中国图象图形学学会
CHINA SOCIETY OF IMAGE AND GRAPHICS

CIG 2023 中国·苏州 | 中国图象图形大会
CHINESE CONGRESS ON IMAGE AND GRAPHICS

基于因果端云协同的可信机器学习

汇报人：张圣宇

浙江大学
百人计划研究员（即将入职）

2023年5月11日

研究背景: 深度学习系统存在不可信风险

JOSEPH SIFAKIS

2007年图灵奖获得者

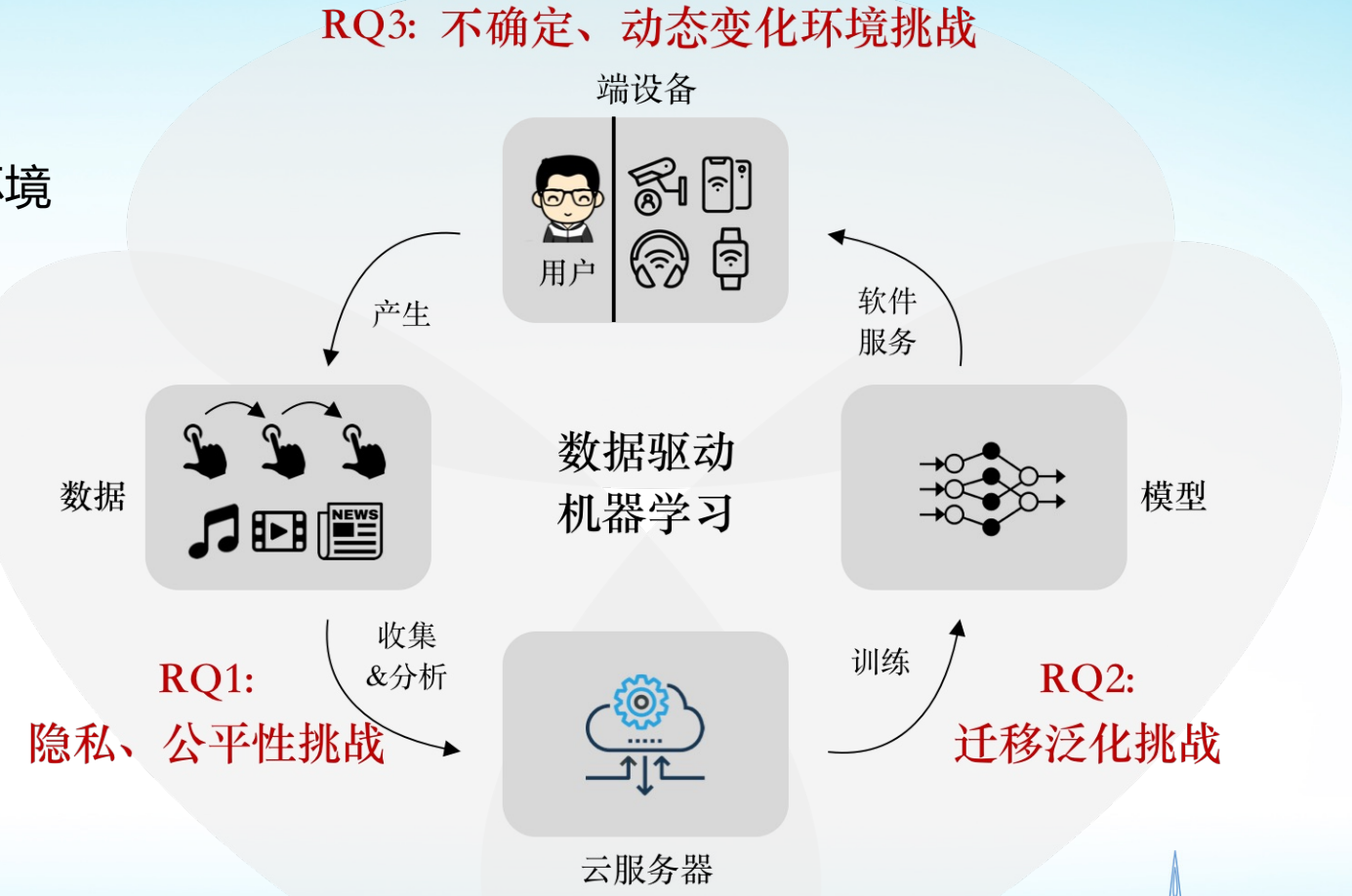
人工智能系统 → **可信系统**

不确定、难以预测、动态变化环境

安全性、实时性挑战

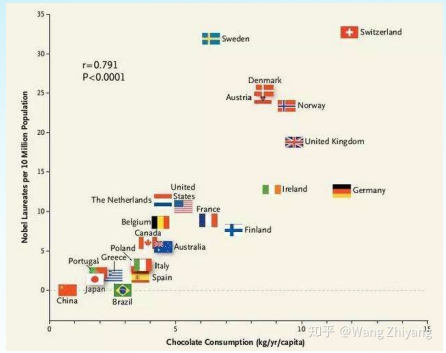
Trustworthy Autonomous System Development. ACM Transactions on Embedded Computing Systems. 2022

