软件学报 ISSN 1000-9825, CODEN RUXUEW
2026,37(6):2607−2646 [doi: 10.13328/j.cnki.jos.007642] [CSTR: 32375.14.jos.007642]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

安全可信的数据要素流通综述*

陈毅飞[1], 李 萌[1], 乔 焰[1], 汪 青[1], 张子剑[2], 祝烈煌[2]

[1](合肥工业大学 计算机与信息学院, 安徽 合肥 230601)

[2](北京理工大学 网络空间安全学院, 北京 100081)

通信作者: 李萌, E-mail: mengli@hfut.edu.cn; 张子剑, E-mail: zhangzijian@bit.edu.cn

摘 要: 随着数字经济的快速发展, 数据作为重要的生产要素, 在推动新质生产力和经济社会高效运转中发挥了核心作用. 数据要素的高效利用及其在不同主体间的有序、安全、合规流通对于数据要素价值释放具有重要意义. 然而, 数据流通过程中面临显著的安全隐患与可信挑战, 如泄露、篡改以及不可用等问题, 同时数据真实性和流通透明性要求也愈发重要. 为应对这些问题, 密码学、区块链、可信执行环境等技术被广泛应用, 但仍存在成本高、灵活性不足等限制, 且当前研究多集中于特定阶段, 缺乏系统性视角. 为此, 以数据要素全生命周期为主线, 构建了包含数据采集、传输、存储、处理、发布、溯源这 6 大阶段的分析框架, 系统性分析其安全与可信挑战. 提炼出安全技术“三线分化、协同融合”和可信技术“验证深度递进”两大演进模型. 旨在为该领域的关键问题提供体系化的解决思路, 并对未来研究方向提出展望.

关键词: 数据要素; 数据流通; 数据真实性; 安全; 可信

中图法分类号: TP311

中文引用格式: 陈毅飞, 李萌, 乔焰, 汪青, 张子剑, 祝烈煌. 安全可信的数据要素流通综述. 软件学报, 2026, 37(6): 2607–2646. http://www.jos.org.cn/1000-9825/7642.htm

英文引用格式: Chen YF, Li M, Qiao Y, Wang Q, Zhang ZJ, Zhu LH. Survey on Secure and Trustworthy Data Factor Circulation. Ruan Jian Xue Bao/Journal of Software, 2026, 37(6): 2607–2646 (in Chinese). http://www.jos.org.cn/1000-9825/7642.htm

Survey on Secure and Trustworthy Data Factor Circulation

CHEN Yi-Fei[1], LI Meng[1], QIAO Yan[1], WANG Qing[1], ZHANG Zi-Jian[2], ZHU Lie-Huang[2]

[1](School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230601, China)

[2](School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China)

Abstract: With the rapid development of the digital economy, data, as an important productive factor, plays a central role in fostering new forms of productive forces and ensuring the efficient functioning of the economy and society. The efficient utilization of data as a production factor, along with its orderly, secure, and compliant circulation among various entities, is essential to realizing its full value. However, data circulation is confronted with significant security risks and trust-related challenges, including leakage, tampering, and unavailability. At the same time, the requirements for data authenticity and circulation transparency are becoming increasingly important. To address these issues, technologies such as cryptography, blockchain, and trusted execution environments are widely applied. However, these technologies still face limitations such as high costs and insufficient flexibility, and current research often focuses on specific stages, lacking a holistic perspective. Therefore, this study is structured around the full life cycle of data factors, develops an analytical framework comprising six stages: data collection, data transmission, data storage, data processing, data publication, and data traceability, and systematically analyzes the security and trust-related challenges at each stage. For the first time, this study explicitly proposes two evolutionary models: the “three-line differentiation and collaborative integration” model for security technologies and the “verification-depth

* 基金项目: 国家自然科学基金区域创新发展联合基金 (U23A20303); 国家自然科学基金面上项目 (62372149, 62572168); 国家留学基金委访问学者项目 (202406690030); 安徽省自然科学基金面上项目 (2508085MF151); 中文大数据知识工程教育部重点实验室开放课题 (BigKEOpen2025-04); 网络与交换技术全国重点实验室 (北京邮电大学) 开放课题 (SKLNST-2025-1-12)
收稿时间: 2025-08-26; 修改时间: 2025-11-25; 采用时间: 2026-01-25; jos 在线出版时间: 2026-04-01
CNKI 网络首发时间: 2026-04-02

progression” model for trustworthy technologies. This study aims to offer systematic solutions to key issues in this field and outline directions for future research.

Key words: data factor; data circulation; data authenticity; security; trustworthy

数字经济时代, 数据已成为关键的生产要素. 数据要素是指投入生产经营活动、参与价值创造的数据资源[1], 其高效流通是推动新质生产力发展的核心驱动力. 然而, 数据流通过程中的安全与可信问题, 正成为制约其价值释放的瓶颈, 并引起了学术界与产业界的广泛关注.

安全问题贯穿数据要素的全生命周期. 在数据采集、传输和存储阶段, 数据面临泄露与篡改等威胁; 在数据处理阶段, 复杂操作可能导致数据被泄露或篡改, 进而影响其可靠性与后续使用[2]; 在数据发布阶段, 存在未授权访问和隐私泄露的风险. 此外, 数据溯源机制是保障数据可信、实现追责的关键, 该机制既可能缺失或遭攻击, 例如, 2017 年的 Equifax 数据泄露事件便凸显出这一问题[3], 也可能因元数据敏感而本身带来泄露风险. 而数据要素流通的可信本质上是对数据真实性的要求, 贯穿于上述所有阶段.

