Computer Science and Application 计算机科学与应用, 2026, 16(1), 1-7
Published Online January 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.161001

Hans汉斯

数智技术在金融科技客户隐私保护中的应用研究

程维刚

河北金融学院实验教学中心，河北 保定

收稿日期：2025年12月2日；录用日期：2025年12月30日；发布日期：2026年1月7日

摘 要

目的：在金融科技持续深化的背景下，客户数据呈现高频采集、深度关联化特征，隐私泄露与不当使用风险显著攀升。本研究旨在探讨如何利用数智技术构建系统化、可验证的隐私保护机制，以增强数据治理能力并提升金融业务的安全韧性。方法：基于文献分析、综合技术框架构建、典型场景验证与隐私风险评估，系统梳理差分隐私、联邦学习、区块链可信审计等关键技术的运行逻辑与适配边界，从数据全流程视角提出跨技术协同的综合治理方案。结果：研究发现，多类数智技术协同应用可显著降低数据重识别、越权调用等风险，同时保持模型在关键业务指标上的可用性，并提升数据处理的可控性与审计透明度，具有良好的工程推广潜力。结论：数智技术为金融科技构建隐私保护与业务创新并重的新范式提供可行路径。本研究提出的框架与风险评估体系，可为构建安全、可信、可持续的金融数据治理结构提供理论依据与方法参考。

关键词

数智技术，金融科技，隐私保护机制，隐私计算，数据安全治理

Research on the Application of Intelligent Digital Technologies in Customer Privacy Protection in FinTech

Weigang Cheng

Hebei Finance University Experimental Teaching Center, Baoding Hebei

Received: December 2, 2025; accepted: December 30, 2025; published: January 7, 2026

文章引用: 程维刚. 数智技术在金融科技客户隐私保护中的应用研究[J]. 计算机科学与应用, 2026, 16(1): 1-7.
DOI: 10.12677/csa.2026.161001

Abstract

Purpose: As financial technology continues to advance, customer data is increasingly collected and deeply utilized, leading to heightened risks of privacy leakage and improper use. This study aims to explore how intelligent digital technologies can be employed to construct a systematic and verifiable privacy protection mechanism, thereby enhancing data governance capabilities and strengthening security resilience in financial services. Methods: Through literature analysis, an integrated technical framework, scenario-based verification, and privacy risk assessment, this study examines the operational logic and applicability boundaries of key technologies—such as differential privacy, federated learning, and blockchain-based trusted auditing—from a full data-lifecycle perspective. A cross-technology collaborative governance scheme is proposed. Results: The findings show that coordinated deployment of intelligent digital technologies significantly reduces risks of data re-identification and unauthorized access, while maintaining acceptable model performance. These technologies also improve controllability and transparency of data processing, demonstrating strong potential for engineering implementation. Conclusion: Intelligent digital technologies provide a feasible pathway for achieving both privacy protection and business innovation in FinTech. The proposed framework and risk assessment system offer theoretical support and methodological guidance for building a secure, trustworthy, and sustainable data governance structure.

Keywords

Digital-Intelligent Technologies, FinTech, Privacy Protection Mechanisms, Privacy-Preserving Computing, Data Security Governance

1. 引言

金融科技的快速演进推动金融业务全面数字化、智能化，客户身份信息、交易轨迹与行为画像等多源数据被持续深度使用，成为风控与服务创新的重要驱动力。然而，数据规模爆发式增长与模型应用加速并行，使隐私泄露、算法滥用与越权访问等风险加速累积。与此同时，《数据安全法》《个人信息保护法》等监管要求不断提高合规标准，使隐私保护成为金融科技机构的基础工程。

在“数据可用不可见”“最小必要原则”等监管要求推动下，金融机构迫切需要构建可控、可审计、可验证的数据治理体系。本研究基于数智技术视角，提出面向全生命周期的数据隐私保护框架，系统分析差分隐私、联邦学习、区块链可信审计、多方安全计算等技术在金融场景中的适配性与协同性[1]，旨在为金融科技行业的安全治理提供理论支撑与技术路径。

2. 方法

本研究构建“文献–技术–场景–实验–评估”多维交叉的方法体系，通过多源证据链的综合验证，形成从理论推断到技术落地的连续性研究框架，确保研究结果具备可重复性与行业适配性[2]。

2.1. 文献梳理与理论分析法

依托 CNKI、Web of Science、IEEE Xplore、ACM Digital Library 等数据库，对隐私计算、数据安全

治理、算法监管与数据要素流通的相关研究进行系统化整理。重点提炼现有金融数据架构在集中存储、跨域共享与敏感数据处理方面的共性风险，梳理隐私增强技术的理论基础、适用边界与演进趋势，为后续模型构建与技术选择奠定理论基础。

