，22(4)：2100-2115.

[2] FAN W，SU Y，LIU J，et al. Joint task offloading and resource allocation for vehicular edge computing based on V2I and V2V modes[J]. IEEE Transactions on Intelligent Transportation Systems，2023，24(4)：4277-4292.

[3] SHEN Z H，GAO Y S，WANG H，et al. Deep deterministic policy gradient caching method for privacy protection in Internet of Vehicles[J]. Journal of Jilin University(Engineering and Technology Edition)，2025，55(5)：1638-1647.

[4] Summary of Academic Research on China ’s Automobile Engineering · 2023[J]. China Journal of Highway and Transport，2023，36(11)：1-192.

[5] XU X，JIANG Q，ZHANG P，et al. Game theory for distributed IoV task offloading with fuzzy neural network in edge computing[J]. IEEE Transactions on Fuzzy Systems，2022，30(11)：4593-4604.

[6] HAN M，YANG C，HUA L，et al. Vehicle Pseudonym Management Scheme for Mobile Edge Computing Vehicle Networking[J]. Computer Research and Development，2021，59(4)：781-795.

[7] JIVTHESH M R，SAMUEL R M，GAUSHIK M R，et al. Smartverse：blockchain based crowdsourced V2X message verification and dissemination system[C]// 2023 15th International Conference on Communication Systems & Networks(COMSNETS). IEEE，2023：84-89.

[8] VIJAYAKUMAR P，AZEES M，KOZLOV S A，et al. An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs[J]. IEEE Transactions on Intelligent Transportation Systems，2022，23(2)：1630-1638.

[9] AGRAWAL N，BINNS R，VAN KLEEK M，et al. Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation[C]// Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. New York：ACM，2021：1-13.

[10] SHINDE S S，TARCHI D. Joint Air-Ground Distributed Federated Learning for Intelligent Transportation Systems[J]. IEEE Transactions on Intelligent Transportation Systems，2023，24(9)：9996-10011.

[11] DAI Y F，ZHOU X Z，FAN Z Y，et al. Key-driven trust mechanisms for identity authentication in vehicular networks[J]. Journal of Jilin University(Engineering and Technology Edition)，2025，55(5)：1788-1797.

[12] LI Z，WU H，LU Y，et al. Matching game for multi-task federated learning in internet of vehicles[J]. IEEE Transactions on Vehicular Technology，2024，73(2)：1623-1636.

[13] ZHANG X，WANG J，ZHANG H，et al. Data-driven transportation network company vehicle scheduling with users’ location differential privacy preservation[J]. IEEE Transactions on Mobile Computing，2023，22(2)：813-823.

[14] YU H，ZHANG H，JIA X，et al. PSafety：Privacy-preserving safety monitoring in online ride hailing services[J]. IEEE Transactions on Dependable and Secure Computing，2023，20(1)：209-

