# 隐私计算在车路协同场景应用的探索与实践

**李明，吕阿斌**
中兴飞流信息科技有限公司，江苏 南京 210012

**摘要**
基于车路协同的发展现状，总结车路协同场景中隐私计算、人工智能等技术的研究进展。设计并实现YITA-TFL平台，为数据管理、模型训练、模型管理及协同推理提供完备的隐私保护方案，为人工智能结合隐私计算在交通行业的应用提供参考。

**关键词**
车路协同；边缘计算；隐私计算；差分隐私

中图分类号：U49 文献标志码：A doi: 10.11959/j.issn.2096-0271.2022069

# *Exploration and practice of privacy preserving computing for vehicle-road collaboration system*

**LI Ming, LYU Abin**
JETFLOW Co., Ltd., Nanjing 210012, China

***Abstract***
Based on the development of vehicle-road collaboration, the research progress of privacy computing, artificial intelligence, and other technologies for the vehicle-road collaboration scene was summarized. YITA-TFL platform was designed and implemented. A complete privacy protection scheme was provided for data management, model training, model management, and collaborative reasoning. And a model was established for the application of artificial intelligence combined with privacy computing in the transportation industry.

***Key words***
vehicle-road collaboration, edge computing, privacy computing, differential privacy

## 0 引言

车路协同概念最早由欧盟委员会第六科技框架计划提出，旨在通过人、车、路、云的信息交互和共享，充分实现多方有效协同决策，提高出行效率及确保人车安全。车路协同是辅助智能网联或自动驾驶车辆安全运行的有效载体，是道路交通运输领域的科技战略制高点[1-2]。车路协同相关技术组成复杂，涵盖汽车、集成电路、无线通信、边缘计算、人工智能、大数据、云计算等多个高新技术。目前，一些国家高度重视车路协同的发展，2021年国务院和交通运输部分别印发《“十四五”现代综合交通运输体系发展规划》《数字交通“十四五”发展规划》，鼓励车路协同及自动驾驶相关产业的健康发展[3-4]。同时，无线通信技术、人工智能等技术的迅速发展进一步推动车路协同系统的迭代升级与成熟。赛迪网预测车路协同产业在2022年进入爆发期，预计2025年产业规模将超万亿元[5]。但随着车路协同产业规模的快速发展以及相关应用的深入，车路协同系统的组成节点通常运行在不可信环境中，一些与安全相关的问题逐渐暴露出来，比如数据采集阶段的数据泄露、模型训练阶段及推理阶段通过获取中间数据复原原始数据造成的隐私泄露、毒化数据影响模型训练等[6-7]。上述安全问题是车路协同系统面临的较大挑战。

如何打造安全的车路协同系统成为行业当前关注的重点问题，本文分析车路协同场景中遇到的安全问题与挑战，结合隐私计算、人工智能技术在车路协同场景的实践经验，设计并实现了YITA-TFL（YITA-trusted federated learning）平台，涵盖数据安全、训练安全以及推理安全等问题的解决方法，为车路协同场景下隐私计算和人工智能技术兼顾发展和安全、平衡效率和风险提供一种可行的系统性解决方案。

## 1 国内外研究进展

车路协同场景的数据安全、模型安全、推理安全等问题不仅涉及技术领域，还涉及管理领域。

- 技术领域。近两年陆续有学者基于隐私计算技术对上述问题展开研究。例如，将差分隐私（differential privacy，DP）、隐私决策树、贝叶斯网络等方法应用于数据发布，实现兼顾数据隐私保护和数据分析的目的[8-9]，基于同态加密（homomorphic encryption，HE）和区块链技术的车联网隐私保护方案支持将隐私数据进行同态加密处理后再写入区块，实现隐私数据以密文状态分发、共享和计算[10]，但是这类方法针对结构化数据比较有效，针对视频、图像、语音等非结构化数据时则受限。基于差分隐私、随机梯度下降等技术实现了模型训练过程中的安全保护[11-12]；采用分割模型的方式提高了训练过程的安全保护程度，分割模型在客户端和服务端分段训练，简单计算部分留存在客户端本地，复杂计算部分留存在服务端，同时在模型执行过程中应用差分隐私算法对分割模型间传输的数据进行隐私保护，确保参与训练的各方无法获取完整的模型，进而提高本地模型的安全性[13-14]。针对车路协同推理阶段，将深度学习网络模型切分为两部分，分别在车载终端和路侧边缘服务器执行场景下，设计出基于差分隐私的防御算法，防止攻击者基于推理阶段的中间数据还原图像，保护用户隐私[15]。

● 管理领域。许多国家和组织出台了相关法律、法规及标准。2021年3月9日，欧洲数据保护委员会（European Data Protection Board，EDPB）通过了《车联网个人数据保护指南》，结合《通用数据保护条例》对车路系统场景处理个人数据进行指导和规范，阐释了该场景下的隐私和数据风险及应对措施，为行业参与者有效地保护数据安全提供指导。国际标准化组织道路车辆技术委员会（ISOTC22）信息安全工作组组织制定了《道路车辆-网络安全工程》（ISO/SAE 21434）等国际标准。我国相关法律，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相继出台，为车路协同相关主体的安全工作提供根本遵循[16]。

综上，面向车路协同场景的隐私计算、人工智能的应用，各方均进行了探索并取得了一定的成果，但是目前尚缺少真正落地的、系统性的解决方案。

## 2 车路协同可信AI平台的设计与实现

对于车路协同场景的数据安全、模型安全、推理安全等问题，需要构建安全可信的AI平台来解决。同时，由于车路协同的应用特性，车载子系统和路侧子系统分布式协同，且均需实时获取感知信息及计算结果，对分布式和实时性要求较高，本文将中兴飞流信息科技有限公司（以下简称中兴飞流）基于数据流理论自主研发的实时计算中间件YITA作为分布式计算引擎，结合隐私计算、人工智能、区块链等技术，设计并实现了面向车路协同场景的可信AI平台——YITA-TFL平台。

### 2.1 相关知识

#### 2.1.1 车路协同

车路协同系统是指一种通过人、车、路、云信息交互，实现车辆与基础设施之间、车辆与车辆之间、车辆与人之间智能协同与配合的智能运输系统体系。车路协同系统由4个主要部分构成[17]：出行者子系统、车载子系统、路侧子系统及云控中心子系统，其系统构成如**图1**所示。