鲁棒性、公平性、可泛化性



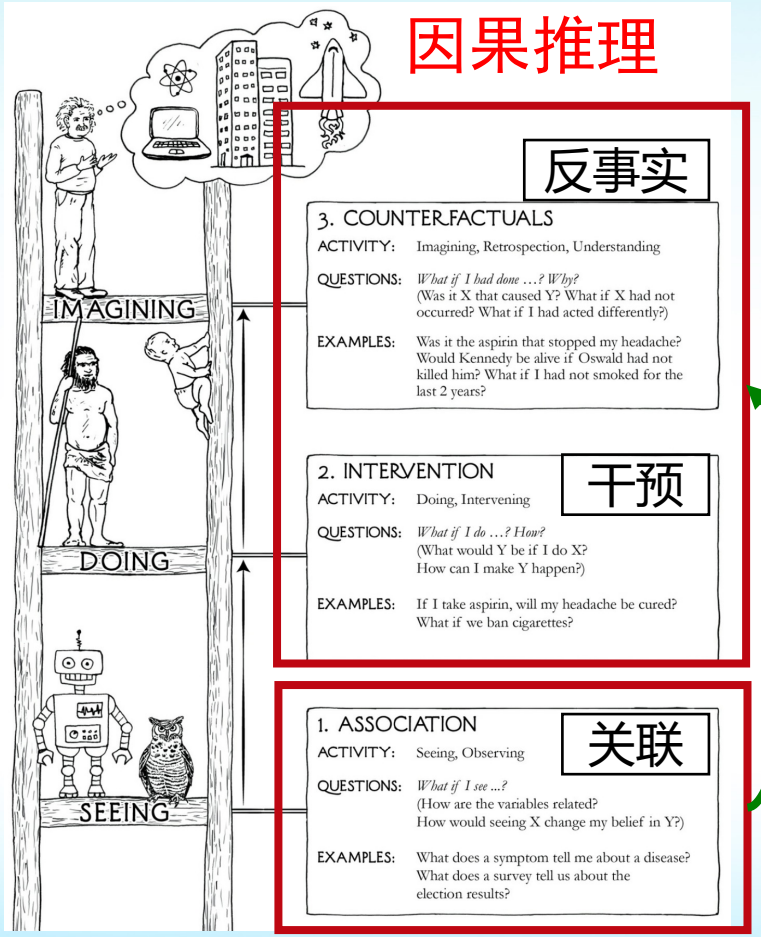
问题主要根源：中心化关联学习的桎梏

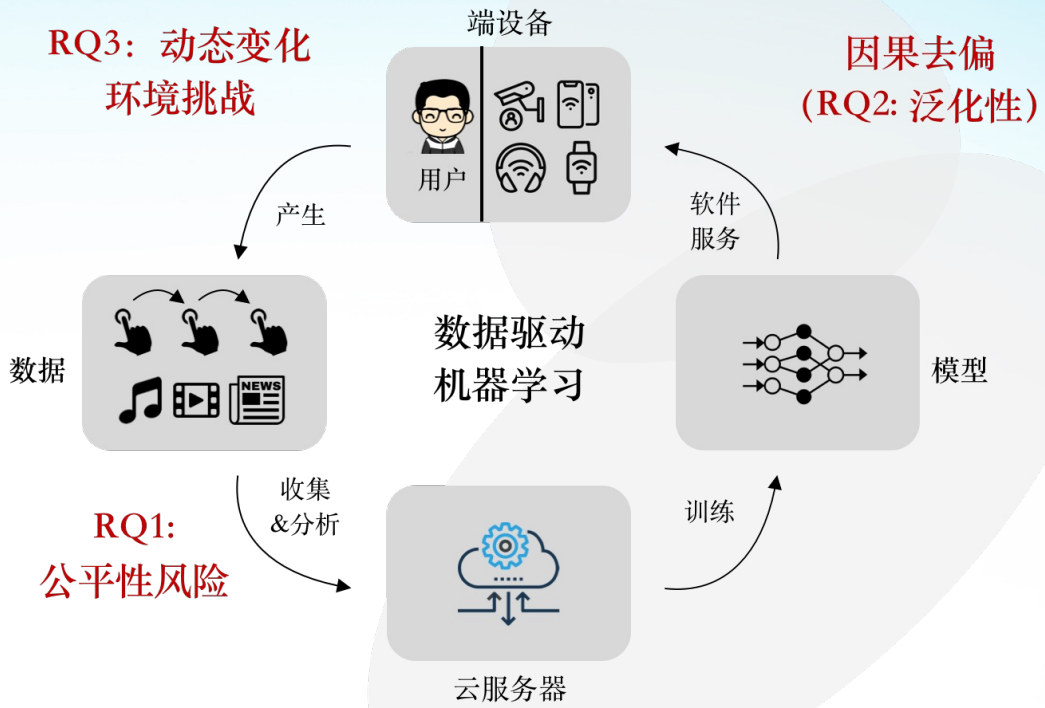
巧克力销量与诺贝尔奖获得数



Judea Pearl

2011年图灵奖获得者





因果端云协同是突破鲁棒性、公平性、可泛化性的重要途径

问题主要根源: 中心化关联学习的桎梏

JOSEPH SIFAKIS

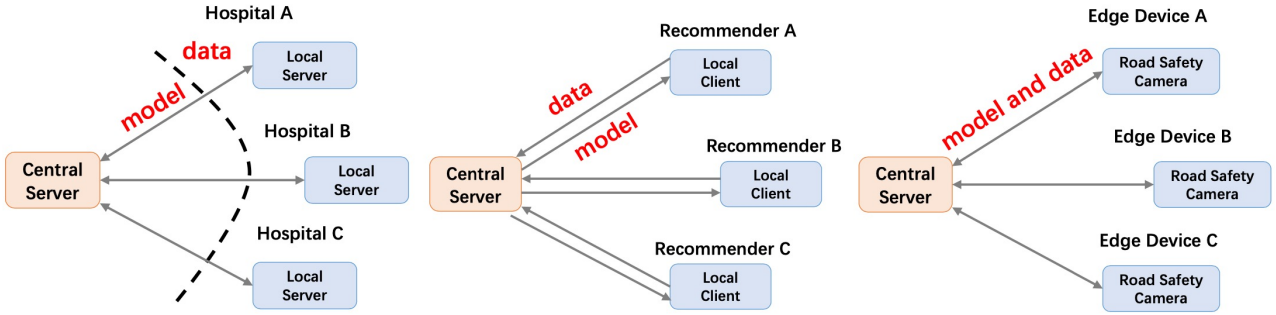
2007年图灵奖获得者

构建可信系统:

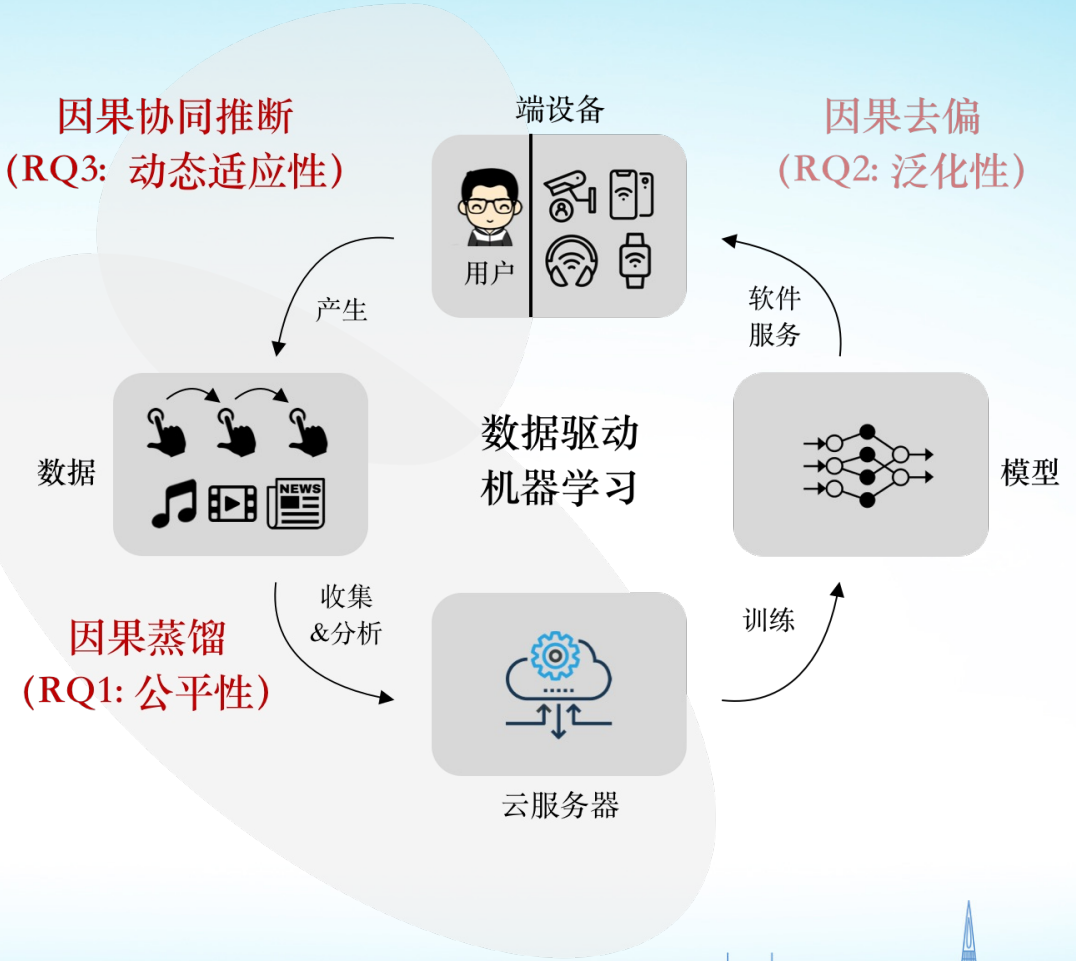
Predictable → Self-adaptation

Centralized → Distributed

Trustworthy Autonomous System Development. ACM Transactions on Embedded Computing Systems. 2022