224.
[15] GHOSAL A, CONTI M. Security issues and challenges in V2X: A Survey[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2020, 169.
[16] HUANG J, FANG D, QIAN Y, et al. Recent Advances and Challenges in Security and Privacy for V2X Communications [J]. IEEE Open Journal of Vehicular Technology, 2020, 1: 244-266.
[17] LU R, ZHANG L, NI J, et al. 5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy[C]// Proceedings of the IEEE. 2020: 373-389.
[18] MOYA OSORIO D P, AHMAD I, SANCHEZ J D V, et al. Towards 6G-Enabled Internet of Vehicles: Security and Privacy [J]. IEEE Open Journal of the Communications Society, 2022, 3: 82-105.
[19] SEDAR R, KALALAS C, VAZQUEZ-GALLEGO F, et al. A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths[J]. IEEE Open Journal of the Communications Society, 2023, 4: 325-391.
[20] DENG Y K, ZHANG L, LI J. Research on Privacy Protection of Internet of Vehicles[J]. Application Research of Computers, 2022, 39(10): 2891-2906.
[21] LIU H, ZHANG L, LI J. Survey on Privacy Preserving Data Aggregation Based on Internet of Vehicles[J]. Application Research of Computers, 2022, 39(12): 3546-3554.
[22] ZHANG X Q, LIU Y W, LIU J X, et al. A Survey of Federated Learning for Edge Intelligence[J]. Computer Research and Development, 2023, 60(6): 1276-1295.
[23] HADDAJI A, AYED S, CHAARI FOURATI L. IoV security and privacy survey: Issues, countermeasures, and challenges[J]. Journal of Supercomputing, 2024, 80(15): 23018-23082.
[24] ABIDI R, AZZOUNA N B, TROJET W, et al. A study of mechanisms and approaches for IoV trust models requirements achievement[J]. Journal of Supercomputing, 2024, 80(3): 4157-4201.
[25] LI R Q, HU X Y, ZHANG J Y, et al. Research on Privacy Protection Technology of Internet of Vehicles[J]. Journal of Information Security, 20240, 9(2): 1-18.
[26] LI S, LI J, PEI J, et al. Eco-CSAS: a safe and eco-friendly speed advisory system for autonomous vehicle platoon using consortium blockchain[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(7): 7802-7812.
[27] WANG S, LI J, WU G, et al. Joint optimization of task offloading and resource allocation based on differential privacy in vehicular edge computing[J]. IEEE Transactions on Computational Social Systems, 2022, 9(1): 109-119.
[28] GUO B, LIU S C, LIU Y, et al. Intelligent Internet of Things: Concept, Architecture and Key Technologies[J]. Chinese Journal of Computers, 2023, 46(11): 2259-2278.
[29] ZHOU H, XU W, CHEN J, et al. Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities[C]// Proceedings of the IEEE. 2020: 308-323.
[30] WANG Z. Automotive Data Gets a "Safety Lock" [N]. People's Daily, 2021-12-26: 004.
[31] Summary and Analysis of Data Leakage Incidents in the Automotive Industry [EB/OL]. https://www.anyong.net/industrynews/1266.html.
[32] GOUPSEC. Volkswagen Group Suffers Severe Data Leakage in Europe, 800 000 Car Owners Can Be Located [EB/OL]. http://mp.weixin.qq.com/s?__biz=MzkxNTI2MTI1NA==&mid=2247501939&idx=1&sn=2a54c17ec6b87ad1ed5a0d59689c9885&chksm=c08436f7495fe0ac6a95d1e79bb9377239d4d1bc6c4ecfe231a62365171a263aa46d544d9678#rd.
[33] U. S. Automotive Parts Giant AutoZone Suffered a Cyber Attack [EB/OL]. https://cn-sec.com/archives/2237681.html.
[34] YANG Z Y. Add a "Safety Lock" to Automotive Data [N]. Economic Daily, 2022-12-23: 009.
[35] WANG Z, HUANG Y, SONG M, et al. Poisoning-assisted property inference attack against federated learning [J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(4): 3328-3340.
[36] ZHOU H L, ZHENG Y F, HUANG H J, et al. Toward robust hierarchical federated learning in internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(5): 5600-5614.
[37] LIU L, WANG Y, LIU G, et al. Membership inference attacks against machine learning models via prediction sensitivity[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(3): 2341-2347.
[38] AZEES M, VIJAYAKUMAR P, JEGATHA DEBORAH L. Comprehensive survey on security services in vehicular ad-hoc networks[J]. IET Intelligent Transport Systems, 2016, 10(6): 379-388.
[39] BARUAH B, DHAL S. A security and privacy preserved intelligent vehicle navigation system[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(2): 944-959.
[40] DWORK C, LEI J. Differential privacy and robust statistics [C]// Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. ACM, 2009: 371-380.
[41] XU Q, ZHAO L, SU Z, et al. Secure federated learning in quantum autonomous vehicular networks[J]. IEEE Network, 2023, 37(6): 240-247.
[42] WANG Z, LI Y, LI D, et al. Enabling fairness-aware and privacy-preserving for quality evaluation in vehicular crowdsensing: a decentralized approach[J]. Security and Communication Networks, 2021, 2021.
[43] SALEEM M A, LI X, AYUB M F, et al. An Efficient and Physically Secure Privacy-Preserving Key-Agreement Protocol for Vehicular Ad-Hoc Network[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9940-9951.
[44] YING Z, CAO S, LIU X, et al. PrivacySignal: Privacy-Preserving Traffic Signal Control for Intelligent Transportation System[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 16290-16303.
[45] FANG K, WANG T, TONG L, et al. Non-intrusive security assessment methods for future autonomous transportation IoV [J]. IEEE Transactions on Automation Science and Engineering, 2023, 21(3): 2387-2399.