为了应对这些挑战, 密码学、身份认证、区块链和可信执行环境 (trusted execution environment, TEE) 等技术虽被广泛应用, 但仍面临成本高、开销大、管理灵活性不足及隐私保护冲突等局限. 当前研究多聚焦于提供单一环节的解决方案, 缺乏对全生命周期的系统性分析.

近年来, 学术界已对数据流通中的安全可信问题给予了广泛关注, 并涌现出一批高质量的综述性研究. 如表 1 所示, 这些研究大致可分为如下 4 类.

表 1　本文与其他综述文献的对比

文献	综述视角	涵盖范围	覆盖方式	侧重点	主要特点
[4]	特定技术 (隐私计算)	技术发展历程、应用挑战	纵向追踪	主要关注安全与隐私	系统梳理隐私计算技术发展
[5]	特定技术 (区块链流通)	存储模型、性能、跨链、溯源	纵向追踪	偏重可信, 安全涉及较少	聚焦区块链在数据流通中的应用
[6]	特定技术 (区块链安全服务)	机密性、完整性、认证、删除	纵向追踪	聚焦安全需求	从区块链视角总结数据安全服务
[7]	特定技术 (联邦学习)	安全、鲁棒性、隐私保护	纵向追踪	聚焦可信与隐私	梳理可信联邦学习的威胁与防御
[8]	特定环节 (数据采集)	包级、流级、连接级、主机级方法	纵向追踪	主要涉及安全	系统分析采集环节的安全挑战
[9]	特定环节 (外包计算)	数据机密性与计算完整性	纵向追踪	聚焦安全	总结云外包中的安全方案与挑战
[10]	应用场景 (智能汽车)	制度、场景、问题与建议	横向覆盖	安全与可信并行	面向应用的系统性综述
[11]	应用场景 (物联网)	IoT架构与生命周期问题	横向覆盖	安全为主, 可信涉及较少	多维分析物联网数据安全挑战
[12]	系统性视角	数据流通全过程 (前、中、后3阶段)	横纵向结合	聚焦隐私保护	梳理隐私风险, 聚焦隐私保护技术
本文	系统性视角	数据要素流通全生命周期	横纵向结合	安全与可信并行	提出6阶段分析框架与演进模型

● 聚焦特定技术的综述. 李建华等人[4]全面回顾了大数据安全与隐私计算的发展历程、技术路线与应用挑战; 钟子岳等人[5]总结了区块链在存储、性能扩展、数据验证、跨链与溯源等方面的进展; 王利朋等人[6]综述了区块链支持的数据安全服务, 涵盖机密性、完整性、身份认证、隐私与可信删除等需求; Zhang 等人[7]系统梳理了可信联邦学习的安全、鲁棒性与隐私保护问题及应对方法. 这些研究为理解单一技术提供了基础支撑.

● 聚焦特定环节的综述. Jing 等人[8]对互联网安全威胁检测与测量中的数据采集与分析方法进行梳理、分类并总结其优缺点, 然后探讨了典型攻击检测与未来方向; Shan 等人[9]关注云计算环境下的数据与计算外包, 总结了保障机密性与完整性的多类方案, 并提出后续挑战. 这类研究有助于加深对特定环节的理解.

● 面向应用场景的综述. 洪启安等人[10]以智能网联汽车为例, 从价值场景出发分析制度适用性, 识别我国数据流通中的问题并提出建议; Hou 等人[11]从数据视角梳理物联网安全, 结合典型架构与数据生命周期, 构建多维度分析框架, 并探讨采集、传输与应用中的安全挑战. 这类研究凸显了数据流通安全与可信在具体应用领域的独特挑战与发展机遇.

● 面向全流程的系统性综述. 刘立伟等人[12]将数据流通划分为前、中、后这 3 个阶段, 系统地梳理了数据最小化、忘却学习等隐私技术, 重点探讨流通中的隐私保护机制.

尽管已有综述取得了丰富成果, 但仍存在一个明显的空白, 即缺乏将数据要素流通视为完整、动态过程的宏观视角. 主要问题体现在 3 个方面: 一是阶段划分与覆盖面局限, 现有研究或仅关注单一技术与环节, 或阶段划分较为宏观 (如仅划分为前、中、后), 未能系统性地贯通数据采集、传输、存储、处理、发布与溯源这 6 大阶段; 二是体系缺失, 尚无研究在统一框架下综合探讨安全与可信这两大核心问题, 而它们在实践中往往紧密耦合、相互影响; 三是缺乏顶层模型, 现有工作多停留于技术细节梳理, 未能抽象出领域发展的宏观演进规律与核心矛盾, 从而难以形成对未来研究的体系化指引.

因此, 本文旨在全面综述数据要素流通中的安全与可信研究, 系统梳理并评价现有方案, 揭示其局限性, 并提出未来研究方向, 为构建一体化的数据要素流通安全可信体系提供参考.

本文的核心贡献主要体现在 3 个方面: 首先, 提出一个更契合数据要素流通特性的 6 阶段生命周期分析框架; 其次, 基于该框架系统性地构建了安全与可信两大维度下的数据要素流通技术图谱; 最后, 提出“三线分化、协同融合”的安全演进模型与“验证深度递进”的可信演进模型, 为理解该领域的发展与趋势提供了新的视角. 全文的分析以 3 大核心矛盾为主线展开, 中心化管控与去中心化信任的博弈, 影响了技术方案的信任根基与架构形态; 安全强度与系统性能的权衡, 揭示了理论完备性与工程实用性的取舍; 静态防护与动态保障的演进, 反映了安全理念从被动防御向主动治理的深刻转变.