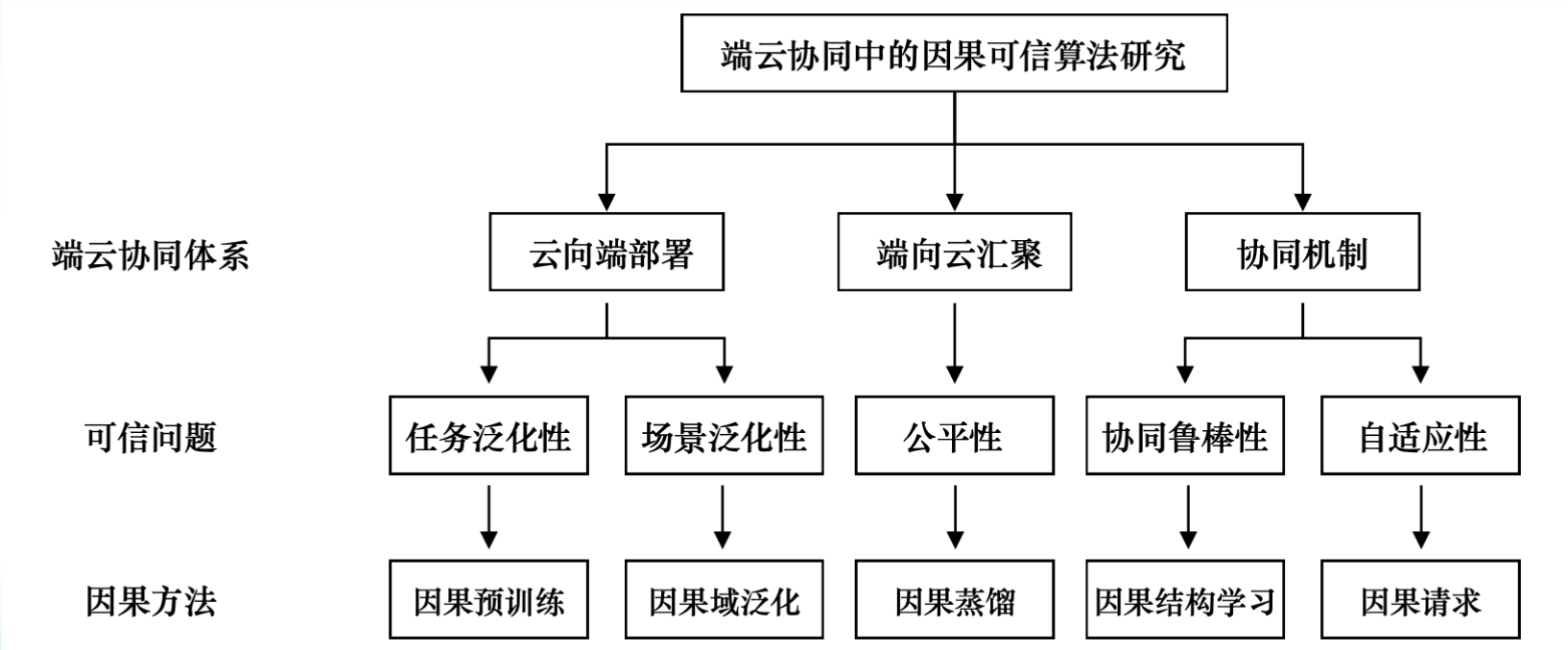
(a) Privacy-Primary Collaboration (b) Efficiency-Primary Collaboration (I) (c) Efficiency-Primary Collaboration (II)



因果端云协同是突破鲁棒性、公平性、可泛化性的重要途径

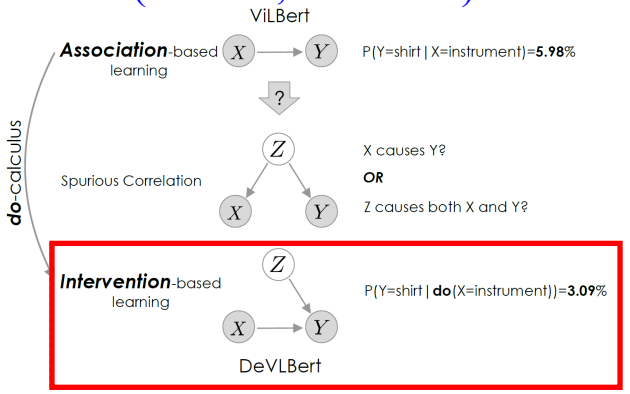
研究成果

- **路线图**：通过因果推断技术和端云协同计算范式突破可信计算对**鲁棒性**、**隐私保护**和**可解释性**的需求

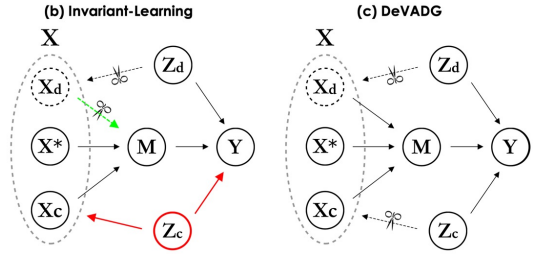


研究成果1: 基于因果推理的去偏、鲁棒学习(Debiased)

大规模因果预训练
(MM 20, CVPR 21)



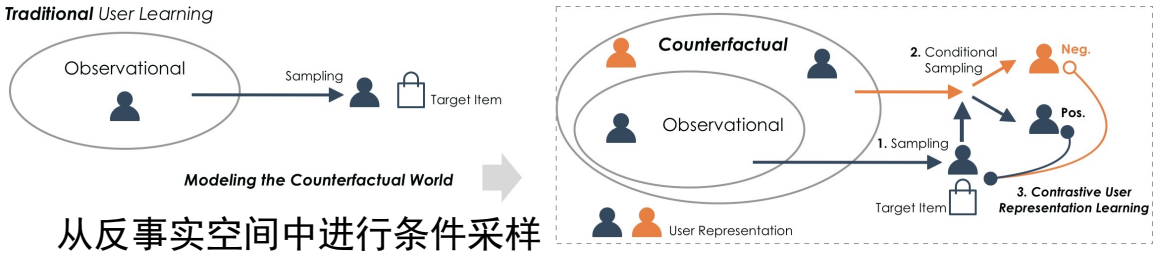
因果跨域泛化（AAAI 2023）



干预

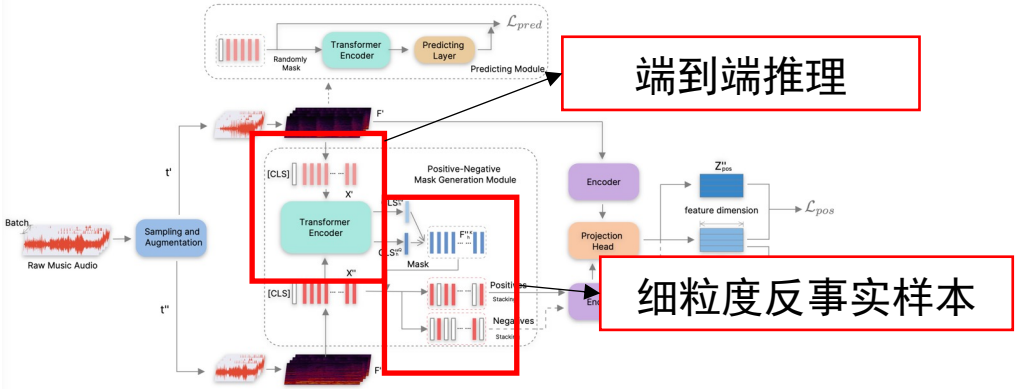
反事实

用户反事实表征学习 (SIGIR 21)



从反事实空间中进行条件采样

内容反事实表征学习 (WWW 22)



端到端推理

细粒度反事实样本

突破传统表征学习在数据稀疏、弱先验、分布迁移下的鲁棒性问题

反事实表征学习与华为诺亚方舟实验室合作，模型上线**华为音乐**

2022年4月提升人均播放次数 5.1%，人均播放时长 5.8%

研究成果1: 基于因果推理的去偏、鲁棒学习(Debiased)

- 数据偏差(bias)使得**关联驱动**的云上大规模预训练吸收虚假关联，影响在**不确定端环境**中的泛化能力，损害鲁棒性

因果分析

P(**衬衫** | **乐器**) = 5.98%

P(**衬衫** | do(**乐器**)) = 3.10%

因共生而存在的强关联 视觉物体/单词 不一定具有 因果关系 （虚假关联）

引入 因果 减弱（消除）虚假关联

“知其然、且知其所以然”

Zhang, S., Jiang, T., Wang, T., Kuang, K,, Yu, J., Yang, H. and Wu, F., DeVLBert: Learning Deconfounded Visio-Linguistic Representations. 28th ACM International Conference on Multimedia (MM), 2020

研究成果1: 基于因果推理的去偏、鲁棒学习(Debiased)