[46] QU Z, TANG Y, MUHAMMAD G, et al. Privacy protection in intelligent vehicle networking: A novel federated learning algorithm based on information fusion[J]. Information Fusion, 2023, 98: 101824.

[47] XU C, DING Y, CHEN C, et al. Personalized location privacy protection for location-based services in vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(1): 1163-1177.

[48] BI R, XIONG J, TIAN Y, et al. Edge-cooperative privacy-preserving object detection over random point cloud shares for connected autonomous vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(12): 24979-24990.

[49] ERLINGSSON Ú, FELDMAN V, MIRONOV I, et al. Amplification by Shuffling: From Local to Central Differential Privacy via Anonymity[J]. arXiv: 1811. 12469, 2018.

[50] LIN G, QIN S, KHATTAK Z H. FedAV: federated learning for cyberattack vulnerability and resilience of cooperative driving automation[J]. Communications in Transportation Research, 2025, 5: 100175.

[51] ZHANG C, ZHANG X M, SOTTIWAT E, et al. Generative gradient inversion via over-parameterized networks in federated learning[C]// Proceedings of the IEEE/CVF International Conference on Computer Vision. 2023: 5126-5135.

[52] LI Y, SHI J, MENG D, et al. FuzzyCom: privacy-aware trajectory data compression using fuzzy sets in edge vehicular networks [C]// 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, 2022: 613-619.

[53] CHEN T, TIAN X, LI Y, et al. FuzzyFollow: A Novel Privacy-Aware Intelligent Vehicle-Following Scheme for Safe Driving on Risky Roads Using Fuzzy Sets[C]// 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD). 2024: 2484-2490.

[54] LI Y, LIU F, ZHANG J, et al. Privacy-aware fuzzy skyline parking recommendation using edge traffic facilities[J]. IEEE Transactions on Vehicular Technology, 2021, 70(10): 9775-9786.

[55] CHEN T, JIANG Q, LI Y, et al. Privacy-aware edge intelligent parking recommendation using intuitionistic fuzzy sets[J]. IEEE Transactions on Industrial Informatics, 2025, 21(5): 3606-3615.

[56] LIU B, XIE S, WANG H, et al. VTDP: privately sanitizing fine-grained vehicle trajectory data with boosted utility[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2643-2657.

[57] CHEN X, ZHANG T, SHEN S, et al. An optimized differential privacy scheme with reinforcement learning in VANET[J]. Computers & Security, 2021, 110: 102446.

[58] CAI S, LYU X, LI X, et al. A trajectory released scheme for the internet of vehicles based on differential privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 16534-16547.

[59] WEI J, LIN Y, YAO X, et al. Differential privacy-based location protection in spatial crowdsourcing[J]. IEEE Transactions on Services Computing, 2022, 15(1): 45-58.

[60] LIU M, CHENG L, GU Y, et al. MPC-CSAS: multi-party computation for real-time privacy-preserving speed advisory systems [J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(6): 5887-5893.

[61] LIU D, YU G, DING Y, et al. Privacy preserving multi-party computation with secret sharing for trajectory prediction in VANETs[J]. IEEE Transactions on Vehicular Technology, 2024, 73(12): 18666-18677.

[62] PENG T, ZHONG W, WANG G, et al. Privacy-preserving truth discovery based on secure multi-party computation in vehicle-based mobile crowdsensing[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(7): 7767-7779.

[63] WANG H, FAN K, ZHANG K, et al. Encrypted data retrieval and sharing scheme in space-air-ground-integrated vehicular networks[J]. IEEE Internet of Things Journal, 2022, 9(8): 5957-5970.

[64] CHENG H, SHOJAFAR M, ALAZAB M, et al. PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(7): 9391-9403.