本文的文献覆盖多种来源的研究成果, 如图 1 所示, 技术类参考文献的主要来源为期刊、会议以及技术文档. 其中, 期刊论文占比为 58.7%; 会议论文占比为 33.3%. 此外, 在被统计的论文中, 55.1% 为 CCF A 类推荐论文, 其中包括 USENIX Security、NDSS、CCS、S&P、TDSC 以及 TIFS 网络与信息安全领域的顶级会议和期刊, 3.6% 为 CCF B 类推荐论文, 其余为 CCF C 类推荐论文以及其他论文.

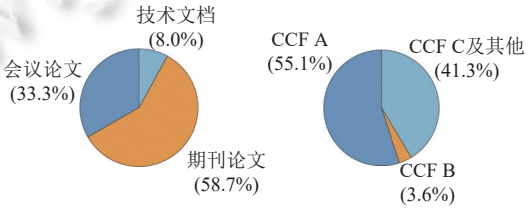

图 1 文献来源及发表等级统计

本文首先系统性地介绍数据要素流通的概念与模式. 接着, 提出一种覆盖数据采集、传输、存储、处理、发布与溯源这 6 大阶段的全生命周期划分方式, 并以此为基础, 分析各阶段面临的安全与可信挑战. 在分析过程中, 本文对现有解决方案的核心思路、局限性与挑战进行对比和评价. 在此基础上, 对前述分析进行系统归纳与提炼, 构建出数据要素流通安全与可信的技术发展路线, 并对未来研究方向进行展望.

1 数据要素流通的概念与模式

数据作为重要生产要素, 其流通可被界定为在多主体、多场景中贯穿全生命周期以实现价值的动态过程, 对经济增长具有重要意义. 然而, 当前实践中的安全与可信问题严重制约了数据价值的释放. 针对这一问题, 国家标准《信息安全技术 数据安全能力成熟度模型》(GB/T 37988—2019) 将数据生命周期划分为采集、传输、存储、处理、交换及销毁这 6 个阶段[13], 为数据安全体系构建提供了重要参考. 但该模型主要面向静态能力评估, 难以完全覆盖数据要素在多方协作、跨域共享的动态流通过程中面临的全链路挑战. 为此, 本文结合数据要素流通的现实特征, 在该标准的基础上, 提出一种更贴合数据要素流通的生命周期划分方式, 包含数据采集、传输、存储、处理、发布与溯源这 6 个阶段, 为系统性地分析数据要素流通中的安全与可信挑战提供了更完备的框架. 该框架的主要改进如下.

1) 将数据发布独立为一大阶段, 即明确区分数据发布的技术过程与数据发布的价值实现过程, 更精准地刻画数据作为生产要素向社会提供服务的关键环节.

2) 将数据溯源提升为关键阶段, 即强调溯源不仅是事后追责的技术手段, 更是贯穿始终、保障全链路可信的基石, 是解决多主体协作信任问题的核心.

1.1 数据要素流通的特点

● 多场景. 数据要素因其可塑性与可移植性, 被广泛应用于工业、金融等多元化场景. 然而, 不同场景对数据敏感度、合规性及保护机制的要求各异 (如医疗重隐私, 金融重追溯), 导致统一的安全治理体系难以建立.

● 多主体. 数据要素流通涉及数据提供方、使用方、平台方和监管机构等多个角色, 构成一个主体间高度依赖但耦合松散的生态. 各方在权限、责任和利益分配上的认知差异, 易导致信任链断裂, 引发数据越权使用或泄露后责任不清等问题.

● 动态性. 数据在格式、内容和应用环境 (跨平台、跨组织) 上不断变化, 呈现高度动态性. 传统的静态边界防护 (如端到端加密) 难以应对这种动态特征, 导致在处理等阶段可能出现安全盲区.

● 价值驱动. 数据的增值与可复用性是其流通的核心驱动力, 催生了数据市场和平台经济. 但高价值也放大了攻击收益预期, 催生了数据投毒、模型污染等新型攻击, 并加剧了数据篡改、非法变现等风险.

1.2 数据要素流通模式

在数据要素成为重要生产要素以及云计算、大数据等信息技术不断发展的背景下, 数据要素流通的方式逐步多样化. 根据不同的参与主体、技术手段和流通方式, 主流模式可分为以下 4 类. 表 2 总结了不同流通模式在组织形态、激励机制和安全需求上的显著差异.