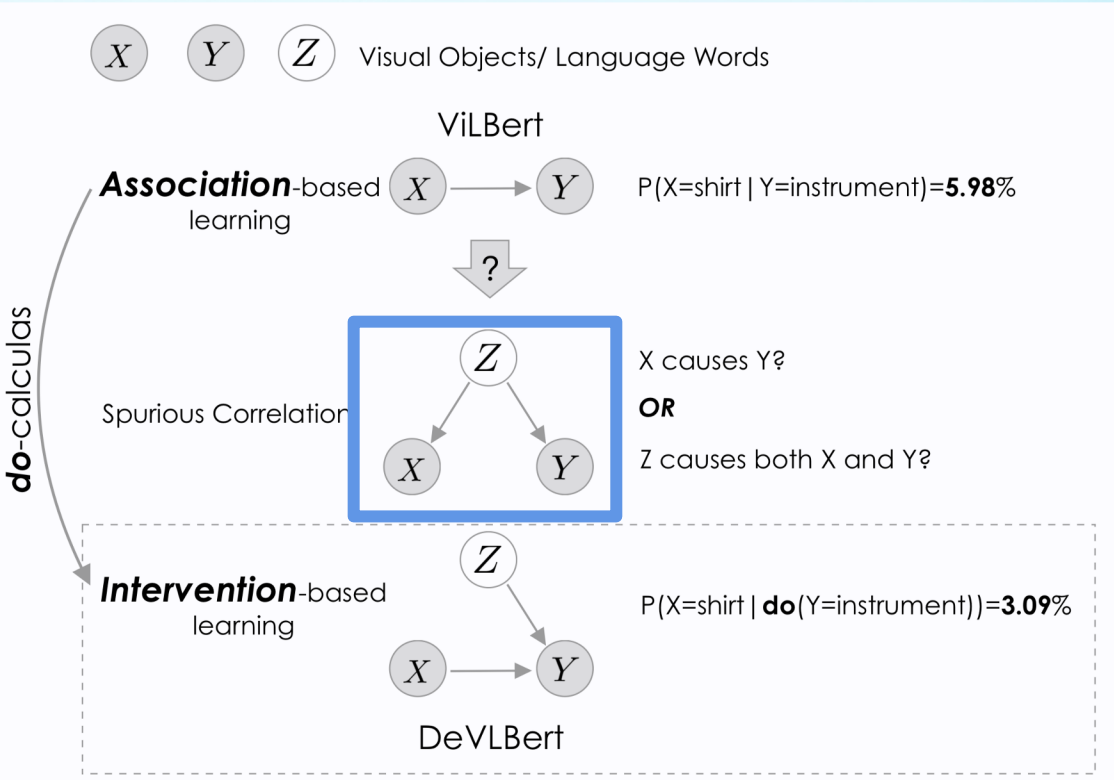
- 从关联驱动到因果干预驱动：
  - 引入***do-***算子（Do-calculas）对上下文进行干预，通过变量干预来显式建模刻画混淆因子对视觉子块和文本单词之间因果效应的影响。

- 因果后门调整
  - 对每个混淆因子进行单独建模，得到关联效应
  - 求取混淆因子先验概率（而非观测下的条件概率）期望，获得干预下因果效应

$$P(Y|X) = \sum_z P(Y, z|X) = \sum_z P(Y|X, z)P(z|X)$$

$$P(Y|X) \rightarrow P(Y|do(X)) = \sum_z P(Y|X, z)P(z)$$

Zhang, S., Jiang, T., Wang, T., Kuang, K., Yu, J., Yang, H. and Wu, F., DeVLBert: Learning Deconfounded Visio-Linguistic Representations. 28th ACM International Conference on Multimedia (MM), 2020

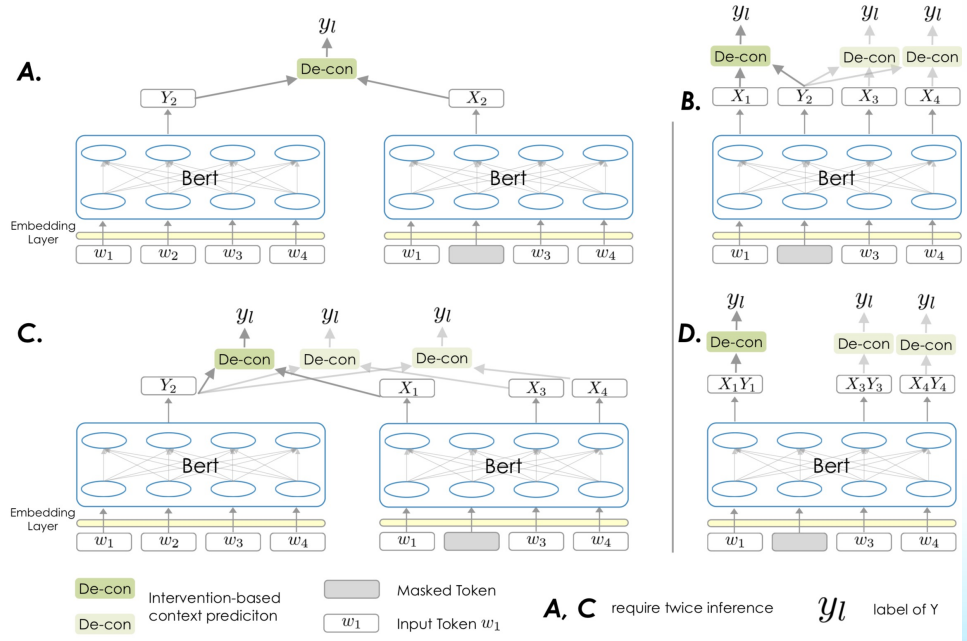


研究成果1: 基于因果推理的去偏、鲁棒学习(Debiased)

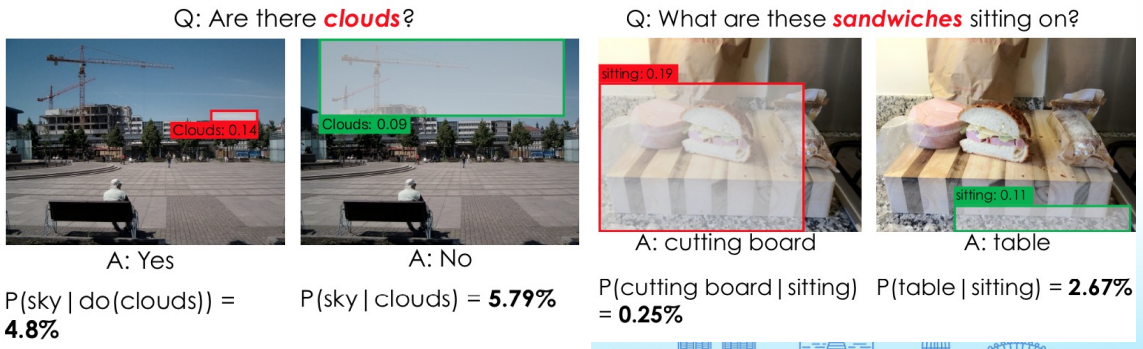
- 基于BERT结构，围绕如何定义干预X和结果Y，设计了四种去混杂因果干预结构以增强预训练模型泛化能力

$$P(Y|do(X)) = \mathbb{E}_z[P(Y|X,z)] = \mathbb{E}_z[\text{softmax}(f_c(\mathbf{x},\mathbf{z}))]$$