[65] JIANG W, GUO Z. An Anonymous Authentication Scheme for Internet of Vehicles Based on TRUG-PBFT Master-Slave Chains and Zero-Knowledge Proof [J]. IEEE Internet of Things Journal, 2024, 12(7): 7763-7777.

[66] GUO Y, WANG Z, CUI H, et al. Vehicloak: A Blockchain-Enabled Privacy-Preserving Payment Scheme for Location-Based Vehicular Services[J]. IEEE Transactions on Mobile Computing, 2023, 22(11): 6830-6842.

[67] BATOOL H, ANJUM A, KHAN A, et al. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy[J]. Information Sciences, 2024, 652: 119717.

[68] ZHAO L, WAN Q, ZOU Q, et al. Privacy-preserving collaborative deep learning with unreliable participants[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 1486-1500.

[69] LI J H, WU Q M. Research on Internet of Vehicles data cooperative learning and communication optimization based on tripartite federated learning [J]. Modern Electronics Technique, 2024, 47(15): 26-33.

[70] KONG Q, YIN F, LU R, et al. Privacy-preserving aggregation for federated learning-based navigation in vehicular fog[J]. IEEE Transactions on Industrial Informatics, 2021, 17(12): 8453-8463.

[71] LI B, JIANG Y, PEI Q, et al. FEEL: Federated end-to-end learning with non-IID data for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 16728-16740.

[72] LI Y, LI H, XU G, et al. Efficient privacy-preserving federated learning with unreliable users [J]. IEEE Internet of Things Journal, 2022, 9(13): 11590-11603.

[73] HUANG H, SUN C, LEI X, et al. Privacy-preserving travel time prediction for internet of vehicles: A crowdsensing and federated learning approach[C]// Neural Information Processing. Singapore: Springer, 2024: 55-66.

[74] ZHAO L, JIANG J, FENG B, et al. SEAR: secure and efficient aggregation for byzantine-robust federated learning[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3329-3342.

[75] XU Z, ZHANG R, LIANG W, et al. A privacy-preserving data aggregation protocol for internet of vehicles with federated learning[J]. IEEE Transactions on Intelligent Vehicles, 2025, 10(1): 217-227.

[76] ZHANG D, FAN L. Cerberus: Privacy-Preserving Computation in Edge Computing[C]// IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2020: 43-49.

[77] CHEN X, DING J, LU Z. A decentralized trust management system for intelligent transportation environments[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(1): 558-571.

[78] ZADEH L A. Fuzzy sets [J]. Information and Control, 1965, 8(3): 338-353.

[79] KAMRA N, ZHU H, TRIVEDI D K, et al. Multi-agent trajectory prediction with fuzzy query attention[C]// Advances in Neural Information Processing Systems. Curran Associates Inc., 2020: 22530-22541.

[80] ISMAEL S F, ALIAS A H, ZAIDAN A A, et al. Toward Sustainable Transportation: A Pavement Strategy Selection Based on the Extension of Dual-Hesitant Fuzzy Multicriteria Decision-Making Methods[J]. IEEE Transactions on Fuzzy Systems, 2023, 31(2): 380-393.

[81] MIAO T, SHEN J, LAI C F, et al. Fuzzy-based trustworthiness evaluation scheme for privilege management in vehicular ad hoc networks[J]. IEEE Transactions on Fuzzy Systems, 2021, 29(1): 137-147.

[82] LI Y, LIU W, ZHU Y, et al. Privacy-aware fuzzy range query processing over distributed edge devices[J]. IEEE Transactions on Fuzzy Systems, 2022, 30(5): 1421-1435.

[83] LIU L, LIAN M, LU C, et al. TCSA: a traffic congestion situation assessment scheme based on multi-index fuzzy comprehensive evaluation in 5G-IoV[J]. Electronics, 2022, 11(7): 1032.

[84] DIAKOULAKI D, MAVROTAS G, PAPAYANNAKIS L. Determining objective weights in multiple criteria problems: The critic method[J]. Computers & Operations Research, 1995, 22(7): 763-770.

[85] LI Y, YANG S, REN X, et al. Multi-Stage Asynchronous Federated Learning With Adaptive Differential Privacy[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2024, 46(2): 1243-1256.

