隐私计算技术保障大数据跨云平台安全共享

任浩，王晓明

西安浩瀚明景信息科技有限公司，陕西 西安 712000

摘　　要： 在当今数字化时代，大数据已成为推动社会进步和经济发展的关键要素。随着云计算技术的广泛应用，不同云平台间的数据共享需求日益增长。然而，数据在跨云平台共享过程中面临着诸多安全挑战，如数据泄露、隐私侵犯等风险，这严重制约了数据价值的充分释放。隐私计算技术作为一种新兴的数据安全解决方案，为解决这一问题提供了有力支撑。因此，探索隐私计算技术在大数据跨云平台安全共享中的应用，对于推动数据要素市场的健康发展、促进数字经济与实体经济的深度融合具有重要意义。

关 键 词： 隐私计算技术；大数据；跨云平台；安全共享

Privacy Computing Technology Ensures the Secure Sharing of Big Data Across Cloud Platforms

Ren Hao, Wang Xiaoming

Xi 'an Haohan Mingjing Information Technology Co., LTD. Xi'an, Shaanxi 712000

Abstract: In today's digital age, big data has become a key factor driving social progress and economic development. With the widespread application of cloud computing technology, the demand for data sharing across different cloud platforms is growing. However, data sharing across cloud platforms faces numerous security challenges, such as data breaches and privacy violations, which severely limit the full realization of data value. Privacy-preserving computation technology, as an emerging data security solution, provides strong support for addressing these issues. Therefore, exploring the application of privacy-preserving computation technology in secure data sharing across cloud platforms is crucial for promoting the healthy development of the data element market and facilitating the deep integration of the digital economy with the real economy.

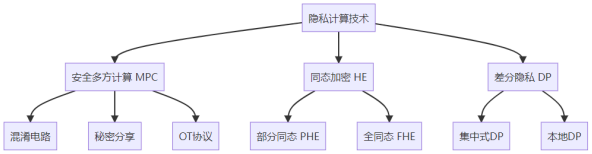
Keywords: privacy computing technology; big data; cross cloud platform; secure sharing

引言

随着大数据技术的飞速发展，数据已成为推动社会进步和经济发展的重要资源。然而，在数据共享与利用的过程中，如何保障数据的隐私和安全成为亟待解决的问题。隐私计算技术作为一种新兴的技术手段，为大数据跨云平台安全共享提供了有效的解决方案。本文将深入探讨隐私计算技术的原理、应用及挑战，并分析其在保障大数据跨云平台安全共享中的重要作用。

一、隐私计算技术概述

隐私计算（PrivacyCompute）是指在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合。它强调数据可用不可见，保护数据全生命周期的安全，旨在通过技术手段确保数据在传输、存储和处理过程中的隐私性。隐私计算技术包括安全多方计算（SecureMulti-PartyComputation,MPC）、同态加密（HomomorphicEncryption,HE）、差分隐私（DifferentialPrivacy,DP）等多种技术手段（见图1）（见表1）。



>图 1 隐私计算技术框架图

作者简介：任浩（1987.11-），男，汉族，陕西商洛人，本科，中级工程师，从事计算机科学与技术研究工作。

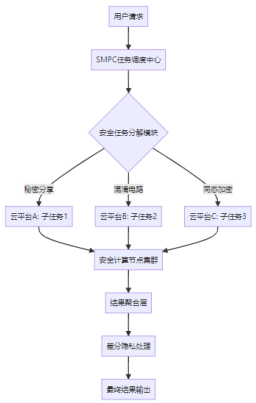
表1 技术对比

技术	核心优势	主要局限	适用场景
MPC	数据不泄露	通信开销高	多方联合计算
HE	密文可计算	计算效率低	云端数据处理
DP	统计隐私保护	数据精度损失	数据发布与分析