车路协同系统也被称为合作式智能运输系统，各组成部分简要介绍如下。

● 出行者子系统：由出行者携带的各类信息终端或其他信息处理设备构成。

● 车载子系统：一般包括OBU（on board unit）设备，也可以包括车载的其他计算控制模块、车载网关、路由器等。车载子系统可以参与YITA-TFL平台的计算。

● 路侧子系统：包括路侧直连通信设施（如路侧单元（road side unit，RSU））、路侧感知设施、路侧计算设施（如多接入边缘计算（multi-access edge computing，MEC）等），也包括用于通信与定位、交通安全与管理的各类设备设施。路侧计算设施可以参与YITA-TFL平台的计算。

● 云控中心子系统：包括云控平台、中心交换、服务组件节点、服务路由器和中心接入节点等，具备网络管理、业务支撑和服务等能力。云控平台对路侧子系统进行管理，包括协同训练、协同推理、模型发布等。

各模块之间均定义了通信协议，例如C-V2X（cellular-vehicle to everything）是基于3GPP全球统一标准的通信技术，包括车辆与车辆之间、车辆与人之间、车辆与路侧设施之间、车辆与网络之间的通信；专用短程通信（dedicated short range

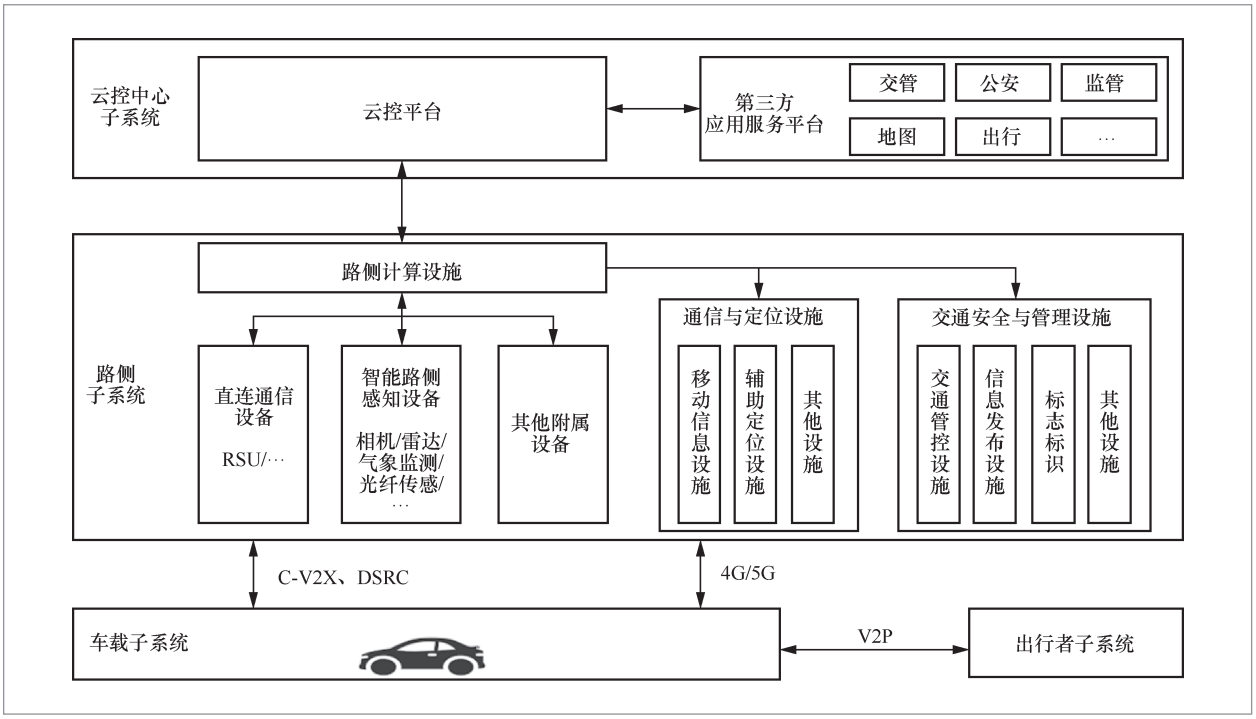


图1 车路协同系统构成示意图

communications，DSRC）协议用于收费设施与车辆之间的通信；V2P（vehicle to person）协议用于车载单元与行人之间的通信。

除云控中心子系统的服务器设备外，车路协同系统的其他子系统由算力较低的终端设备和边缘设备构成，无法承担复杂计算，这些子系统对YITA-TFL平台有特定的要求。

### 2.1.2 联邦学习

隐私计算主要是指以可信执行环境、多方安全计算（secure multi-party computation，MPC）和联邦学习为代表的可以保护数据不外泄的一类数据分析计算技术[18]。本文设计的YITA-TFL平台基于联邦学习技术实现分布式学习功能。联邦学习是由谷歌在2016年提出的分布式机器学习框架[19]，其核心思想是“数据不动模型动，数据可用不可见”，根据参与方数据集的特征空间和样本空间的分布，联邦学习可被分为横向联邦学习、纵向联邦学习，以及联邦迁移学习[20]。

### 2.1.3 差分隐私

差分隐私是一种被广泛认可的隐私保护技术，最早由微软提出[21]。($\varepsilon$,$\delta$)差分隐私定义如下[22]。

一个随机算法$M$：$D\rightarrow R$满足($\varepsilon$,$\delta$)-差分隐私，对于任意仅相差一条数据的相邻数据集$d$、$d'\in D$和任意输出$S\subseteq R$，满足如下条件：

$$P\left[M(d)\in S\right]\leqslant e^{\varepsilon}P\left[M(d')\in S\right]+\delta \quad (1)$$

其中，$M(d)$和$M(d')$分别表示算法$M$在数据集$d$、$d'$上的输出；$P$表示算法的输出概率；$\varepsilon$为隐私预算，用于控制隐私保护级别，$\varepsilon$越小，提供的隐私保护能力越强；$\delta$为另一个隐私预算，表示可容忍的隐私