[86] LI Y, TAO X, ZHANG X, et al. Break the Data Barriers While Keeping Privacy: A Graph Differential Privacy Method [J]. IEEE Internet of Things Journal, 2023, 10(5): 3840-3850.

[87] WANG X, KIM B G, AMOON M, et al. Federated learning with local differential privacy for autonomous electronic vehicles: enhancing security and performance[J]. IEEE Transactions on Consumer Electronics, 2025, 71(2): 6147-6157.

[88] AN D, YANG Q, LI D, et al. Where Am I Parking: Incentive Online Parking-Space Sharing Mechanism With Privacy Protection[J]. IEEE Transactions on Automation Science and Engineering, 2022, 19(1): 143-162.

[89] AN D, YANG Q, YU W, et al. LoPrO: Location Privacy-preserving Online auction scheme for electric vehicles joint bidding and charging[J]. Future Generation Computer Systems, 2020, 107: 394-407.

[90] ANDRES M E, BORDENABE N E, CHATZIKOKOLAKIS K, et al. Geo-indistinguishability: Differential privacy for location-based systems[C]// Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM, 2013: 901-914.

[91] HAN W L, SONG L S, RUAN W Q, et al. Secure Multi-Party Learning: From Secure Computing to Secure Learning[J]. Chinese Journal of Computers, 2023, 46(7).

[92] YANG H, VIJAYAKUMAR P, SHEN J, et al. A location-based privacy-preserving oblivious sharing scheme for indoor navigation[J]. Future Generation Computer Systems, 2022, 137: 42-52.

[93] BI R, XIONG J, TIAN Y, et al. Achieving lightweight and privacy-preserving object detection for connected autonomous vehicles[J]. IEEE Internet of Things Journal, 2023, 10(3): 2314-2329.

[94] MOHANTY T, SRIVASTAVA V, DEBNATH S K, et al. Quantum Secure Threshold Private Set Intersection Protocol for IoT-Enabled Privacy-Preserving Ride-Sharing Application[J]. IEEE Internet of Things Journal, 2024, 11(1): 1761-1772.

[95] SUTRADHAR K. A Quantum Cryptographic Protocol for Secure Vehicular Communication[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(5): 3513-3522.

[96] HAN X, TIAN D, ZHOU J, et al. Privacy-preserving proxy re-encryption with decentralized trust management for MEC-empowered VANETs[J]. IEEE Transactions on Intelligent Vehicles, 2023, 8(8): 4105-4119.

[97] LI L, LIU J, CHENG L, et al. CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(7): 2204-2220.

[98] LI T, XIE S, ZENG Z, et al. ATPS: An AI Based Trust-Aware and Privacy-Preserving System for Vehicle Managements in Sustainable VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(10): 19837-19851.

[99] JIANG S, LI J, SANG G, et al. Vehicular edge computing meets cache: An access control scheme with fair incentives for privacy-aware content delivery[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(8): 8404-8418.

[100] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data [J]. arXiv: 1602.05629, 2016.

[101] GU Y H, BAI Y B. Research Progress on Security and Privacy of Federated Learning Model[J]. Journal of Software, 2022, 34(6): 2833-2864.

[102] GEIPING J, BANUERMEISTER H, DROGE H, et al. Inverting gradients-how easy is it to break privacy in federated learning? [C]// Proceedings of the 34th International Conference on Neu-

ral Information Processing Systems. Red Hook，NY：Curran Associates Inc.，2020：16937-16947.

[103]JIANG S，LI J，SANG G，et al. Vehicular edge computing meets cache：An access control scheme with fair incentives for privacy-aware content delivery[J]. IEEE Transactions on Intelligent Transportation Systems，2024，25(8)：8404-8418.

[104]LI Y，TAO X，ZHANG X，et al. Privacy-preserved federated learning for autonomous driving[J]. IEEE Transactions on Intelligent Transportation Systems，2022，23(7)：8423-8434.

[105]ZHAO J，CHANG X，FENG Y，et al. Participant selection for federated learning with heterogeneous data in intelligent transport system[J]. IEEE Transactions on Intelligent Transportation Systems，2023，24(1)：1106-1115.