表 2 典型数据要素流通模式

流通模式	优势	局限	典型应用场景	主要挑战
组织内部流通	数据归属清晰, 治理集中, 整合效率高	缺乏激励, 跨域协作难, 易形成内部孤岛	企业集团内部、政府机关等	部门壁垒、权限管理复杂、内部滥用风险
数据交易	激励机制强, 促进数据资产化	数据质量难评估, 交易可信度不高, 追责机制薄弱	数据市场、第三方平台等	合规风险高、隐私泄露风险、监管缺失
数据共享	降本增效, 促进协同合作	授权控制难, 隐私保护不足, 信任关系难建立	公共服务、行业协同 (如医疗、交通)	共享意愿不足、责任边界模糊、安全机制不完善
数据跨境	推动全球协同, 促进国际数据价值释放	法规冲突大, 合规成本高, 技术体系差异显著	跨国企业、国际平台、数据出海	组织形态复杂, 合规、跨国监管难, 责任追溯困难

● 组织内部流通. 该模式旨在通过内部数据共享提升运营效率与决策支持, 数据中台是其典型实践, 例如 Lyu 等人[14]基于微服务架构构建电网数据中台, 解决了数据隔离与重复开发问题, 提高了开发与迭代效率; 李炳森等人[15]设计了具有贴源、共享、分析这 3 层服务架构的数据中台, 支撑内部决策分析与外部需求响应; Liu 等人[16]整合多源异构数据, 构建可扩展的数据服务平台, 规范化管理数据资源并推动其增值. 实践表明, 组织内部模式通过优化数据要素流通机制, 为数字化转型与高效运营提供了重要支撑. 此模式下组织边界清晰, 但存在由激励不足、跨部门协同难所导致的数据孤岛问题.

● 数据交易. 该模式通过市场机制匹配供需, 是数据资产化的重要途径. 去中心化平台近年来受到广泛关注, 例如, Lu 等人[17]构建了基于区块链的物联网数据交易系统, 该系统使企业能够通过购买数据提升服务质量, 同时帮助数据所有者实现数据变现. Hu 等人[18]基于智能合约完善数据质量评估与收益分配机制, 以提升交易公平性. 该模式激励明确, 但对交易过程的合规透明及使用后的责任追溯提出了更高要求.

● 数据共享. 该模式旨在打破数据孤岛, 常以无偿或低成本方式进行. 为解决隐私保护、共享效率和用户自主性问题, 研究者提出了多种技术方案. Lyu 等人[19]基于数据胶囊范式的系统赋予个人数据共享自主权, 数据所有者可完全掌控数据共享. Lu 等人[20]利用联邦学习和区块链架构提升车联网数据共享的隐私性与效率, 促进车辆数据协作和服务优化. Chatziantoniou 等人[21]采用基于图的概念模型数据虚拟机, 简化数据操作流程, 提升数据共享的

灵活性和易用性, 即便非 IT 人员也能便捷地参与数据处理. 该模式的关键挑战在于共享意愿不足、责任划分不清以及多主体间合规与技术能力的差异.

● 数据跨境. 该模式旨在平衡数据自由流动与合规监管, 以促进全球数据资源协同. 目前研究主要聚焦于法律法规层面, 技术保障仍处于起步阶段. Peng 等人[22]提出基于区块链的框架, 简化合规流程, 构建安全透明的全球数据共享平台. Rahman 等人[23]提出了一个基于区块链的跨境数据共享平台, 通过安全网关和多层签名机制实现数据共享的可追责性, 设计了不当行为的检测和处罚算法. 其主要挑战在于组织形态复杂、合规壁垒高, 对全链条的安全可信机制提出了更高要求.

综上, 不同流通模式在组织形态、激励机制和安全需求上差异显著. 组织内部流通聚焦于数据采集到数据处理阶段的协同, 数据交易与共享则更强调发布与溯源机制, 而跨境流通则对全生命周期的安全可信提出了最高要求, 这凸显了构建系统性安全可信保障体系的必要性.

2 数据要素流通阶段

数据要素流通的安全性和可信性是制约其高效利用与价值释放的关键因素. 为便于系统性分析安全与可信挑战, 如图 2 所示, 本文将数据要素流通划分为以下 6 个阶段.

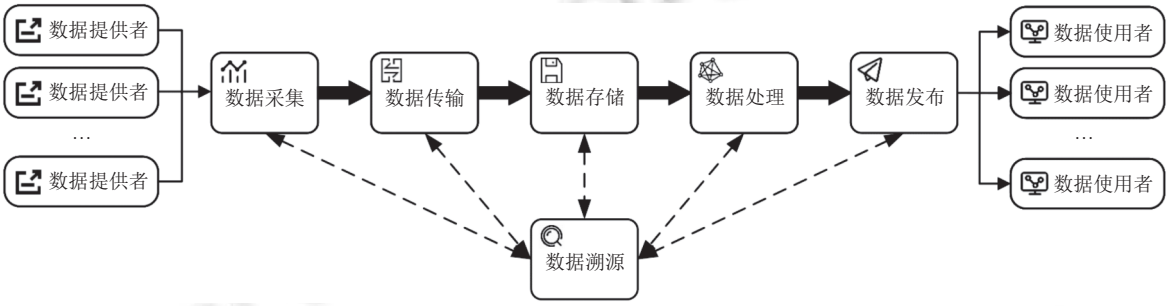

图 2 数据要素流通阶段

● 数据采集. 作为流通起点, 此阶段通过传感器、API 接口、网络爬虫或人工录入等方式获取多源异构数据, 其核心目标是确保原始数据的准确性与真实性.

● 数据传输. 此阶段负责将数据从源头传递至存储或处理系统, 主要通过有线或无线网络实现, 其关键在于保障数据流动的高效、稳定与安全.

● 数据存储. 此阶段负责数据的集中管理与长期保存, 主要形式包括本地、云及分布式存储, 其核心目标是实现大规模异构数据的高效、安全存取.

● 数据处理. 作为价值实现的核心环节, 此阶段通过清洗、转换、分析及建模等操作, 从原始数据中提取潜在价值, 其效果直接决定了数据的最终应用成效.