预算超出$\varepsilon$的概率。如果$\delta=0$，就称$M$满足$\varepsilon$-差分隐私。

差分隐私可以基于输入扰动、中间参数扰动、目标扰动及输出扰动等方式用于模型训练和模型推理等阶段的隐私保护，例如，模型训练过程中可以应用差分隐私技术给梯度参数、权重参数、目标函数添加噪声扰动，从而实现对模型或训练数据的隐私保护。

分析差分隐私的原理发现，其算法相对简单，系统开销较小，适用于低算力设备参与者较多的车路协同场景。

## 2.2 YITA-TFL平台架构设计

本节简要介绍YITA-TFL平台架构及各模块实现的核心功能，其系统架构如**图2**所示。

YITA-TFL平台各模块介绍如下。

- 分布式引擎YITA：YITA是流批一体的分布式计算引擎，为YITA-TFL平台提供统一的分布式计算环境以及资源管理功能。
- 隐私计算工具：为YITA-TFL平台提供各种加密隐私保护机制，包括各类加密算法以及区块链组件，为平台实现数据管理安全、模型训练安全、模型发布安全以及模型推理安全提供保护技术。
- 联邦学习：为YITA-TFL平台提供安全的分布式训练支撑，在移动端、边缘云以及中心云间建立共享模型，实现训练、推理过程中数据的“可用不可见”。
- 可信数据管理：为YITA-TFL平台模型训练与推理提供安全的数据基础，提供数据集管理、隐私保护策略（如数据加密、防篡改等）、数据质量管理（如异常数据检测、偏见消除等）、数据标注等功能。
- 可信开发环境：包括可信模型训练

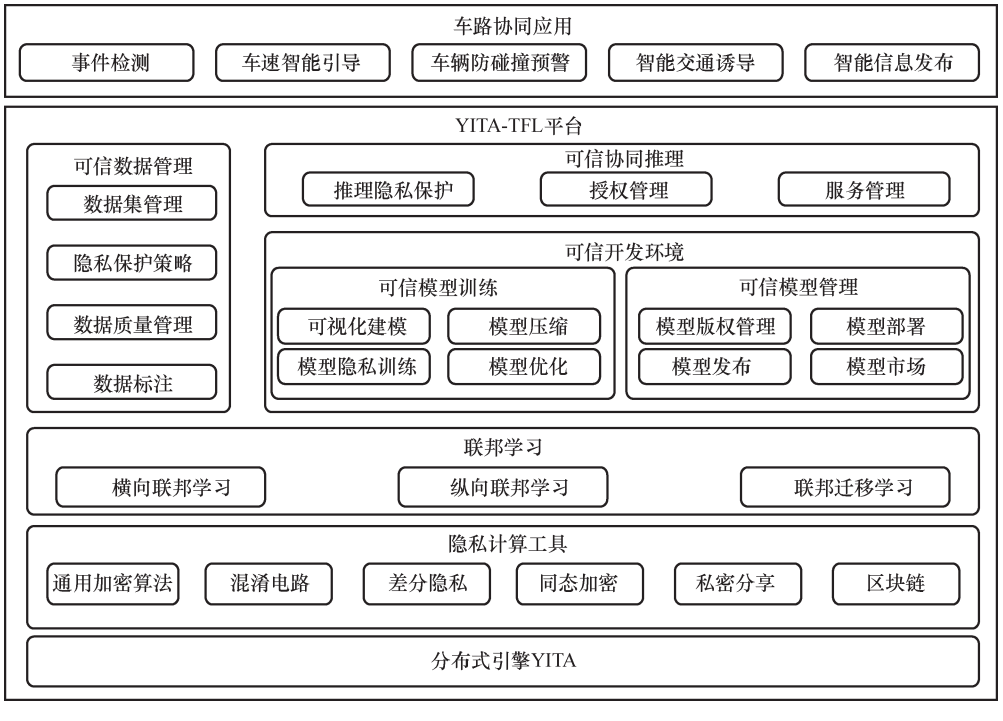


图 2 YITA-TFL 平台的系统架构

与可信模型管理两部分。可信模型训练提供可视化建模、模型隐私训练（如基于差分隐私的训练、模型分割发布等）、模型压缩、模型优化，支持对模型的自动化减枝、编译优化等功能，从而提升模型推理阶段的性能，或者为边缘端提供轻量化模型等；可信模型管理提供模型版权管理（如在模型中增加水印）、模型发布、模型部署以及模型市场等功能。

- 可信协同推理：为YITA-TFL平台提供安全的模型执行机制。推理隐私保护采用分割推理、差分隐私等技术保障模型在推理阶段的安全运行；授权管理配合版权管理实现对模型的知识产权保护；服务管理提供模型运行状态跟踪与检测等功能。

YITA-TFL平台综合应用隐私计算技术、区块链技术和人工智能技术，涵盖数据管理、模型训练、模型管理以及模型推理的全流程，为车路协同领域构建安全的人工智能应用提供了安全的开发环境和执行环境。同时，YITA-TFL平台可被应用到其他重视数据及模型安全的领域。

## 2.3 YITA-TFL平台实现

本节重点介绍联邦学习、可信数据管理、可信模型训练、可信模型管理以及可信协同推理5个子模块关键功能的实现方法和技术。

### 2.3.1 联邦学习

联邦学习是YITA-TFL平台可信模型训练的支撑模块，包括服务端和客户端两部分。其架构如**图3**所示。

联邦学习子平台相关模块介绍如下。

（1）联邦学习子平台服务端

服务端包括支撑与管理模块、联邦聚合模块、安全能力模块、传输交换模块及作业实例模块。各模块功能介绍如下。

- 支撑与管理模块提供集群管理、资源配置等应用程序接口（application programming interface，API），作业计划，客户端管理与选择，以及路由转发服务等功能。
- 联邦聚合模块提供FedProx、FedAvg、SCAFFOLD等聚合算法，保证不同场景下的收敛速率和收敛性。同时，支持用户扩展自定义的聚合优化算法。
- 安全能力模块提供多种隐私算法，包括差分隐私、密钥共享等。
- 传输交换模块支持多种数据传输和调用模式，如超文本传送协议（hypertext transfer protocol，HTTP）、