$$\approx \text{softmax}(\mathbb{E}_z[f_c(\mathbf{x},\mathbf{z})])$$



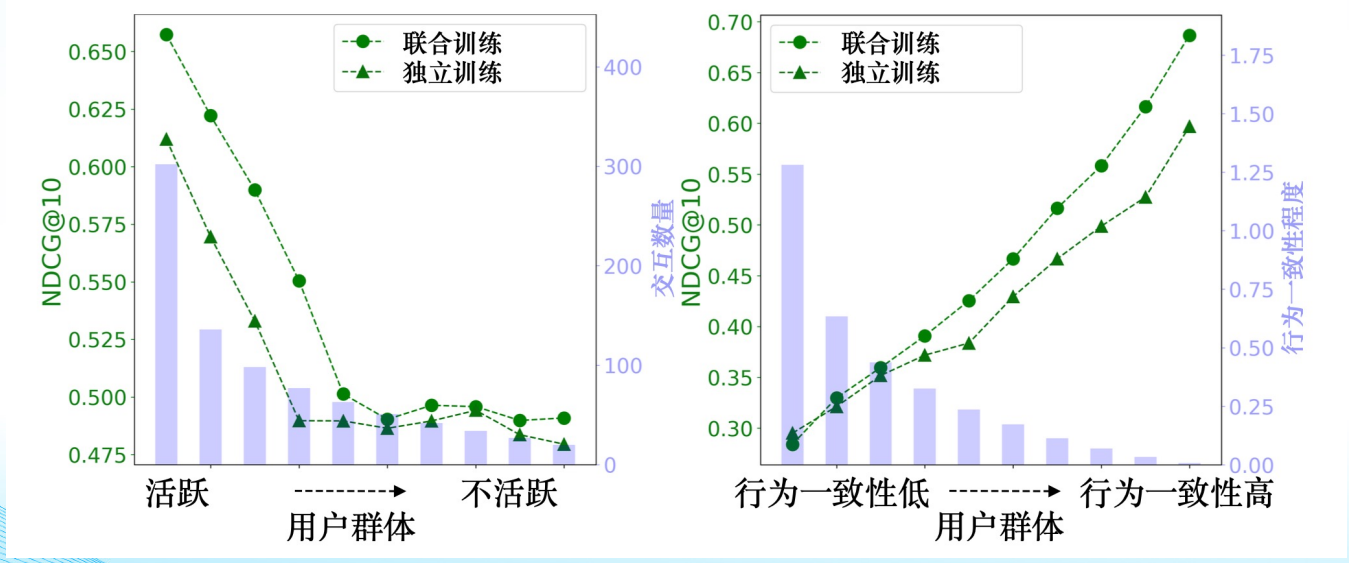
Methods	Image Retrieval (IR) R@1	R@5	R@10	Zero-shot IR R@1	R@5	R@10	VQA test-dev	test-std
SCAN [22]	48.6	77.7	85.2	-	-	-	-	-
BUTD [1]	-	-	-	-	-	-	65.3	65.7
•VisualBERT [24]	-	-	-	-	-	-	70.8	71.0
⊙InterBert [25]	61.9	87.1	92.7	49.2	77.6	86.0	70.3	70.6
°ViLBERT [29] (Baseline)	58.2	84.9	91.5	31.9	61.1	72.8	70.6	70.9
°DeVLBert	61.6	87.1	92.6	36.0	67.1	78.3	71.1	71.5