● 数据发布. 此阶段面向数据使用者, 通过 API 接口、可视化报表或数据集下载等形式, 实现数据的定向或公开发布. 其重点在于确保数据能被高效、合规地访问与利用.

● 数据溯源. 此阶段贯穿整个生命周期, 通过记录数据的来源、流转路径及变更历史, 实现全流程的可追溯. 其目标是为数据质量管理、责任界定及合规审计提供技术支撑. 需要注意的是, 虽然传输、存储等阶段也会使用局部审计机制提升安全可信性, 但这些机制仅用于阶段内部的局部验证, 不构成独立的溯源能力. 本文所定义的溯源阶段指面向跨主体、跨系统、跨阶段的全链路追踪, 用于重建数据路径并实现责任界定.

综上, 数据从产生到价值释放需经历数据采集、传输、存储、处理、发布与溯源这 6 个阶段, 环环相扣, 风险也随之累积与扩散. 例如, 数据采集质量影响后续利用价值, 数据传输与存储关乎数据安全, 而数据发布与溯源则直接决定可信度与责任归属. 每个阶段都面临独特的安全与可信挑战, 例如数据采集阶段的来源验证问题、数据传输与存储阶段的数据泄露与篡改风险、数据处理与发布阶段的越权滥用隐患, 以及数据溯源阶段可能存在的机

制缺失与责任不清. 不同的流通模式对各阶段的安全与可信需求存在显著差异. 例如, 组织内部流通模式更关注数据处理阶段的权限控制与防泄露; 数据交易模式则高度依赖数据发布阶段的质量证明与数据溯源阶段的血缘验证; 而数据跨境模式对数据传输阶段的合规性与数据存储的本地化要求严格.

为更好地厘清海量技术方案的发展脉络, 本文基于对现有研究的归纳, 提炼出如下两大核心演进模型, 作为技术分析的理论框架, 并在第 3、4 节分别对数据要素流通 6 大阶段的安全问题与可信问题展开详细剖析.

● 安全技术: “三线分化、协同融合”模型. 即安全技术从单一传统密码学基础防线, 逐步分化为应对数据动态计算的隐私增强路线、应对环境风险的硬件隔离路线及应对多方协作风险的分布式可追溯路线, 最终走向协同融合.

● 可信技术: “验证深度递进”模型. 即信任机制的构建呈现出从身份可验证 (你是谁), 深化到行为可验证 (行为是否合规), 最终达到数据内容可验证 (数据本身及其声明为真) 的层层递进规律.

3 数据要素流通安全问题

安全问题是制约数据要素高效流通与价值释放的核心挑战, 其风险贯穿于流通全过程 (如图 3 所示). 本节结合数据要素流通的 6 个阶段, 分析各阶段的主要安全挑战, 并探讨现有解决方案和待解决问题.

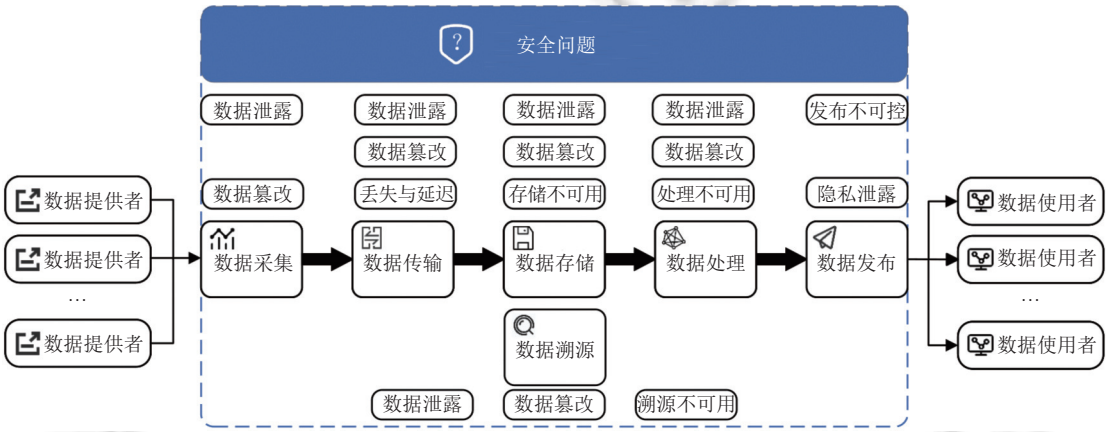

图 3 数据要素流通各阶段安全问题

3.1 数据采集阶段

数据采集作为流通起点, 其安全性直接决定了后续环节的可靠性与合法性. 此阶段面临数据泄露、篡改、伪造注入及账户冒用等威胁. 针对这些挑战, 现有研究主要沿硬件安全、密码学、身份认证与访问控制、系统架构安全及协议安全等路线展开, 但普遍存在成本、性能与安全性之间的权衡问题. 本节将围绕自动化设备采集、人工录入、第三方接口调用与网络爬虫这 3 类典型采集方式, 剖析其安全挑战、技术方案及局限.

3.1.1 自动化设备采集

自动化设备 (如物联网设备) 因成本敏感和功能优先的设计, 普遍存在安全机制薄弱的问题, 成为攻击者的主要目标, 易遭受蠕虫和病毒攻击[24]或窃听攻击[25]等威胁. 这一场景的关键挑战在于受限资源与安全需求之间的矛盾, 推动了两条主要技术路线的发展.