[106]WU W，HE L，LIN W，et al. SAFA：a semi-asynchronous protocol for fast federated learning with low overhead[J]. IEEE Transactions on Computers，2021，70(5)：655-668.

[107]WU Y H，BAI G W，SHEN H. Multi-Dimensional Resource Dynamic Allocation Algorithm Based on Federated Learning in Vehicular Networks[J]. Computer Science，2022，49(12)：59-65.

[108]MO Z J，GAO Z P，YANG Y，et al. An Efficient Distributed Model Sharing Strategy for Data Privacy Protection in Vehicular Networks[J]. Journal of China Institute of Communications，2022，43(4)：83-94.

[109]WANG L L，WU S L，YANG N，et al. Research on Double-Layer Asynchronous Federated Learning of Vehicle Network Based on Two-Factor Update[J]. Journal of Electronics and Informatics，2022，46(7)：1-8.

[110]JIANG X，BORCEA C. Complement sparsification：low-overhead model pruning for federated learning[C]// Proceedings of the AAAI Conference on Artificial Intelligence. 2023：8087-8095.

[111]SHANG E，LIU H，YANG Z，et al. FedBiKD：federated bidirectional knowledge distillation for distracted driving detection[J]. IEEE Internet of Things Journal，2023，10(13)：11643-11654.

[112]ZHAO C，GAO Z，WANG Q，et al. FedSup：a communication-efficient federated learning fatigue driving behaviors supervision approach[J]. Future Generation Computer Systems，2023，138：52-60.

[113]ZHANG J，ZHANG J，MA Z，et al. RUPT-FL：robust two-layered privacy-preserving federated learning framework with unlinkability for IoV[J]. IEEE Transactions on Vehicular Technology，2025(4)：74.

[114]YU D，ZHANG H，CHEN W，et al. Gradient perturbation is underrated for differentially private convex optimization[C]// Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence. 2021：3117-3123.

[115]CAO S X，CHEN C M，TANG P，et al. Differential Privacy Federated Learning Algorithm Based on Function Mechanism[J]. Chinese Journal of Computers，2023，46(10)：2178-2195.

[116]LI J，WEI K，MA C，et al. DP-GenFL：A local differentially private federated learning system through generative data [J]. Science China Information Sciences，2023，66(8)：189303：1-189303：2.

[117]ZHANG S，YUAN W，YIN H. Comprehensive privacy analysis on federated recommender system against attribute inference attacks[J]. IEEE Transactions on Knowledge and Data Engineering，2024，36(3)：13.

[118]LIU D，PEI X K，LAI J S，et al. Privacy Protection Scheme Combining Edge Intelligent Computing and Federated Learning[J]. Journal of the University of Electronic Science and Technology of China，2023，52(1)：95-101.

[119]HUI Y，HU J，CHENG N，et al. RCFL：Redundancy-Aware Collaborative Federated Learning in Vehicular Networks[J]. IEEE Transactions on Intelligent Transportation Systems，2024，25(6)：5539-5553.

[120]GUO H，HUANG W，LIU J，et al. Inter-Server Collaborative Federated Learning for Ultra-Dense Edge Computing[J]. IEEE Transactions on Wireless Communications，2022，21(7)：5191-5203.

[121]LI Z，WU H，LU Y. Coalition based utility and efficiency optimization for multi-task federated learning in internet of vehicles [J]. Future Generation Computer Systems，2023，140：196-208.

[122]JAI VINITA L，VETRISELVI V. Federated Learning-based Misbehaviour detection on an emergency message dissemination scenario for the 6G-enabled Internet of Vehicles[J]. Ad Hoc Networks，2023，144：103153.

[123]ZHANG X，CHANG Z，HU T，et al. Vehicle Selection and Resource Allocation for Federated Learning-Assisted Vehicular Network[J]. IEEE Transactions on Mobile Computing，2024，23(5)：3817-3829.

[124]TOLPEGIN V，TRUEX S，GURSOY M E，et al. Data poisoning attacks against federated learning systems[C]// Computer Security-ESORICS 2020. Cham：Springer，2020：480-501.

[125]KUMAR S P，GOPE P，PUTHAL D. Blockchain and federated learning-enabled distributed secure and privacy-preserving computing architecture for IoT network[C]// 2022 IEEE European Symposium on Security and Privacy Workshops(EuroS&PW). IEEE，2022.