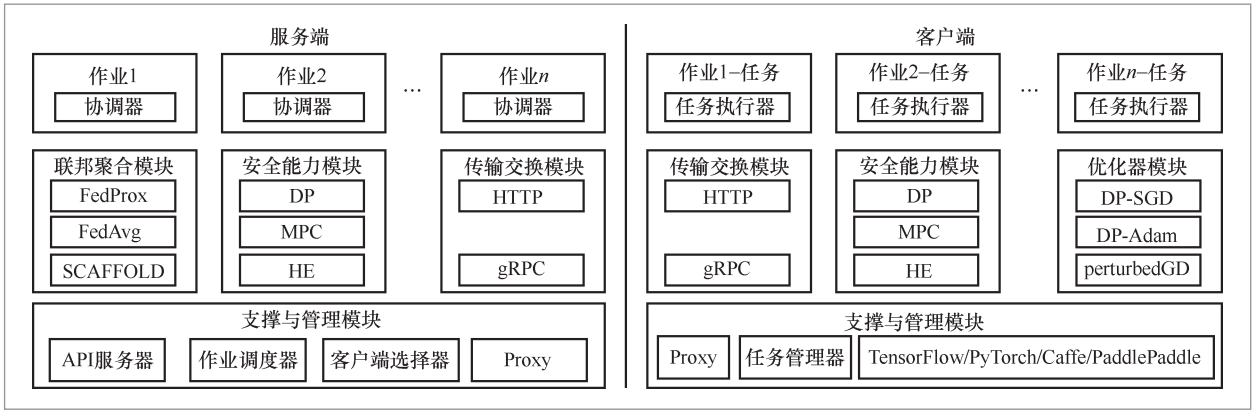


图 3 联邦学习模块架构

谷歌远程过程调用(Google remote procedure call, gRPC)等。

- 作业实例模块根据客户端提交的训练作业动态创建实例，协同客户端和服务端完成联邦学习，包括作业启动、创建训练任务、联邦聚合等。

(2)联邦学习子平台客户端

客户端各模块同服务端的模块基本一一对应，客户端和服务端协作完成联邦学习过程。客户端支持的深度学习框架包括TensorFlow、PyTorch、Caffe以及PaddlePaddle等。

在联邦学习过程中，客户端负责每轮训练任务的创建及本地训练执行、每轮训练参数的上报以及聚合后数据的获取等。

在隐私安全的前提下，客户端与服务端协同实现高效、安全、易用的联邦学习过程。

### 2.3.2 可信数据管理

数据是AI的基础，为AI提供训练资源，推动AI的快速发展。数据是核心资产，在AI领域的竞争中举足轻重。车路协同系统运行过程中产生大量的隐私数据，如身份信息、位置信息、轨迹信息等，数据安全尤其重要。

数据隐私保护是应用AI技术首先需要考虑的问题，可信数据管理在数据收集阶段就实现了数据隐私保护，其功能架构如**图4**所示。

(1)数据集管理

平台支持各类数据采集，包括实时消息、日志、文件、时序数据、数据库以及视频和图片等，并支持数据本地存储或分布式存储。

(2)数据标注

平台支持对数据的半自动化标注，支持文本、语音、视频、结构化数据等多种类型的数据。

(3)数据质量管理

平台提供完备的数据质量管理，包括数据标准、规则管理、依据数据标准对数据进行质量检查并形成数据质量报告。同时，还提供异常数据检查，包括分布检测、偏见检测、活体检测等。毒化数据危害较大，平台提供如下方法消除毒化数据。

- 数据清洗处理：通过异常样本检测、合理数据采样等数据预处理技术消除恶意样本，提升数据分布合理性；采用平滑去噪等数据预处理技术降低异常样本的影响。

- 鲁棒性算法：通过鲁棒性的聚合算法，如修整均值(trimmed mean, TRIM)、中值聚合、拒绝负面影响(reject

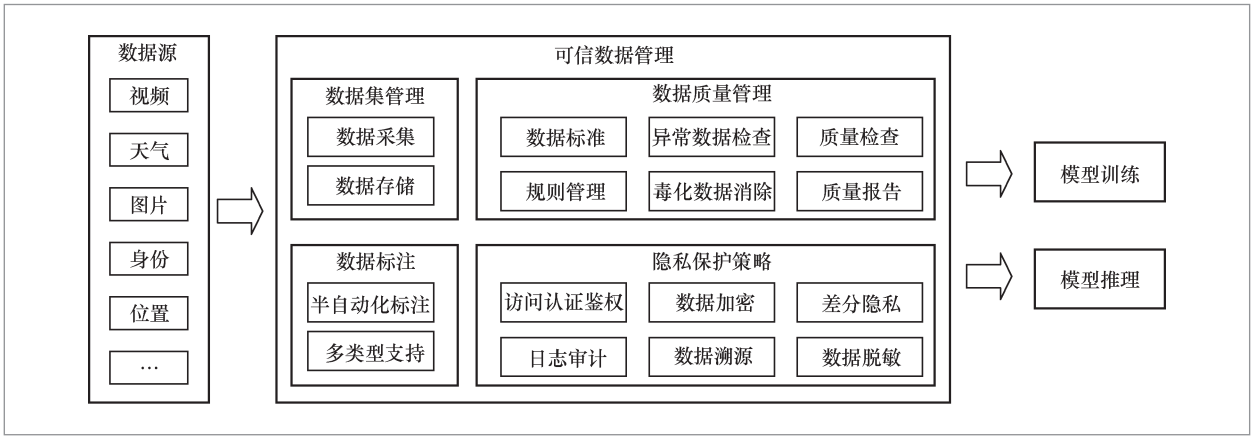


图 4 可信数据管理功能架构

on negative impact，RONI）等，降低恶意梯度数据的影响，提高算法鲁棒性。

- 数据净化法：借鉴参考文献[23–24]等提出的方法，净化因攻击而中毒的数据，从而达到移除中毒数据或其他异常数据的目的。

（4）隐私保护策略

平台提供丰富的隐私保护策略，其实现介绍如下。

- 访问认证鉴权模块实现用户管理、安全认证和服务授权。对用户的登录信息进行合法性鉴定，避免出现非法用户登录系统的情况，同时根据用户角色限定用户功能权限，控制访问数据和参与联邦计算的范围，防御恶意攻击者。
- 日志审计与数据溯源模块监控所有与数据相关的事务，包括会话、用户信息以及数据的增、删、改、查、用等行为，提供完备的访问审计溯源功能。
- 平台支持动态脱敏，对关键隐私信息自动脱敏。平台还支持多种加密算法，如DES加密、同态加密等。对于统计信息等数据，系统提供差分隐私保护，支持噪声扰动、随机响应等机制。