针对设备安全机制等问题, 以可信执行环境 (TEE) 为代表的硬件安全路线呈现出场景驱动特征. 例如, Guan 等人[26]利用 TrustZone 为物联网应用构建可信执行环境, 即使操作系统遭受攻击, 关键安全应用仍能在隔离环境中安全运行. 然而, 其局限性在于依赖特定硬件支持, 具有较高的使用成本.

这一局限性推动了软件 TEE 的发展, Han 等人[27]提出了一种无需 TrustZone 的可信执行环境, 采用内核降权和精确内存管理等技术, 在软件层面实现隔离. 其主要优势在于不依赖专有硬件, 部署成本低, 适用于更多种类的嵌入式设备. 然而, 其隔离强度弱于硬件 TEE, 易受到内核及旁路攻击等威胁. 为适应资源更受限的端侧设备, 杜冬

冬等人[28]提出了基于段隔离机制的可信执行环境 SegTEE, 通过嵌套段隔离、段滑动窗口等技术有效提升隔离能力, 使得 TEE 方案可以适用于更小型、计算能力更有限的设备.

综合来看, 硬件安全路线主要围绕两个关键方向: 一是降低对专用硬件的依赖, 二是优化资源管理以适应资源受限场景. 然而, 在面对高强度攻击、动态威胁演化等复杂场景时, 现有方案仍存在一定局限, 需要进一步研究更为灵活、可扩展的安全机制. 密码学路线与硬件路线并行, 旨在从密码算法层面优化, 为资源受限设备提供低成本保护[29]. 然而, 其关键挑战在于平衡安全强度与资源消耗. 未来研究应聚焦于在保障安全性的前提下优化算法的效率与适应性.

3.1.2 人工录入

人工录入方式高度依赖用户行为与操作环境, 易受账户劫持、虚假身份冒充、环境伪造等攻击, 是数据泄露和篡改的高风险环节. 例如, 2020 年新冠疫情期间, 攻击者伪造信息并录入应用, 导致大量敏感数据泄露[30]. 其解决方案主要围绕身份认证和环境隔离两条路线.

身份认证路线旨在确认用户身份的合法性, 多因素身份验证 (multi-factor authentication, MFA) 和基于风险的身份验证 (risk-based authentication, RBA) 被广泛应用以提升用户账户安全性[31]. MFA 通过结合口令、生物识别和设备指纹等身份要素, 提升账户劫持难度. RBA 则根据用户行为特征 (如登录时间、IP、设备类型等) 动态调整认证策略, 增强系统主动防御能力. 然而, 这些方法在实践中存在局限, 复杂的验证流程可能影响用户体验, 而动态策略则面临高误判率和维护成本的问题. 该路线是安全的第 1 道防线, 正从静态向动态、多维演进, 但其根本局限在于无法解决录入环境本身的安全问题.

为应对环境安全威胁, 研究者提出了环境隔离路线. 例如, Song 等人[32]提出了一种基于容器沙箱的输入隔离机制, 将用户输入操作限制在受控环境中, 以阻断恶意代码对主系统的影响. 这一方案利用容器轻量级虚拟化特性, 在确保隔离效果的同时尽可能降低性能开销, 相较于传统虚拟机方案具有更好的可部署性, 代表了环境隔离路线的核心思路. 然而, 隔离机制依然会带来一定的资源消耗, 尤其在移动或嵌入式设备等资源受限场景下.

可以说, 环境隔离路线在另一个维度上解决了人工录入的安全问题, 其核心挑战在于如何以更低的性能代价实现更强的隔离效果, 这也是其未来发展的关键方向.

3.1.3 第三方接口调用与网络爬虫

第三方接口调用与网络爬虫等外部数据采集方式因依赖外部数据源, 容易受到恶意干扰. 例如, 攻击者可能伪造合法接口诱导系统采集错误数据, 通过中间人攻击窃取数据, 或通过分布式拒绝服务攻击破坏系统可用性. 这催生了宏观的系统架构优化与微观的协议安全增强两条技术路线.

在系统架构优化层面, 零信任模型提供了宏观防护思路, 其核心是摒弃传统边界信任并对每次访问都进行持续验证. 例如, Hong 等人[33]开发的零信任系统安全框架 SysFlow 通过可编程方式对系统活动进行动态安全控制, 实现对数据源的持续认证, 其优势在于跨系统、跨协议的灵活性, 适用于复杂场景下的接口保护需求. 然而, 由于其依赖持续行为监控与策略匹配, 在大规模部署时可能带来一定的性能负担.

综上, 零信任等系统架构路线提供了一种宏观的安全方法, 重塑安全与信任模型以实现普遍安全防护, 适用于异构复杂的系统环境. 但其根本挑战在于如何平衡高灵活性与大规模部署时可能带来的显著性能负担.

与之互补的是协议安全增强路线, 聚焦于加固具体通信协议以提供精准防护. 鉴于 HTTPS 在 API 调用中的主导地位, Karapanos 等人[34]提出了 SISCA 机制, 通过通道 ID 验证和服务器状态检查来抵御链路劫持和中间人攻击. 该方案精准高效, 但局限性也十分明显, 主要面向 HTTPS, 难以覆盖采用 HTTP、WebSocket、gRPC 等多种协议的异构采集环境.

总体来说, 协议安全路线代表了微观的防护策略, 对主流协议进行深度优化与增强, 是宏观架构的重要补充, 提供了针对性的解决方案, 但通用性不足.

3.1.4 小 结

数据采集阶段的安全方案始终在安全性、性能与成本之间权衡, 其技术演进呈现出多维趋势.