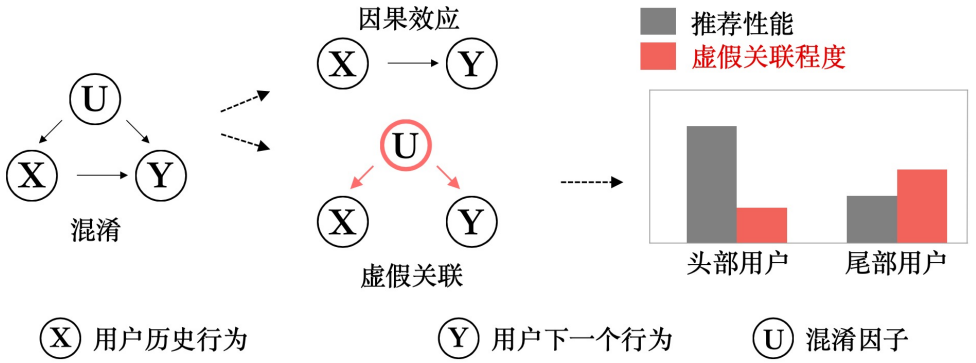


通过减弱虚假关联，注意到更少共现但正确的区域

研究成果2: 异构端模型的因果公平汇聚（端到云）

- 从数据和模型的角度来看，端用户性能异质性有两个主要来源，即自然来源和模型来源。
- 消除模型训练偏差对于异质性的放大影响

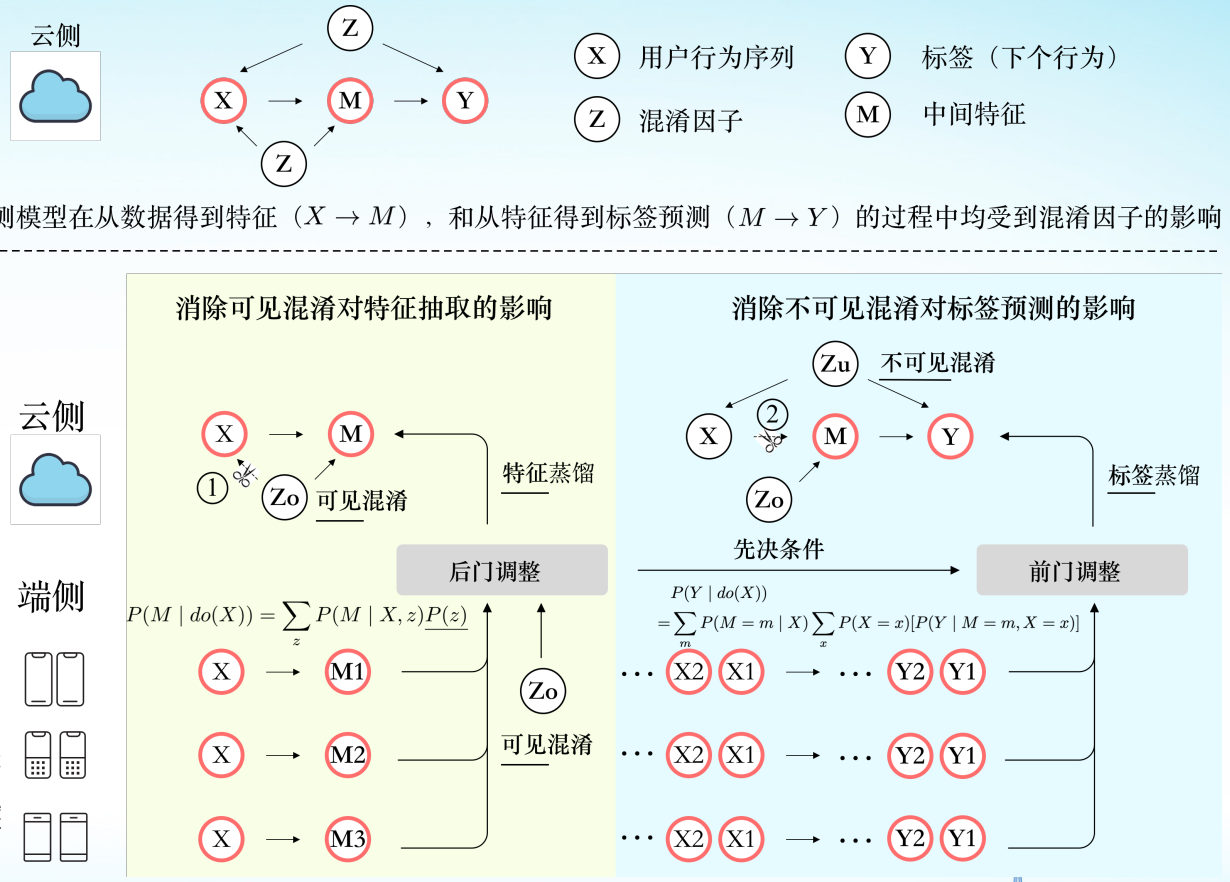




研究成果2: 异构端模型的因果公平汇聚（端到云）

- 引入**后门调整**作用于特征抽取阶段，消除可观测的混淆偏差，是前门调整的先决条件；**前门调整**作用于标签预测阶段，消除未能观测的混淆偏差。

- 后门调整实现了免受**可见混淆**影响的**特征表达（特征因果蒸馏）**，前门调整实现了免受**不可见混淆**影响的**标签预测（标签因果蒸馏）**。

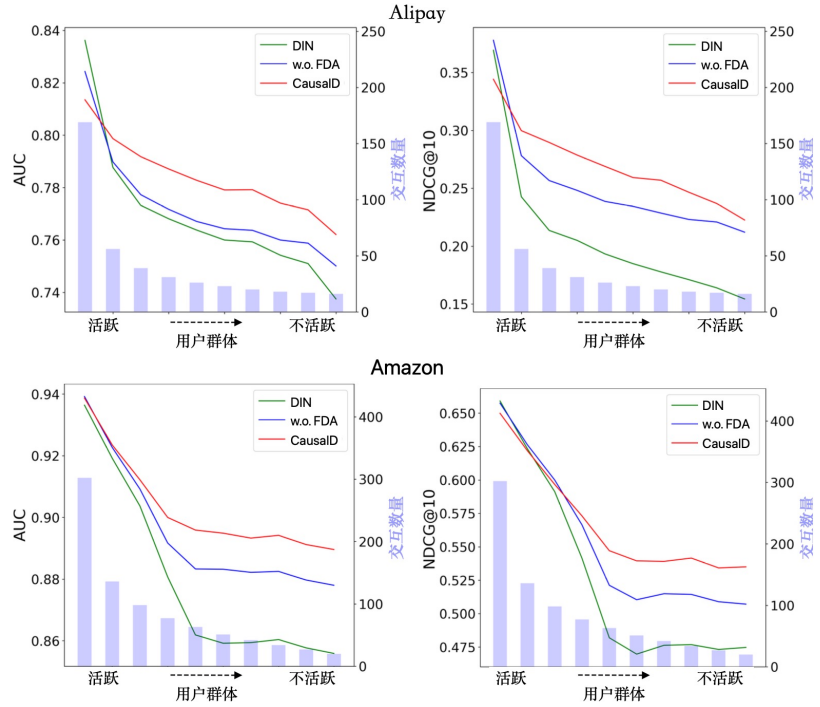


研究成果2: 异构端模型的因果公平汇聚（端到云）

大规模工业推荐数据集上取得显著优势

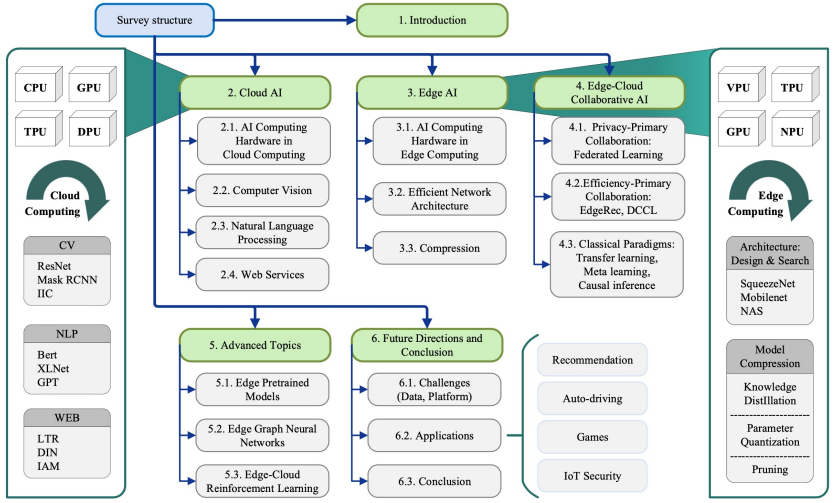
- 在亚马逊推荐数据集和阿里巴巴支付宝推荐数据集上进行了验证
- 模型效果显著优于现有模型去偏差和多模型蒸馏方法
- 模型显著提升长尾用户的服务性能，缓解马太效应

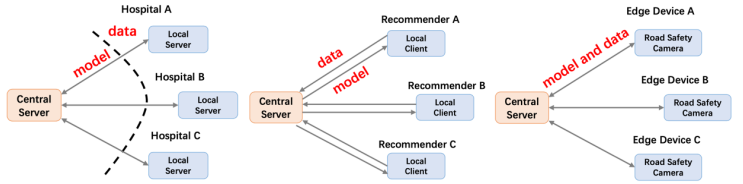
Datasets	Metric	**DIN**	KD	IPS	DebiasD	EnsCTR	MEAL	CausalD	Improv.
MovieLens	AUC	0.8185	0.8187	0.8034	0.8227	0.8257	0.8233	**0.8329**	1.76%
	R@5	0.3102	0.3104	0.3066	0.3231	0.3354	0.3213	**0.3556**	14.64%
	R@10	0.4682	0.4763	0.4652	0.4831	0.4930	0.4837	**0.5170**	10.42%
	NDCG@5	0.2378	0.2382	0.2362	0.2485	0.2589	0.2492	**0.2755**	15.85%
	NDCG@10	0.3145	0.3187	0.3136	0.3258	0.3355	0.3281	**0.3538**	12.50%
	Heterogeneity ↓	6.7422	6.4664	6.3187	6.7020	6.9662	6.7904	**6.1937**	8.14%
Amazon	AUC	0.8873	0.8704	0.8788	0.8954	0.8983	0.8867	**0.9027**	1.74%
	R@5	0.5644	0.5336	0.5555	0.5886	0.5911	0.5698	**0.6069**	7.53%
	R@10	0.6854	0.6515	0.6760	0.7060	0.7087	0.6863	**0.7216**	5.28%
	NDCG@5	0.4794	0.4516	0.4706	0.5007	0.5038	0.4857	**0.5190**	8.26%
	NDCG@10	0.5384	0.5092	0.5294	0.5580	0.5612	0.5426	**0.5751**	6.82%
	Heterogeneity ↓	5.6278	4.8558	4.5988	4.6458	4.6880	5.3794	**4.5514**	19.13%
Alipay	AUC	0.7691	0.7615	0.7623	0.7712	0.7700	0.7749	**0.7777**	1.12%
	R@5	0.1669	0.1727	0.1778	0.2057	0.1831	0.2343	**0.2547**	52.61%
	R@10	0.3518	0.3682	0.3953	0.3675	0.3689	0.3938	**0.4457**	26.69%
	NDCG@5	0.1186	0.1221	0.1237	0.1532	0.1307	0.1745	**0.1851**	56.07%
	NDCG@10	0.2076	0.2165	0.2289	0.2314	0.2204	0.2517	**0.2779**	33.86%
	Heterogeneity ↓	4.7834	4.7798	4.2870	4.5788	4.8856	4.5540	**3.4622**	27.62%



研究成果3: 因果端云协同机制 (协同推断)

从端云协同的角度梳理和统一了传统学习框架，描绘了新的端云协同范式和应用(T-KDE)

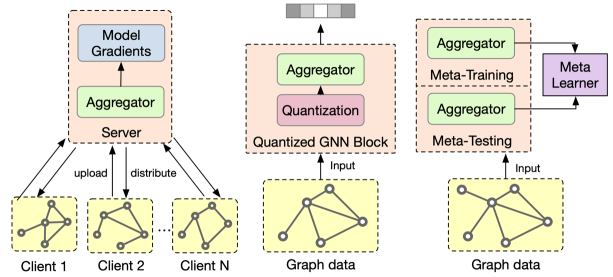




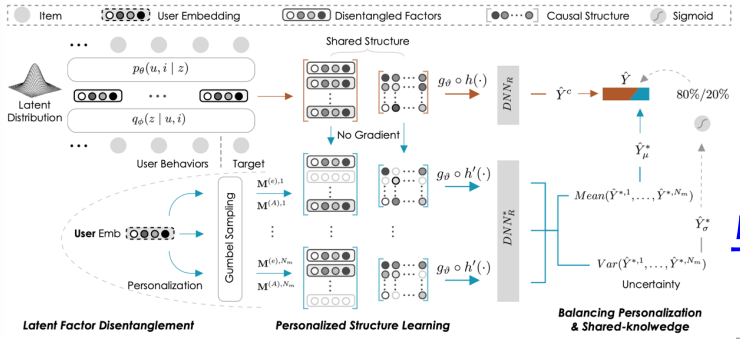
(a) Privacy-Primary Collaboration (b) Efficiency-Primary Collaboration (I) (c) Efficiency-Primary Collaboration (II)

TABLE 2: Device-Cloud Collaborative Modeling

	Collaboration Manner		Collaboration Concerns			
	co-training	co-inference	privacy	storage efficiency	communication efficiency	personalization
Semantic QA cache [212]		✓			✓	✓
EdgeRec System [24]		✓			✓	✓
Auto-Split [213]		✓		✓	✓	
CoEdge [214]		✓		✓	✓	
Colla [215]	✓			✓		✓
DCCL [216]	✓			✓		✓
MC^2-SF [217]	✓	✓				✓
FedAvg [23]	✓		✓		✓	
FML [204]	✓		✓	✓	✓	✓
Personalized FedAvg [202]	✓		✓		✓	✓
HyperCluster [200]	✓		✓		✓	✓
Federated Evaluation [201]	✓	✓	✓			✓

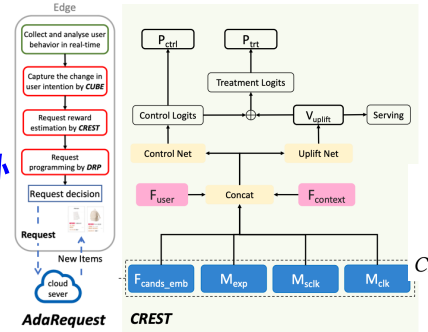


(a) Federated GNN (b) Quantized GNN (c) GNN with Meta Learning



因果约束的共性-个性发现与协同(T-PAMI)