基于上述数据管理与隐私技术的应用，在较少增加计算和通信负担的情况下，实现对数据的持续保护，夯实车路协同场景下安全应用人工智能技术的基础。

### 2.3.3 可信模型训练

本节主要介绍在模型训练阶段，可信模型训练模块如何实现对数据和模型的隐私保护。

一般来说，在车路协同场景下，处于模型训练阶段的系统面临以下威胁。

威胁1：潜在模型异常。攻击方通过数据中毒攻击并破坏训练数据集合的完整性，或者通过模型中毒攻击破坏学习过程的完整性，从而导致模型异常[25]。

威胁2：潜在隐私泄露。云、边、端在训练阶段协同时，虽然不传输原始数据，但涉及参数的上传和下发，通过模型逆向攻击或模型提取攻击，利用模型参数依然可以推测出本地设备数据的部分隐私信息。

针对威胁1，第2.3.2节给出了部分防御方法。除此之外，在训练阶段，针对数据投毒，系统还提供优化客户端选择的方法进行对抗，例如针对每一轮训练，系统按规则重新选择参与训练的客户端，降低恶意攻击的影响；优化联邦激励机制，提升可信客户端的选择权重等。

防御威胁2的核心思想是利用隐私安全算法，将传输的中间数据加密为密文数据，避免获取参与方的原始数据。系统目前支持两种隐私安全算法：基于差分隐私的中间参数扰动隐私保护算法和基于密钥共享的安全聚合算法。下面介绍其具体实现。

（1）基于差分隐私的中间参数扰动隐私保护算法实现

采用差分隐私算法在中间数据中加入特定分布的噪声（如高斯噪声、拉普拉斯噪声），避免通过数据差异分析等方式恢复原始数据，从而达到保护隐私安全的目的。参与方客户端利用本地数据进行训练，在梯度（对应图5（a））或$\Delta w$（对应图5（b））中加入噪声，客户端上报携带噪声的中间数据，并直接在中间数据上聚合得到新模型[26]。DP-Gradient算法在梯度中添加噪声，客户端本地训练的每次梯度更新都需要添加噪声；DP-Weight算法在$\Delta w$中加噪声，客户端在每轮联邦训练中只需要针对$\Delta w$添加一次噪声即可。两种算法的收敛效率和性能基本一样，但DP-Weight算法的客户端计算开销相对较小。

（2）基于密钥共享的安全聚合算法实现

通过密钥共享将本地密钥分片发送给各参与方，在服务端联邦聚合过程中，每个客户端上报的参数采用本地掩码分片加

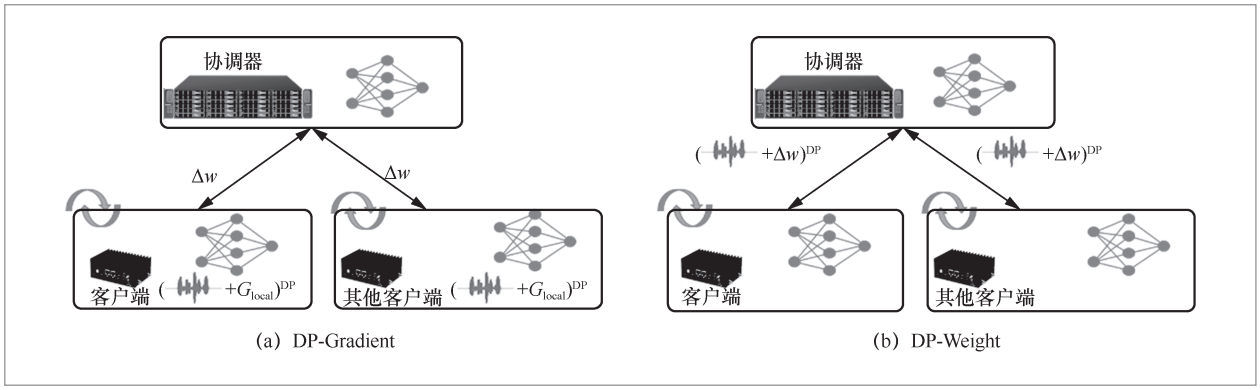


图 5 差分隐私算法实现框架

密，聚合过程中掩码被抵消，从而得到聚合结果。训练过程中参与方无法知晓任意一个客户端的原始数据，从而达到保护隐私的目的。算法特征总结如下：

- 模型在密文状态下聚合，具有密码级的安全保证，与差分隐私相比，具有更高的安全性；
- 采用掩码加密，训练过程中服务端通过密钥共享将掩码分片广播到各参与方，传输数据量只与参与方客户端的数量相关，与模型大小无关；
- 模型权重等原始数据不需要在参与方之间传递，遵从联邦协议；
- 双重掩码机制允许客户端在训练过程中掉线，适用于客户端稳定性差的联邦训练场景；
- 通过分层聚合解决了安全聚合随参与方数量增加，计算和传输开销快速上升的问题，方案具备较好的弹性。

除模型隐私训练功能外，可信模型训练模块还提供可视化建模、模型压缩和模型优化等功能，共同实现安全地构建模型、训练模型和编译模型的目的。

### 2.3.4 可信模型管理

模型管理是模型使用过程中非常重要的环节，但是当前对这一部分的研究相对较少。本文设计的可信模型管理包括模型版权管理、模型发布、模型部署以及模型市场等功能。

(1) 模型版权管理

算法模型是研究人员通过数月努力设计训练出来的，是一种非常有价值的知识产权资产，需要做好算法模型的知识产权管理工作。模型版权管理主要包括两部分功能：模型加密和模型水印。

①模型加密

为了防止模型被他人挪用、恶意复制，在模型部署前需要对模型进行加密，模型部署后，在推理阶段的运行时模块加载模型时，根据加密机制进行反向解密即可。YITA-TFL平台采用OpenSSL中的高级加密标准(advanced encryption standard，AES)实现模型加密，AES是美国联邦政府采用的一种区块加密标准，是目前对称密钥加密中非常流行的算法之一。