1) 硬件与软件演进. 在自动化设备场景, 安全技术正从依赖特定硬件的 TEE 向更普适的软件实现方案演进. 这一软硬路线的分野, 正是本文“三线分化”模型中硬件隔离路线与隐私增强路线在端侧设备上的早期体现.

2) 强度与性能的权衡. 无论是轻量化 TEE 还是轻量级密码学, 都体现了为适应资源受限场景而对强度与性能的持续优化.

3) 单点防护到协同防御. 如身份认证与环境隔离的结合, 以及宏观的零信任架构与微观协议增强的互补, 共同构成了纵深防御体系.

这些趋势表明, 数据采集阶段的安全技术正从静态、单一的防护向动态、多维的保障体系演进, 但也揭示了各技术路线在跨场景适用性和理论统一性上的不足, 为未来的融合创新指明了方向. 这也表明, 单一技术路线已难以满足需求, 不同路线间的协同融合已成为数据采集安全发展的必然方向.

3.2 数据传输阶段

数据传输阶段的安全性核心在于保障数据的机密性、完整性和可用性. 在传输过程中, 数据面临窃听、篡改、丢失或延迟等威胁, 尤其是在开放网络中, 可能导致敏感信息泄露或传输中断. 现有技术如流量加密、完整性验证和多路径传输等方案, 在复杂网络环境中仍面临计算开销高和适应性不足的问题. 本节将围绕传输数据窃听防护、传输数据完整性保护及传输可用性保障这 3 个方面展开讨论.

3.2.1 传输数据窃听防护

数据窃听是数据传输阶段最常见的威胁之一, 通常由不安全的协议或其实现漏洞引发. 为应对此问题, 主流方案是采用加密协议来实现端到端加密, 但其安全性在理论与实践层面均面临挑战.

在协议理论层面, 挑战源于其固有的复杂性与依赖. 例如, 传输层安全性 (transport layer security, TLS) 1.3 协议虽通过 0-RTT 等机制增强了安全性和效率[35], 但其对公钥基础设施 (public key infrastructure, PKI) 的依赖增加了系统的维护复杂性. 同时, 在资源受限环境中, TLS 的握手和加密开销可能导致显著的性能瓶颈.

在工程实践层面, 挑战则体现为实现的脆弱性. 例如, 著名的 Heartbleed 漏洞能够使攻击者窃听通过 TLS 传输的数据[36]. 为解决协议实现中的缺陷, Maehren 等人[37]提出了一种基于组合测试的测试工具 TLS-Anvil, 解决了 TLS 实现中的测试判定问题, 提高协议实现的正确性和可靠性. 形式化验证工具虽然能发现潜在的安全问题, 但仍然面临覆盖范围有限、学习门槛高、使用成本高等挑战, 限制了其大规模应用.

综上所述, 传输数据窃听防护矛盾从协议本身转移到了理论与实践的鸿沟. 协议理论日趋完善, 但在复杂依赖、资源限制和代码实现等工程环节中暴露出的脆弱性. 如何跨越这道鸿沟, 是未来研究需要关注的重点问题.

3.2.2 传输数据完整性保护

数据篡改是完整性面临的主要威胁, 攻击者可通过包注入、重放或中间人攻击等手段实现. 例如, 2015 年, Superfish 广告软件被发现在用户电脑中安装不安全根证书从而劫持用户流量[38]. 传统的数据完整性保护技术主要包括基于哈希函数的消息认证码 (message authentication code, MAC) 和基于非对称密钥体系的数字签名技术. 然而, 这些技术在实际应用中面临密钥管理复杂、计算性能瓶颈以及难以应对动态攻击等挑战. 为此, 近期研究沿着两条优化路径发展: 面向资源受限场景的轻量化以及面向未来威胁的抗量子化.

● 轻量化完整性验证路线, 旨在满足物联网等低功耗、低算力设备的需求. 例如, Rao 等人[39]通过定制 BLAKE2b 哈希算法并结合椭圆曲线数字签名, 在低功耗设备上实现高效的签名与验证. 此类方法的核心是在保证基本安全性的前提下, 尽可能压缩计算与通信开销, 重点在于关注安全与性能的平衡.

● 抗量子完整性验证路线, 旨在应对量子计算对传统密码体系的威胁. 为此, 研究者探索了基于后量子密码学的完整性验证技术. 例如 Ducas 等人[40]提出一种基于格的签名方案 Dilithium, 已被 NIST 纳入后量子密码标准化候选方案. 尽管其理论安全性高, 但较大的签名长度和计算复杂度仍是当前部署面临的工程难题.

这两条路线反映了当前研究的共性问题. 首先, 机制选择缺乏动态适应能力, 难以根据资源、网络或威胁变化进行调整. 其次, 缺乏统一评估标准, 不同方案难以系统对比. 未来应提升机制自适应性, 建立统一评估体系, 以增强实用性和可比性.

3.2.3 传输可用性保障

传输中断是可用性面临的主要威胁, 可由网络攻击或链路故障等引发. 例如, 2021 年 Fastly 导致全球大量网

站数据传输中断, 影响了多个企业级用户的业务[41]. 提升可用性的核心思路是引入冗余与调度机制, 通过构建备用或并行路径来规避单点故障.

并发多路径传输是该思想的典型实现, 例如, Zheng 等人[42]提出的基于流控制传输协议的并发多路径与负载均衡技术, 有效提升了传输的可靠性. 然而, 冗余与调度策略的根本挑战在于其必然引入的管理复杂性和额外开销, 这成为大规模部署的主要障碍.