二、隐私计算技术在大数据跨云平台安全共享中的应用

（一）安全多方计算

安全多方计算（SecureMulti-partyComputation,SMPC）通过密码学协议实现多方数据协同计算，确保各参与方仅获取计算结果而无法窥探原始数据。在跨云平台场景中，SMPC技术通过分布式计算框架（如秘密分享、混淆电路）将计算任务分解为多个子任务，由各云平台独立执行（见图2）。例如，金融风控领域可通过SMPC实现跨机构黑名单联合查询，各银行输入加密后的用户标识，系统输出匹配结果而不暴露具体数据。技术挑战包括计算效率与通信开销的平衡，需结合轻量级算法（如SPDZ协议）优化性能[1]。



>图2 分布式计算框架图

（二）同态加密

同态加密（HomomorphicEncryption,HE）支持对密文的直接代数运算，结果解密后与明文运算一致（见表2）。跨云平台中，HE允许数据所有者将加密数据上传至第三方云，云端无需解密即可完成分析。例如，政府统计部门可汇总加密的GDP数据，云端直接计算总和或平均值[2]。全同态加密（FHE）虽功能完备但计算成本高，实际应用多采用部分同态加密（如Paillier算法）。当前研究重点在于硬件加速（如GPU/FPGA优化）和层次化HE方案，以提升处理大规模数据的可行性[3]。

表2 技术对比表

类型	计算支持	跨云适用场景	性能损耗
加法同态	SUM/AVG	金融跨平台对账	20-50x
乘法同态	乘积/方差	供应链联合预测	100-200x
全同态	任意计算	军事情报协同分析	1000x+

（三）差分隐私

差分隐私（DifferentialPrivacy,DP）通过数学机制（如拉普拉斯噪声、指数机制）确保查询结果对单条记录的敏感性可控。跨云数据共享中，DP可应用于聚合统计或数据发布场景。例如，电商平台在联合用户行为分析时，对访问量添加噪声后再汇总，避免推断特定用户的购物记录。技术实现需权衡隐私预算（ε值）与数据效用，动态调整噪声量。新兴研究探索本地化差分隐私（LDP）在边缘计算中的应用，以及DP与深度学习模型的结合（如PATE框架），进一步扩展其在跨云环境中的适应性[4]。

三、隐私计算技术的未来发展趋势

（一）标准化与规范化

隐私计算技术的标准化与规范化是未来发展的关键方向之一。随着数据安全法规（如GDPR、CCPA、《数据安全法》）的逐步完善，企业和机构对隐私保护的需求日益增长。然而，当前隐私计算技术（如同态加密、安全多方计算、差分隐私）在不同平台和行业中的实现方式各异，缺乏统一的协议和接口标准，导致跨平台数据共享存在兼容性问题[5]。未来，国际组织（如ISO、IEEE）和行业联盟（如隐私计算联盟）将推动隐私计算技术的标准化进程。例如，制定通用的数据加密格式、计算协议和API接口，确保不同云服务商（如AWS、Azure、阿里云）能够无缝集成隐私计算能力。此外，标准化还将涉及性能评估指标，如计算延迟、通信开销、隐私保护强度等，以便企业选择合适的技术方案。标准化不仅能降低技术应用门槛，还能促进监管合规。例如，在跨境数据流动场景中，统一的标准可帮助各国监管机构评估隐私计算方案的安全性，减少合规成本。同时，开源社区（如FATE、TensorFlowPrivacy）的贡献也将加速标准落地，推动隐私计算成为数据流通的基础设施[6]。

（二）跨行业合作

目前，金融、医疗、政务、物联网等行业对数据共享的需求强烈，但各自的数据格式、安全要求和业务逻辑存在差异，单一技术方案难以满足所有需求。在医疗领域，隐私计算可用于跨机构联合研究，如多中心临床试验或流行病预测[7]。例如，医院可通过安全多方计算（SMPC）共享加密的患者数据，在不泄露个人隐私的情况下训练AI模型。金融行业则关注反欺诈和信用评估，银行可利用同态加密进行加密数据联合分析，避免敏感信息泄露。物联网领域（如智能家居、车联网）需要轻量级隐私计算方案，确保设备数据在边缘计算环境中安全聚合。未来，行业联盟（如医疗数据共享联盟、金融科技协会）将推动跨行业合作，建立通用的数据共享框架。例如，医疗行业可借鉴金融行业的隐私计算标准，优化自身的患者数据脱敏方案。同时，跨行业合作也将促进技术创新，如结合区块链的隐私计算方案，确保数据共享的不可篡改性[8]。