因果指导的大-小模型协同 (KDD)



$$CIA: \{Y_i(0), Y_i(1)\} \perp z_i | X_i,$$
$$CATE_P(X_i) = E[Y_i(1)|X_i] - E[Y_i(0)|X_i].$$

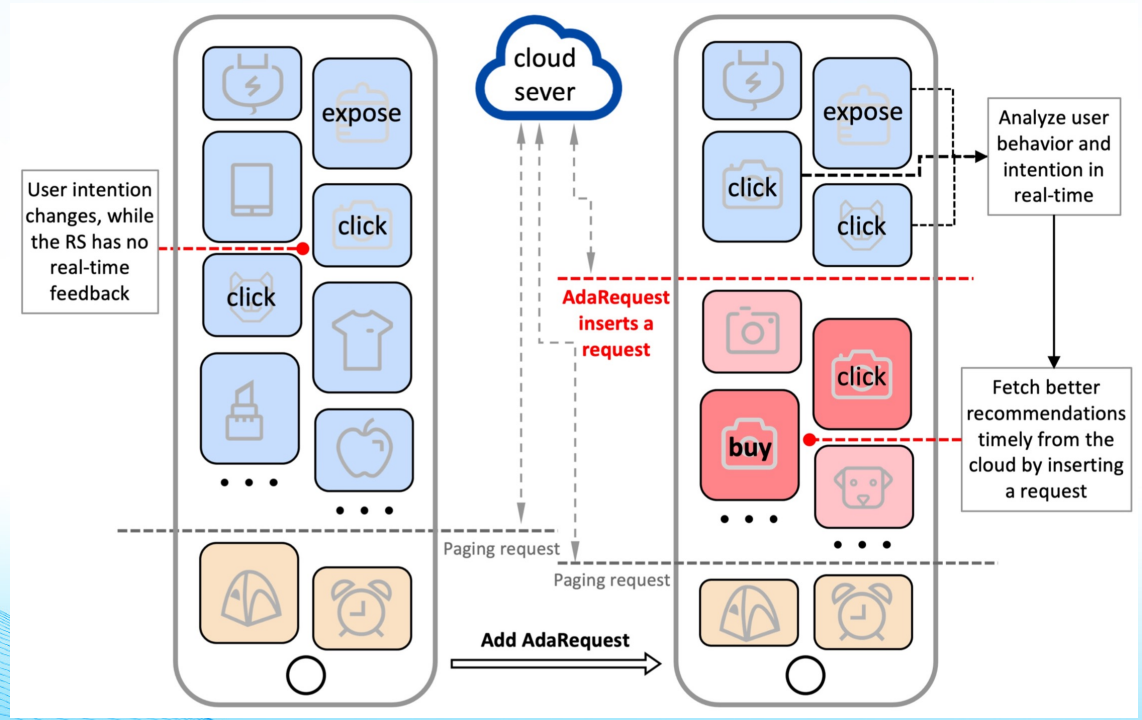
$$\text{Maximize} \sum\nolimits'_{X_i \in \mathcal{X}} z_i CATE_P(X_i),$$
$$\text{subject to} \sum\nolimits_{X_i \in \mathcal{X}} z_i CATE_Q(X_i) < \theta,$$
$$CATE_Q(X_i) = E[Q_i(1)|X_i] - E[Q_i(0)|X_i] = \lambda,$$

在资源、隐私约束下有效提升机器学习模型的自适应能力和稳定性

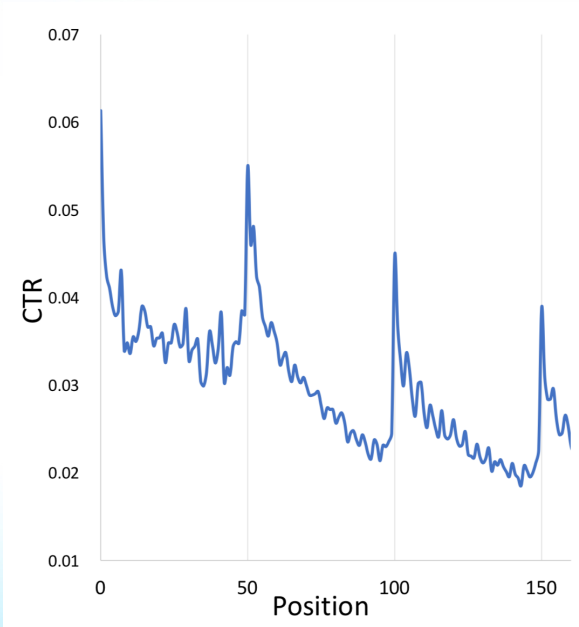
研究成果3: 因果端云协同机制（协同推断）

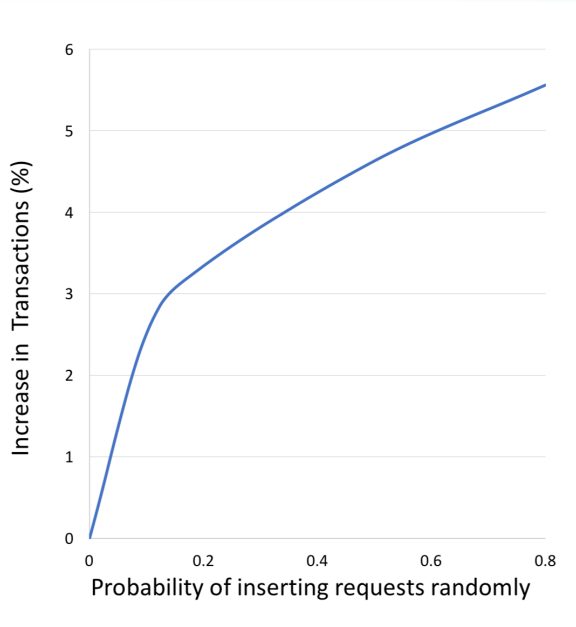
- **动态变化的端环境**导致资源有限情况下云模型的延迟响应，导致端侧服务与端侧环境的不匹配，损害用户的服务体验