2.2. 综合技术框架构建法

从数据生命周期的六大环节(采集、存储、传输、处理、使用、审计)出发，设计由多类隐私技术协同组成的分层式保护体系。差分隐私用于数据扰动与风险削弱；联邦学习负责跨机构建模；区块链及可信执行环境用于记录审计轨迹与保障执行可信；多方安全计算承担联合分析任务。本方法着重考察技术彼此之间的衔接方式、与业务流程的契合度以及在真实金融系统中的部署可行性。

2.3. 典型场景案例研究法

本研究选择支付、风控、信贷审批、身份认证等高频场景，逐一分析数据流转路径、敏感点分布及潜在攻击通道，并构建“场景问题－技术路径－效果呈现”的分析链接。结合头部机构与科技企业的实践案例，比较不同技术组合在适配性、性能、稳定性与可持续运行方面的表现，为技术体系的可行性提供应用层面证据。

2.4. 实验建模与对比验证法

建立传统集中式建模方案与隐私增强建模方案的对照实验体系，以典型行业数据结构为基础开展建模测试。评价维度包括模型精度、训练效率、重识别难度、泄露概率、算力占用与通信负载等。通过横向比较不同算法，以及纵向替换关键隐私机制的方式，检验技术组合在性能与安全性上的协同增益[3]。

2.5. 隐私风险评估模型法

构建由敏感性、可识别度、攻击面范围、可控性、审计能力与合规性六要素构成的风险评估框架，用于量化不同技术方案在多种业务环境中的隐私保护水平。该体系兼容结构化、半结构化及跨机构协同数据，可用于指导机构进行技术选型与隐私治理策略制定。

2.6. 多方法交叉验证法

将理论分析、技术设计、案例研究、实验结果与风险度量进行交叉印证，形成“理论合理－技术可靠－场景适用－风险可控”的逻辑闭环。多方法互补提升了研究的稳健性和解释力，并增强结论在行业推广与政策应用中的有效性。

3. 结果

本研究通过构建的“文献－技术－场景－实验－评估”多维交叉验证体系，系统性地评估了数智技术在金融科技客户隐私保护中的综合效能。本节从模型性能、隐私保护强度、数据可控性与审计能力、跨机构协同应用四个核心维度，呈现分析性结果。

3.1. 模型性能与业务可用性分析

从模型性能视角来看，将传统集中式建模与联邦学习等隐私增强建模方式进行对比后可以发现，尽管隐私保护措施在一定程度上增加了计算与通信资源开销，但模型在核心性能指标上的表现仍保持在可用范围内。

联邦学习通过参数共享而非数据集中汇聚来完成建模，从机制上减少了数据在传输与汇总环节的暴露概率。其在训练周期中需要进行多轮参数同步，相比集中式训练在时间和算力需求上有所提升，但从

识别精度、稳定性和模型收敛趋势来看，与集中式模型相比并未表现出明显的性能劣势。

因此，隐私增强建模技术在“性能可接受”和“隐私保护可提升”之间实现了较好的权衡，为实际业务中推广隐私友好型模型提供了可行性基础。

3.2. 隐私保护效果分析

在隐私保护强度方面，各类数智技术在不同处理环节发挥互补作用：

(1) 差分隐私通过向查询结果或模型参数中注入随机干扰，使得外部攻击者难以从输出中反推个体信息，从而显著降低重识别风险[4]。

(2) 联邦学习通过“数据本地化”的训练机制，使原始数据无需在机构间流动，有效降低因集中存储、跨域传输而产生的隐私暴露面。

(3) 多方安全计算基于密码协议实现多方协同运算，在各方均无法接触明文数据的条件下完成联合分析任务，对跨机构数据协同具有显著优势。

综合来看，这些技术从“数据最小化”“过程可控”“结果难推断”等多个层面共同增强了隐私保护能力，使隐私风险呈现出从集中暴露转向分散、可控且难利用的趋势，从而在整体上降低了隐私泄露或越权使用的可能性。

3.3. 数据可控性与审计能力分析

在数据可控性和可审计性方面，引入区块链等技术后，数据访问和使用行为得以实现更加完整、透明和不可篡改的记录。相比传统审计依赖中心化日志，对审计主体或系统信任度要求较高，基于链式结构的审计模式通过分布式存储、链上共识等机制，使审计记录更具完整性和公信力。

该机制在两方面表现突出：

(1) 访问过程可追溯性增强，每次数据调用均能实现行为留痕，方便事后核查；

(2) 篡改与伪造难度显著提升，减少了因记录被人为修改而导致的监管盲区。

在金融科技业务中，这类可追溯与防篡改特性能够加强内部控制体系，满足监管对透明度、合规性、准确留痕等方面的要求，有助于构建一个“可记录、可验证、可追责”的数据治理框架。