②模型水印

模型水印的思想来自于数字水印技术，人工智能模型水印最早由Uchida Y等人[27]提出。目前主要的人工智能模型水印算法包括后门植入水印、利用对抗样本构建水印、利用投影矩阵构建水印、利用聚类将图片按输出激活分类编码、利用对抗

网络训练等[28]。综合分析各类算法的优缺点，YITA-TFL平台采用后门植入水印为平台算法提供版权保护。其算法框架如图6所示[29]。

- 水印植入：模型持有者提取一部分数据作为触发集，可以在图片上加上特定的噪声或者标志，使得触发集数据中带有版权信息，然后输入目标模型进行训练，特别的是，将触发集图片对应的输出标记为特定输出，比如在车路协同场景中，将触发集中的轿车标记为自行车，对目标模型进行有监督的训练，使模型学习到这种特定的噪声或标志的特征，则水印植入成功。
- 水印验证：向模型输入触发集的图片以及原图片，当模型的输出为指定的特殊标签以及原本的标签时，水印验证成功，否则失败。

（2）模型发布

平台支持两种模型发布：模型完整发布和模型分割发布。因为车载终端计算资源有限，难以执行完整模型，所以对模型进行分割，比如把特征提取等算力需求较小的网络放在车载终端上执行，把算力需求较大的部分算法放在边缘服务器上执行，提升车路协同场景的整体模型推理效率。模型分割发布时，需要采用差分隐私对两方推理过程中传递的中间结果进行加密，确保数据隐私安全。

（3）模型部署

平台支持将模型远程部署到边缘设备和终端设备，支持实时监测模型下发及部署的进度，支持模型文件下发断点续传。

（4）模型市场

平台提供模型的交易服务，详细功能描述如下。

- 模板集市：用于用户间的模型交换。用户可以将自己训练好的模型发布到模板集市中，也可以从模板集市中下载模型，用于训练和推理。
- 数据集市：用户可以下载数据集市中的数据。
- 能力集市：展示用户发布成功的模型能力，并提供下载。

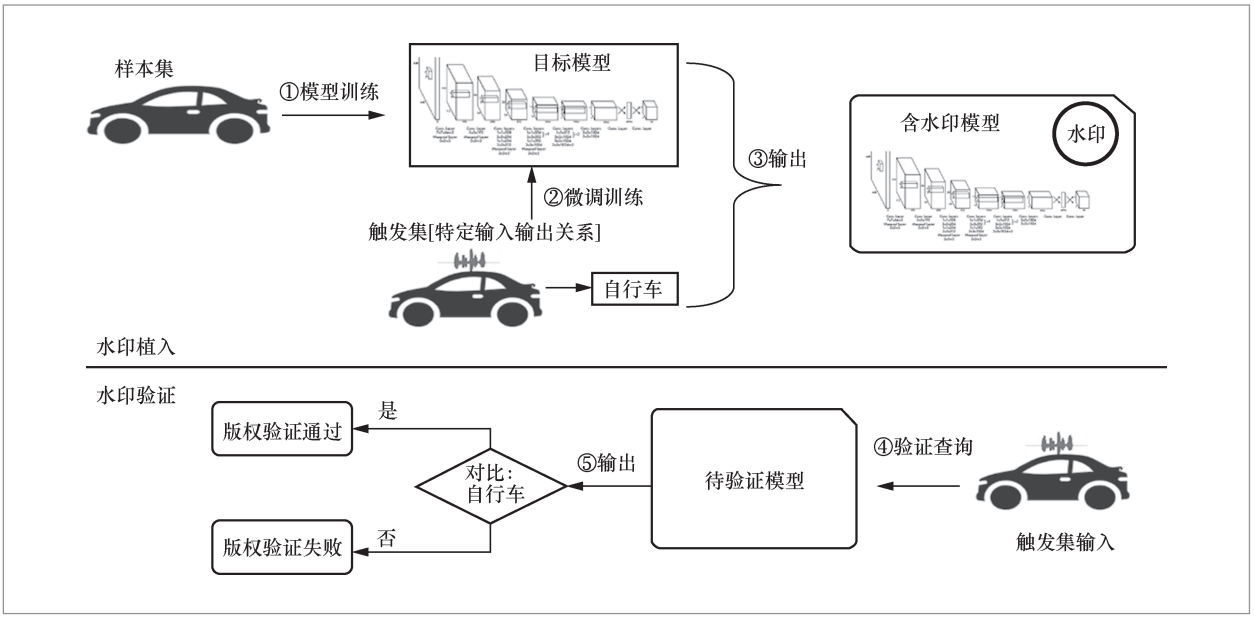


图 6 后门植入水印算法框架

#### 2.3.5 可信协同推理

推理阶段是应用模型解决实际问题的阶段，是最重要的执行阶段，包括授权管理、服务管理及推理隐私保护等功能。

（1）授权管理

结合模型加密和模型水印等功能，保证模型的知识产权。

（2）服务管理

主要实现模型的资源监控、弹性扩容、流量控制、灰度升级等功能。

（3）推理隐私保护

推理阶段对模型的攻击通常被称为推理攻击，一般不会破坏目标模型，主要是影响模型的输出结果或者通过反卷积网络等技术获取原始数据，从而引起数据泄露。后一种情况对分割发布的模型风险较大。本节简要介绍YITA-TFL平台对后一种情况的防御方式。

分割发布的模型一般由终端设备和边缘服务器协同推理，终端侧执行完整模型中算力消耗较小的部分，如特征提取等；服务侧执行完整模型中算力需求较大的部分。其算法过程如图7所示。

算法核心是对终端设备的输入数据增加输入扰动，对其输出的中间结果增加输出扰动。输入扰动和输出扰动均采用差分隐私算法生成。

在推理过程增加扰动在一定程度上会影响模型推理结果的准确率，如果扰动参数值等设置不合理，甚至会影响模型的可用性。不过，不同模型的合理扰动参数值不同，需要通过实验确定扰动参数的合理取值范围，保证模型准确率和隐私保护之间的平衡。

## 3 应用案例

YITA-TFL平台已成功应用于多个车路协同及高速公路视频分析项目，某省高速公路的车路协同系统架构如图8所示。YITA-TFL平台和YITA大数据平台协同，在项目中发挥核心作用，YITA-TFL平台支撑团队快速构建面向智能终端、路侧设备和云控平台等多方参与的安全人工智能应用体系，从数据采集、数据发布、模型在线训练、模型管理、模型发布到在线推理，保证数据和模型的全流程隐私和安全。该项目已接入超过500台智能终端和路侧设备，运行数十个深度学习模型和机器学习模型，为高速公路安全生产带来显著效益。