[126]WANG Y，LI G L，LI K Y. A Review of Federal Learning Contribution Assessment[J]. Journal of Software，2023，34(3)：1168-1192.

[127]ZHAO Z，XIANG T，BI Y，et al. A Novel Multi-Criteria Contribution Evaluation Scheme for Federated Learning in Internet of Vehicles[C]// 2023 15th International Conference on Communication Software and Networks(ICCSN). IEEE，2023：319-325.

[128]LI C，SONG M，LUO Y. Federated learning based on stackelberg game in unmanned-aerial-vehicle-enabled mobile edge computing. [J]. Expert Systems With Applications，2024，235：121023.

[129]WU Q，ZHAO Y，FAN Q，et al. Mobility-aware cooperative caching in vehicular edge computing based on asynchronous federated and deep reinforcement learning[J]. IEEE Journal of Selec-ted Topics in Signal Processing，2023，17(1)：66-81.

[130]OUALIL S，OUCHEIKH R，EL KAMILI M，et al. A personalized learning scheme for internet of vehicles caching[C]// 2021 IEEE Global Communications Conference(GLOBECOM). 2021：1-6.

[131]LI Y，ZENG D，GU L，et al. PASTO：enabling secure and effi-

cient task offloading in TrustZone-enabled edge clouds[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 8234-8238.
[132]CHEN G, ZHANG Y. Securing TEEs with verifiable execution contracts[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(4): 3222-3237.
[133]MIAO X, CHANG R, ZHAO J, et al. CVTEE: A compatible verified TEE architecture with enhanced security. [J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(1): 377-391.
[134]ULLAH I, KHALIL I, BAI X, et al. An ensemble-based hybrid model for the detection of attacks in the internet of vehicular things[J]. IEEE Transactions on Intelligent Transportation Systems(Early Access), 2025: 1-14.
[135]CHEN X, SONG X, REN R, et al. Fine-grained privacy detection with graph-regularized hierarchical attentive representation learning[J]. ACM Transactions on Information Systems, 2020, 38(4): 1-26.
[136]AMARAL O, ABUALHAIJA S, TORRE D, et al. AI-enabled automation for completeness checking of privacy policies[J]. IEEE Transactions on Software Engineering, 2022, 48(11): 4647-4674.
[137]CHEN C, ZHOU D, YE Y, et al. CLEAR: towards contextual LLM-empowered privacy policy analysis and risk generation for large language model applications[C]// Proceedings of the 30th International Conference on Intelligent User Interfaces. New York: ACM, 2025: 277-297.
[138]CAO X, YU J, HAN J, et al. A transformer decoder-based generative adversarial model with TrajLoss function for privacy-preserving trajectory publishing[C]// Proceedings of the 5th International Conference on Machine Learning and Natural Language Processing(MLNLP 2022). 2022: 271-278.
[139]HU Y, WU F, LI Q, et al. SoK: Privacy-Preserving Data Synthesis[C]// 2024 IEEE Symposium on Security and Privacy(SP). 2024: 4696-4713.
[140]SHANG F J, DENG X X. Blockchain-based privacy-preserving internet of vehicles data sharing scheme [J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2025, 37(2): 155-164.
[141]ZHOU J, CHEN S, CHOO K K R, et al. EPNS: Efficient Privacy-Preserving Intelligent Traffic Navigation From Multiparty Delegated Computation in Cloud-Assisted VANETs[J]. IEEE Transactions on Mobile Computing, 2023, 22(3): 1491-1506.
[142]CAI Z, XIONG A. Understand users' privacy perception and decision of V2X communication in connected autonomous vehicles [C]// 32nd USENIX Security Symposium, USENIX Security 2023. 2023: 2975-2992.

LI Jiahui, born in 2000, postgraduate, is a member of CCF(No. Y8989G). Her main research interests include privacy-preserving computation and IoV.

LI Yinglong, born in 1981, Ph.D, master's supervisor, is a member of CCF (No. 31138M). His main research interests include privacy-preserving computation in edge mobile networks and artificial intelligence.

(责任编辑:柯颖)