手机淘宝商品推荐系统



用户点击率在云模型响应后陡升

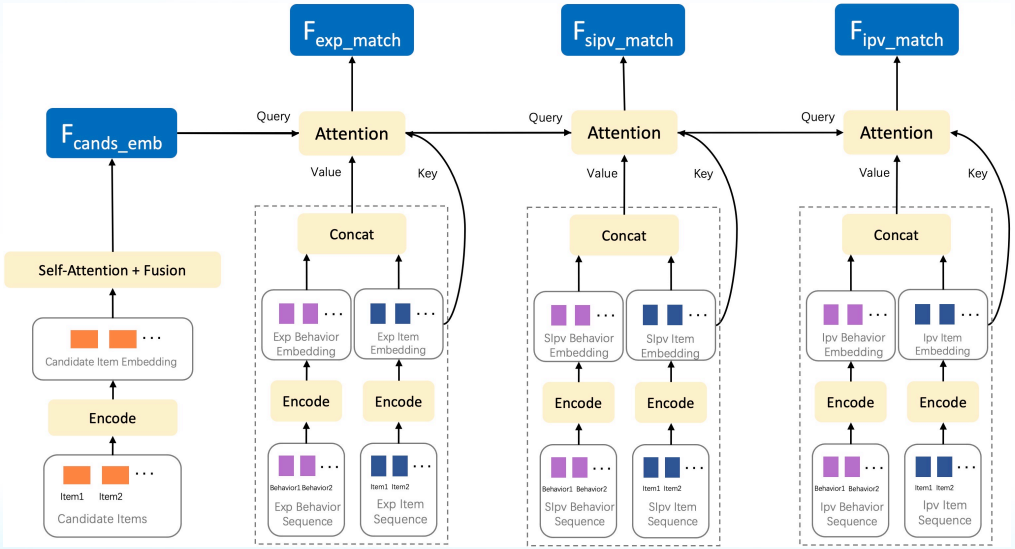




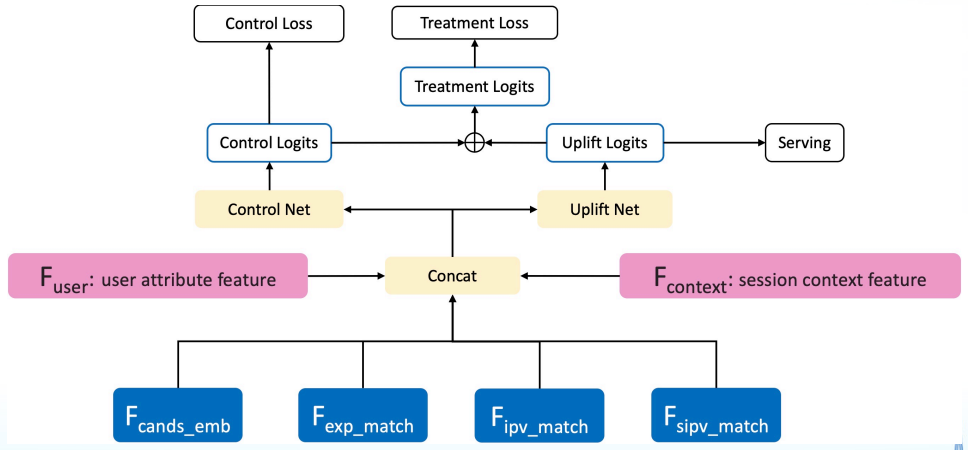
[3] Xufeng Qian, Yue Xu, Fuyu Lv, **Shengyu Zhang***, Ziwen Jiang, Qingwen Liu, Xiaoyi Zeng, Tat-Seng Chua, Fei Wu. Intelligent Request Strategy Design in Recommender System, KDD 2022. (**Corresponding Author**)

研究成果3: 因果端云协同机制（协同推断）

- **端设备部署小模型**实时检测端环境变化（用户兴趣意图变化）



- 通过**因果潜在结果**模型预估请求大模型响应价值
- **动态规划对云侧大模型的请求**，最大化资源有限时的线上收益。



[3] Xufeng Qian, Yue Xu, Fuyu Lv, **Shengyu Zhang***, Ziwen Jiang, Qingwen Liu, Xiaoyi Zeng, Tat-Seng Chua, Fei Wu. Intelligent Request Strategy Design in Recommender System, KDD 2022. (**Corresponding Author**)

研究成果3: 因果端云协同机制（协同推断）

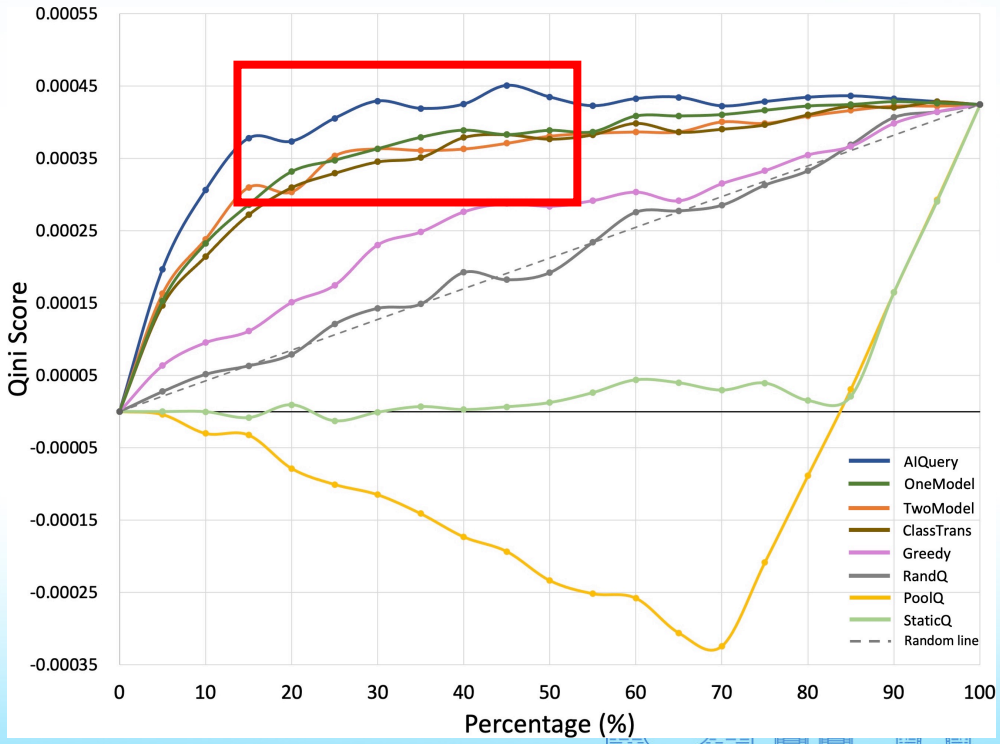
- 淘宝首页推荐

#Num of Records	#Num of Users	#Num of Items
1.76×10^8	1.01×10^7	2.98×10^7

Metric	AIQuery	OneModel	TwoModel	ClassTrans	Greedy	RandQ	PoolQ	StaticQ	p-value
Qini AUUC ↑	**1.8288**	1.4767	1.4007	1.3558	0.4802	0.0398	−3.0404	−1.6724	1.3298×10^{-6}
Qini (50) ↑	**4.3450**	3.8859	3.8061	3.7662	2.8371	1.9209	−2.3353	0.1229	2.3100×10^{-3}
MSE Y* ↓	**4.3497**	4.3526	4.3524	-	-	-	-	-	7.5479×10^{-6}
AUC ↑	**0.8145**	0.7980	0.7980	-	0.7974	0.5017	0.4706	0.4817	3.5235×10^{-9}
MSE ↓	**1.0833**	1.0843	1.0839	-	1.0840	504.9	711.9	846.6	6.3846×10^{-3}

- X轴
  - 响应量限制（云模型计算资源限制）

- 在不同资源限制下取得了一致的提升
- 在**低资源**情况下提升更为显著



[3] Xufeng Qian, Yue Xu, Fuyu Lv, **Shengyu Zhang***, Ziwen Jiang, Qingwen Liu, Xiaoyi Zeng, Tat-Seng Chua, Fei Wu. Intelligent Request Strategy Design in Recommender System, KDD 2022. (**Corresponding Author**)

研究成果3: 因果端云协同机制（协同推断）

当前推荐系统存在的问题

通信开销大
隐私破坏风险
隐时反馈噪声多
无法实时感知用户

因果结构学习机制
因果潜在结构框架
不确定性预估方法
…

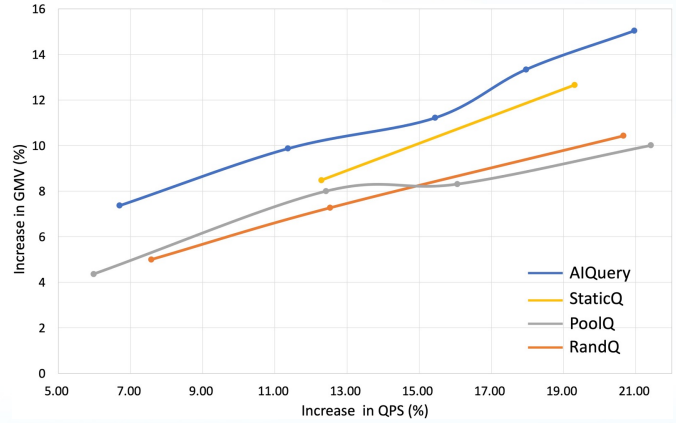
因果+端云协同

共性-个性协同
大-小模型协同
隐私-效率协同
…

直接经济效益
(购买率)

PR in N	NoQ	RandQ	PoolQ	StaticQ	AIQuery
10	0.889	1.174	1.177	1.130	**2.289**
20	1.660	2.197	2.164	2.045	**4.173**

平台经济效益
(商品交易总值)



该系列工作与阿里巴巴达摩院、淘宝搜索推荐团队合作，**因果端云协同系统**于2021年10月成功应用上线于淘宝首页推荐，支持**亿级**用户端侧推理实时在线需求，于**2021 年双 11 期间提升日均成交金额超 3%**

总结

云向端泛化

面向异构端设备、复杂端场景的大规模预训练

端向云汇聚

融合不同场景、不同能力的统一模型

协同推断/训练

结合端计算和云计算的优势互补，端云一体化

端云协同的分布式机器学习系统

异构设备：音箱、手环、手机
复杂能力：听觉、触觉、视觉
动态环境：天气、活动、光照

谢谢！