## 4 结束语

近年来，以大数据、人工智能以及5G为代表的信息技术推动车路协同的快速发

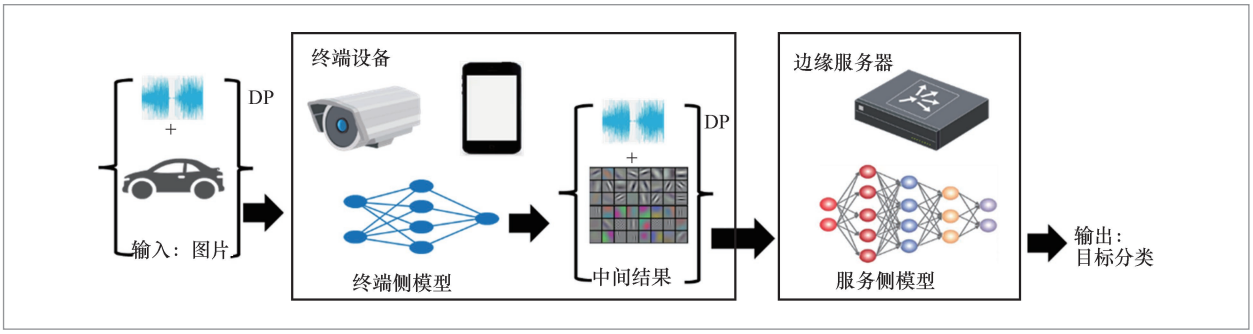


图 7 协同推断场景下基于差分隐私的中间结果隐私保护算法框架

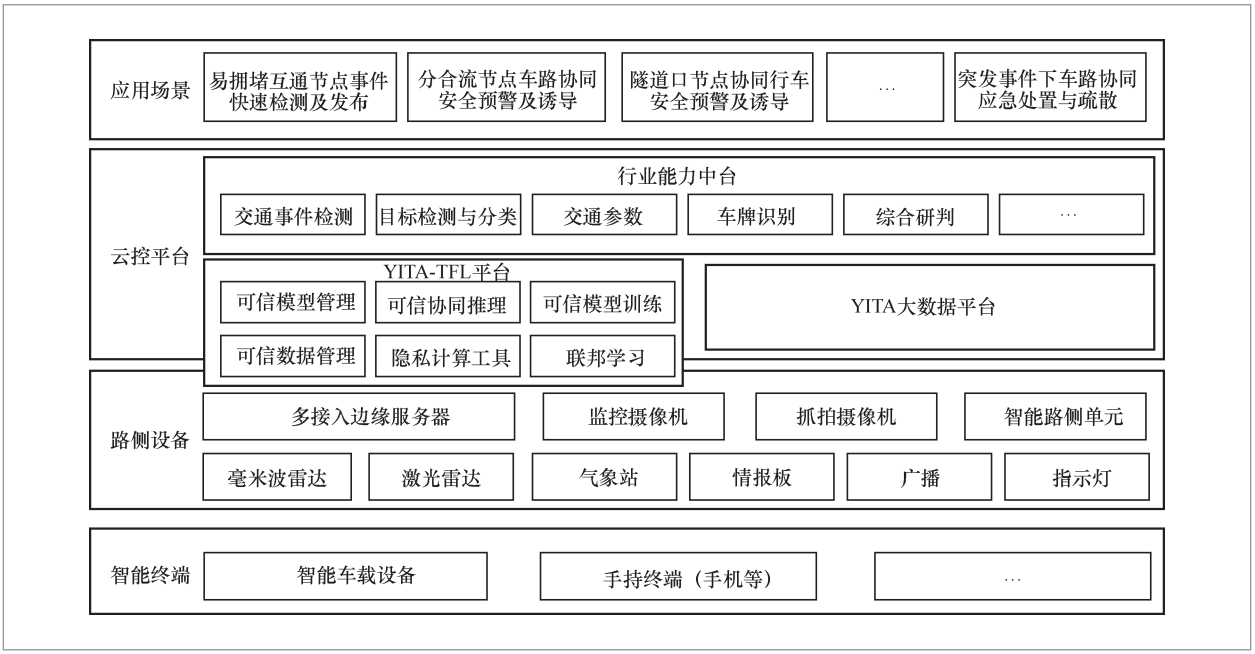


图 8 某省高速公路的车路协同系统架构

展，人们在不知不觉中已经成为车路协同系统中的一员。上述技术为人们的生活带来极大的便利，然而车路协同场景中的隐私泄露风险也给人们带来巨大的威胁。

本文介绍了车路协同场景的特点，分析了该场景下隐私计算、人工智能等技术的研究进展并进行总结，设计并实现了YITA-TFL平台，并在交通行业的车路协同及视频分析场景中落地应用。该平台不仅适用于车路协同场景，同样适用于其他重视数据和模型隐私的场景。未来的工作中，笔者团队将不断融合新技术，持续迭代优化，进一步提升平台的性能和普适性。

## 参考文献:

[1] 陈超，吕植勇，付姗姗，等. 国内外车路协同系统发展现状综述[J]. 交通信息与安全，2011, 29(1): 102–105, 109.
CHEN C, LYU Z Y, FU S S, et al. Overview of the development in cooperative vehicle–infrastructure system home and abroad[J]. Journal of Transport Information and Safety, 2011, 29(1): 102–105, 109.

[2] 李克强，戴一凡，李升波，等. 智能网联汽车(ICV)技术的发展现状及趋势[J]. 汽车安全与节能学报，2017, 8(1): 1–14.
LI K Q, DAI Y F, LI S B, et al. State–of–the–art and technical trends of intelligent and connected vehicles[J]. Journal of Automotive Safety and Energy, 2017, 8(1): 1–14.

[3] 国务院. “十四五”现代综合交通运输体系发展规划[Z]. 2021.
The State Council. Development plan of modern comprehensive transportation system during the “14th Five–Year Plan”[Z]. 2021.

[4] 交通运输部. 数字交通“十四五”发展规划[Z]. 2021.
Ministry of Transport of the People’s Republic of China. Development plan of digital transportation during the “14th Five–Year Plan”[Z]. 2021.