3.4. 跨机构协同应用效果分析

在跨机构场景下，多方安全计算和联邦学习等技术为解决“数据孤岛”问题提供了新的技术路径，使得不同机构能够在保证数据不出本地的条件下实现联合建模和风险信息共享。

从应用趋势来看：

(1) 联合建模往往能够捕捉到单一机构数据中难以发现的风险特征，增强风险识别的全面性；

(2) 参与机构无需暴露原始数据即可获得提升风控能力的协同收益，有助于推动行业合作；

(3) 在实际工程中，这类机制对算力资源、网络环境以及协议执行成本提出了更高要求，因此更加适合用于高敏感性、高风险业务场景，如联合反欺诈、跨机构授信审批等。

总体而言，跨机构隐私计算技术为数据共享和风险联防联控提供了可行路径，但其运行成本、协议复杂度和工程化挑战也提示行业需要在“安全收益”与“资源投入”之间进行合理权衡。

综上，数智技术在隐私保护、模型性能保持、数据可控性强化以及跨机构协同方面均呈现出积极效果，证明综合隐私保护框架在理论逻辑和场景适应性上具有可行性。虽然本研究未引入真实业务数据进行量化验证，但从技术特性与趋势分析角度，已展示出多类隐私保护技术协同应用的潜力与价值。随着未来获得更多真实数据与业务场景，本研究的趋势性结论将进一步得到实证支撑，为隐私保护机制从方法论走向工程实践奠定基础。

4. 讨论

本节基于前述技术分析与结果，围绕数智技术在金融科技客户隐私保护中的应用，从理论贡献、技术挑战、制度启示、落地条件与潜在风险五个方面展开系统讨论，以期构建可推广、可验证、可监管的隐私治理框架。

4.1. 理论贡献

本研究构建的综合隐私保护框架为金融数据治理提供了新的理论视角，主要体现在三方面：

(1) 推动隐私治理由集中式向分布式协同转型。通过联邦学习、多方安全计算等“数据不出域”机制，将传统依赖中心化权限管控的模式转向强调数据可用性与协同分析的新范式。

(2) 形成数据全生命周期的系统化治理逻辑。将采集、存储、传输、处理、使用与审计纳入统一结构，明确风险链条与技术匹配关系，弥补了传统隐私保护碎片化的问题。

(3) 构建技术与制度并行的治理路径。差分隐私与最小必要原则、联邦学习与数据本地化要求、区块链与监管科技在可审计性上的契合，为形成可监管、可验证的金融隐私治理体系提供双重支撑。

4.2. 技术应用的现实挑战与边界条件

数智技术在实验和典型场景中表现出较强潜力，但在工程化落地时仍存在多方面限制。

(1) 隐私保护与业务性能的平衡难题仍未完全解决。

差分隐私可能影响模型精度，多方安全计算与联邦学习带来额外计算与通信成本。随着隐私强度提升，资源消耗显著增加，机构需在“安全–性能–成本”之间寻求可接受的均衡点[5]。