（三）技术创新与优化

隐私计算技术的核心挑战在于如何有效平衡安全性、计算效率和实际可用性之间的关系。当前主流技术方案均存在各自的局限性：全同态加密（FHE）虽然能提供最高级别的隐私保护，但其巨大的计算开销使其难以应用于大规模数据场景；安全多

方计算（SMPC）在计算效率方面表现较好，但随着参与方数量的增加，其通信成本会呈指数级上升；差分隐私（DP）虽然在统计查询场景中表现优异，但在机器学习等复杂计算任务中往往会显著影响模型的精度[9]。针对这些技术瓶颈，未来的创新突破将主要沿着四个关键路径展开：在算法层面，层次化同态加密（LeveledHE）和稀疏化差分隐私（SparseDP）等新型算法可以在保证安全性的同时显著降低计算负担；硬件加速方面，通过GPU、FPGA、TPU等专用计算芯片来优化加密计算流程，将大幅提升FHE和SMPC的实用价值；混合计算架构通过将多种隐私计算技术（如SMPC+DP、HE+区块链）进行有机整合，可以针对不同应用场景提供更加灵活的解决方案；联邦学习与隐私计算的深度融合则能在分布式机器学习框架中嵌入隐私保护机制，实现安全可靠的协同模型训练。值得注意的是，随着量子计算技术的快速发展，现有加密体系正面临前所未有的挑战，这使得后量子密码学（PQC）研究成为隐私计算领域的重要方向[10]。综合来看，隐私计算技术正在向更高效、更通用、更安全的方向持续演进，其作为数字经济时代关键基础设施的战略地位将日益凸显，有望为跨行业数据要素的安全流通提供坚实的技术保障。

四、结束语

隐私计算技术为大数据跨云平台安全共享提供了有效的解决方案。通过安全多方计算、同态加密等技术手段，隐私计算技术实现了数据在传输和处理过程中的隐私保护。然而，隐私计算技术还面临技术壁垒和商业挑战等问题。未来，随着标准化、规范化和跨行业合作的不断推进，隐私计算技术将在更多领域得到广泛应用，为大数据的安全共享和利用提供有力保障。

参考文献

[1] 王森强 . 物联网大数据安全服务云平台建设分析 [J]. 数字通信世界 ,2023,(04):56-58.

[2] 姚利侠 , 付萍华 , 周红艳 . 云平台的大数据信息安全机制的几点探讨 [J]. 网络安全技术与应用 ,2022,(08):68-70.

[3] 张晓伟 . 基于云平台的大数据信息安全保护策略分析 [J]. 信息记录材料 ,2021,22(08):185-187.

[4] 宋飞 , 王亮 , 张景中 , 等 . 物联网大数据安全服务云平台解决方案 [J]. 信息技术与标准化 ,2019,(09):50-52+72.

[5] 王垒 . 新时期云平台下大数据信息的安全机制探讨 [J]. 通讯世界 ,2019,26(02):82-83.

[6] 王冰 . 在“大数据”时代背景下探究计算机信息处理技术 [J]. 长江信息通信 ,2021(11):173-175.

[7] 科尔仑 . 基于大数据时代背景下计算机信息处理技术研究 [J]. 电子测试 ,2021(22):132-134.

[8] 程颂阳 . 大数据环境下计算机信息处理技术的运用研究 [J]. 信息与电脑 (理论版),2021(21):1-3.

[9] 何春 . 云环境下的大数据计算机处理技术研究 [J]. 数码世界 ,2020(11):81-82.

[10] 曾麒 . “大数据”环境下的计算机信息处理技术分析与研究 [J]. 科技资讯 ,2020(20):16-18.