[5] 马承恩. 车路协同相关产业发展趋势[J]. 电子产品世界, 2021, 28(9): 4-6, 106.
MA C E. The development trend of vehicle-infrastructure cooperation industry[J]. Electronic Engineering & Product World, 2021, 28(9): 4-6, 106.

[6] GU T Y, DOLAN-GAVITT B, GARG S. BadNets: identifying vulnerabilities in the machine learning model supply chain[J]. arXiv preprint, 2017, arXiv:1708.06733.

[7] MOHAMMED N, CHEN R, FUNG B C M, et al. Differentially private data release for data mining[C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2011: 493-501.

[8] 傅继彬, 张啸剑, 丁丽萍. MAXGDDP: 基于差分隐私的决策数据发布算法[J]. 通信学报, 2018, 39(3): 136-146.
FU J B, ZHANG X J, DING L P. MAXGDDP: decision data release with differential privacy[J]. Journal on Communications, 2018, 39(3): 136-146.

[9] ZHANG J, CORMODE G, PROCOPIUC C M, et al. PrivBayes[J]. ACM Transactions on Database Systems, 2017, 42(4): 1-41.

[10] 王瑞锦, 唐榆程, 张巍琦, 等. 基于同态加密和区块链技术的车联网隐私保护方案[J]. 网络与信息安全学报, 2020, 6(1): 46-53.
WANG R J, TANG Y C, ZHANG W Q, et al. Privacy protection scheme for Internet of vehicles based on homomorphic encryption and block chain technology[J]. Chinese Journal of Network and Information Security, 2020, 6(1): 46-53.

[11] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective[J]. arXiv preprint, 2017, arXiv:1712.07557.

[12] ABADI M, CHU A, GOODFELLOW I, et al. Deep learning with differential privacy[C]//Proceedings of 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 308-318.

[13] MAO Y L, HONG W B, WANG H, et al. Privacy-preserving computation offloading for parallel deep neural networks training[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1777-1788.

[14] THAPA C, CHAMIKARA M A P, CAMTEPE S, et al. SplitFed: when federated learning meets split learning[J]. arXiv preprint, 2020, arXiv:2004.12088.

[15] 吴茂强, 黄旭民, 康嘉文, 等. 面向车路协同推断的差分隐私保护研究[J]. 计算机工程, 2022, 48(7): 29-35.
WU M Q, HUANG X M, KANG J W, et al. Research on differential privacy protection for collaborative vehicle-road inference[J]. Computer Engineering, 2022, 48(7): 29-35.

[16] 中国信息通信研究院. 车联网白皮书[Z]. 2021.
China Academy of Information and Communications Technology. White paper on Internet of vehicles[Z]. 2021.

[17] 中国智能交通产业联盟. 车路协同信息交互技术要求[Z]. 2021.
China ITS Industry Alliance. Technical requirements for vehicle-road coordination system information interaction[Z]. 2021.

[18] 袁博, 王思源. 隐私计算产品评估体系[J]. 信息通信技术与政策, 2021, 47(6): 12-18.
YUAN B, WANG S Y. Privacy preserving computing product evaluation system[J]. Information and Communications Technology and Policy, 2021, 47(6): 12-18.

[19] MCMAHAN B, MOORE E, RAMAGe D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. [S.l.:s.n.], 2017: 1273-1282.

[20] 梁天恺, 曾碧, 陈光. 联邦学习综述：概念、技术、应用与挑战[J]. 计算机应用, 2021: 已录用.
LIANG T K, ZENG B, CHEN G. Federated learning survey: concept, technology, application and challenge[J]. Journal of Computer Applications, 2021: accepted.

[21] DWORK C. Differential privacy[M]// Encyclopedia of cryptography and security. Boston: Springer US, 2011: 338-340.

[22] 谭作文, 张连福. 机器学习隐私保护研究综述[J].

软件学报, 2020, 31(7): 2127–2156.
TAN Z W, ZHANG L F. Survey on privacy preserving techniques for machine learning[J]. Journal of Software, 2020, 31(7): 2127–2156.
[23] BHOWMICK A, DUCHI J, FREUDIGER J, et al. Protection against reconstruction and its applications in private federated learning[J]. arXiv preprint, 2018, arXiv:1812.00984.
[24] CARLINI N, LIU C, KOS J, et al. The secret sharer: measuring unintended neural network memorization & extracting secrets[J]. arXiv preprint, 2018, arXiv:1802.08232.
[25] 王健宗, 孔令炜, 黄章成, 等. 联邦学习隐私保护研究进展[J]. 大数据, 2021, 7(3): 130–149.
WANG J Z, KONG L W, HUANG Z C, et al. Research advances on privacy protection of federated learning[J]. Big Data Research, 2021, 7(3): 130–149.
[26] SHOKRI R, SHMATIKOV V. Privacy-preserving deep learning[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 1310–1321.
[27] UCHIDA Y, NAGAI Y, SAKAZAWA S, et al. Embedding watermarks into deep neural networks[C]//Proceedings of 2017 ACM on International Conference on Multimedia Retrieval. New York: ACM Press, 2017: 269–277.
[28] 谢宸琪, 张保稳, 易平. 人工智能模型水印研究综述[J]. 计算机科学, 2021, 48(7): 9–16.
XIE C Q, ZHANG B W, YI P. Survey on artificial intelligence model watermarking[J]. Computer Science, 2021, 48(7): 9–16.
[29] 樊雪峰, 周晓谊, 朱冰冰, 等. 深度神经网络模型版权保护方案综述[J]. 计算机研究与发展, 2022, 59(5): 953–977.
FAN X F, ZHOU X Y, ZHU B B, et al. Survey of copyright protection schemes based on DNN model[J]. Journal of Computer Research and Development, 2022, 59(5): 953–977.

## 作者简介

**李明**(1978– ), 男, 中兴飞流信息科技有限公司副总经理, 大数据系统计算技术国家工程实验室副主任, 主要研究方向为大数据、人工智能、云存储、分布式数据库等。

**吕阿斌**(1970– )男, 中兴飞流信息科技有限公司董事长、总经理, 主要研究方向为云计算、大数据、人工智能等。

**收稿日期:** 2022–04–11