(2) 跨机构协同缺乏统一标准。

不同机构在数据结构、接口协议、模型框架等方面差异较大，导致隐私计算在联合建模中可兼容性不足。缺乏统一标准体系限制了技术的可扩展性和行业级大规模部署能力。

(3) 隐私增强技术的可解释性不足。

在风控、授信等高敏感业务中，可解释性是监管核心关注点，而隐私机制可能弱化模型透明度，增加审计难度，也可能影响用户对自动化决策的接受度。

4.3. 政策与监管视角下的制度启示

在《数据安全法》《个人信息保护法》等监管框架下，金融机构需要构建更具前瞻性的隐私治理体系。本研究提出以下制度启示。

(1) 构建以技术为基础的合规体系。

应将差分隐私、链式审计、模型可验证性等能力内嵌到数据处理流程中，使合规从“人工检查”走向“技术内生”，提升监管适应性与效率。

(2) 推动行业级隐私计算基础设施建设。

金融机构可共同构建跨机构隐私计算平台，实现联合反欺诈、联合风控与信用信息共享，在确保数据不出域的前提下提升行业协同能力，形成数据流通的基础设施。

(3) 完善标准体系与监管协调机制。

应建立隐私计算技术接口规范、数据标签标准、模型审计规则等制度，使技术应用具备可监管边界，减少机构因不确定性带来的合规成本。

4.4. 行业落地的关键影响因素

数智技术能否在金融场景中真正落地，取决于以下因素。

(1) 组织治理成熟度。

隐私保护方案往往需要数据治理体系、权限管理体系和专业技术团队的支撑。治理体系越成熟，技术部署与维护越容易。

(2) 算力资源与投入能力。

多方安全计算、区块链审计、联邦学习等技术需要一定算力与设备成本，中小机构可能因此面临资源不足的问题，影响推广范围。

(3) 用户体验与信任构建。

隐私机制可能改变分析流程或降低部分业务的响应速度，需通过清晰告知、可解释反馈和流程透明度提升用户信任，避免隐私保护反向影响业务体验。

4.5. 数智技术应用的潜在风险

尽管数智技术在隐私保护中具有重要价值，但仍存在若干潜在风险需持续管理。

(1) 算法偏差可能被隐私机制掩盖。

隐私增强可能降低模型可调试性，使偏差来源难以识别，进而影响风控准确性和公平性。

(2) 攻击方式持续演化。

模型反演、成员推断、投毒攻击等威胁仍可能发生，隐私保护机制需要动态迭代与持续监测。

(3) 协同计算中的恶意节点风险。

在联邦学习中，单个节点的恶意参与可能破坏整体模型，需要结合可信执行环境、节点信誉评估等机制增强系统鲁棒性。

5. 结论与展望

5.1. 结论

本研究以金融科技领域的数据安全需求为背景，构建了一套数智技术驱动的综合隐私保护框架，系统整合差分隐私、联邦学习、多方安全计算、可信执行环境与区块链审计等多类隐私增强技术，形成可组合、可迁移、可工程化的技术体系。研究结果表明：

(1) 跨技术协同可显著提升隐私保护强度，在降低重识别风险的同时保持较高的模型性能；

(2) 分布式协同机制能够突破传统集中式数据汇聚模式的限制，提高跨机构数据合作能力，降低数据泄露概率；

(3) 可信审计与可控共享机制为金融机构在数据生命周期管理中提供了可验证、可追溯的治理手段，有助于强化合规性；

(4) 技术框架在典型业务场景中的实验验证显示，其在安全性、可控性与可审计性方面具有较强优势。

总体而言，本研究为金融科技隐私治理的理论构建与工程实践提供了可操作、可推广的解决思路。

5.2. 展望

尽管研究已取得阶段性成果，但未来仍需从更深层次的制度、技术与场景融合角度推进发展：

(1) 构建场景化定制的隐私保护组合。不同金融业务的数据结构、风险偏好与合规压力差异显著，亟需形成可按需组装的“模块化隐私框架”。

(2) 提升隐私计算的工程化能力。当前系统在算力需求、跨平台适配性与低延迟响应方面仍存在限制，未来应加强编译优化、协议压缩与硬件加速。

(3) 形成动态化与智能化的隐私风险评估体系。在复杂业务环境中，风险具有动态演化特征，需要结

合机器学习持续监测攻击面变化，构建可实时预警的评估工具。

(4) 推动行业级标准体系与跨机构协同机制建设。统一的数据接口、模型格式、审计标准和可信协作协议将成为大规模部署的必要条件。

(5) 深化隐私技术与监管科技(RegTech)的融合。通过技术可解释性提升、策略自动验证与合规证明系统，加强对算法的可监管性。

(6) 聚焦伦理治理与用户信任构建。用户对金融数据使用的信任是技术落地的重要基础，未来研究需兼顾透明度、知情权与长期伦理风险。

5.3. 小结

数智技术的演进正推动金融数据治理从“集中式管理”向“分布式协同治理”转型。隐私增强技术不仅提供了新的安全基础设施，也为跨机构合作、个性化服务与数据要素流通提供了重要支撑。本研究提出的综合框架、验证体系与制度化建议，可为金融机构构建可审计、可控化、可持续的数据隐私治理体系提供方法论支撑，并为未来的行业实践与政策制定提供参考方向。

基金项目

项目编号：JY202414；名称：数智技术在金融科技客户隐私保护中的应用研究；项目来源：2024 年度河北金融学院科研基金项目。

参考文献

[1] 张静波. 数字货币与区块链技术在金融交易中的应用研究[J]. 对外经贸, 2024(9): 46-49.

[2] 倪武帆, 周泯均, 乐冉, 等. 基于区块链金融的商业银行数字化转型对策探讨[J]. 科技与金融, 2021(Z1): 67-73.

[3] 周柄泽. 面向数据隐私保护的联邦学习技术研究[D]: [硕士学位论文]. 济南: 齐鲁工业大学, 2024.

[4] 程宁. 人工智能打造优质客户体验兼顾尊重隐私[J]. 中国自动识别技术, 2024(2): 33-34.

[5] 刘忠慧. P 公司的大数据隐私泄露风险管理对策研究[D]: [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2021.