可以说, 传输可用性保障的本质是在更高的可靠性与更低的系统开销之间进行权衡. 未来的研究方向在于设计更有效、更轻量化的调度机制, 以更低的成本实现更强的可用性保障, 特别是在大规模异构网络环境中.

3.2.4 小 结

本节围绕数据传输阶段的机密性、完整性和可用性展开分析. 可以发现, 与数据采集阶段类似, 其技术方案的演进同样需要在安全性、性能与成本之间寻求平衡, 但也具有独特的发展趋势.

无论是窃听防护中的协议实现问题、完整性保护中后量子算法高昂的部署成本, 还是可用性保障中冗余调度带来的管理开销, 都指向了同一个趋势, 即能否在复杂的现实环境中低成本、高性能、无差错地部署和维护这些方案, 成为重点关注对象.

从应用场景来看, 高强度的传输机密性与完整性保护技术, 对于解决数据跨境流通模式中长链路、跨域传输的安全合规问题具有显著的针对性优势.

总的来说, 数据传输阶段的安全防护需要在保障安全性的同时兼顾性能和成本, 未来应聚焦于提升技术方案的适应性和可部署性, 以应对复杂多变的网络环境和不断演进的安全威胁.

3.3 数据存储阶段

数据存储阶段的安全性取决于机密性、完整性和可用性, 旨在抵御因外部攻击或内部威胁导致的数据泄露、篡改或服务中断. 现有技术方案包括基于硬件安全模块 (hardware security module, HSM) 的加密存储、数据擦除技术、基于星际文件系统 (interplanetary file system, IPFS) 的完整性保护以及高可用存储架构. 然而, 这些方法在安全性与性能之间仍存在固有权衡. 本节将围绕存储数据泄露防护、存储数据篡改防护、存储可用性保障这 3 个核心安全属性, 剖析其挑战与解决方案.

3.3.1 存储数据泄露防护

数据泄露是数据存储阶段最主要的安全威胁, 常由系统配置错误或存储介质丢失引发. 例如, 2020 年, 微软因 ElasticSearch 服务器的安全配置错误, 导致 2.5 亿条客户服务数据泄露[43]. 为应对此威胁, 现有研究已形成覆盖硬件、算法和物理这 3 个层面的纵深防御体系.

● 在硬件层面, 主要通过硬件级别的加密和密钥管理机制提供保护. 例如, Dauterman 等人[44]提出的 SafetyPin 系统利用 HSM 集群分散信任, 即使部分硬件被攻破也能保障数据安全, 有效抵御暴力破解攻击. 该类方案安全性高, 但其硬件成本与集成复杂性限制了其广泛应用.

● 在算法层面, 核心在于运用密码学技术保障数据以密态形式存储, 同时确保数据在密态下能够被有效利用和服务. 相关研究发展具有鲜明的演进分支. 一方面, 研究者针对车联网等特定应用场景, 设计了隐私保护导航与查询方案[45–48], 通过升级传统查询机制来保护用户身份和位置隐私. 另一方面, 为了支持更通用的查询需求, 研究者们设计了支持近邻查询、动态更新、时间限制访问以及支持灵活通配符查询的通用安全方案[49–51]. 这些方案虽增强了安全性, 但其复杂的加密与索引结构带来了显著的计算开销, 限制了在资源受限环境下的应用. 针对复杂的图结构数据, Shen 等人[52]提出了支持最短路径模糊查询的图加密方案, 利用新型数据结构解决了查询中信息不精确的问题, 并在保证安全性的同时显著提升了响应效率.

● 在物理层面也存在独特安全威胁, 存储介质一旦丢失、被盗或转移, 便有被暴力破解或非法利用的风险. 例如, 2019 年日本神奈川县政府丢失含有个人信息的硬盘, 该硬盘被售卖[53]. 针对介质丢失问题, 数据销毁技术已成为关键应对措施. 目前, 国际标准 NIST SP 800-88r1[54]和国内技术规范 T/CAICI 80-2024[55]提供了关于物理介质安全销毁的具体指导, 包括覆盖法、填充法等多种实现方式. 但现有方法仍在稳定性和效率之间难以权衡, 如覆盖法

高效但不稳定, 而填充法稳定但低效[56].

总体来看, 当前数据存储的机密性保护已形成多层次防御体系, 但仍面临挑战. 首先, 机制碎片化, 不同技术路线缺乏统一的密态数据管理框架; 其次, 硬件依赖型方案部署成本高、门槛高; 此外, 加密与查询效率的矛盾尚未解决. 未来应构建统一的管理框架, 降低成本和性能开销.

3.3.2 存储数据篡改防护

数据篡改威胁着存储数据的完整性, 攻击者可通过植入恶意代码或利用硬件漏洞实现. 为此, 完整性保护机制正从外部校验向内部自证的模式演进 (如表 3 所示).

表 3 存储数据完整性保护模式

保护模式	核心思想	性能	优势	缺陷	适用场景
外部校验	数据与完整性证明分离, 依赖中心化服务进行校验	高, 校验过程与数据处理分离, 集中式管理	实现简单、与现有系统兼容、便于集中管理	需可信第三方, 校验和数据可被分离, 存在潜在篡改风险	传统IT系统、中心化业务场景
内部自证	完整性验证嵌入存储结构, 内容寻址、结构化哈希自证	低, 内容寻址与结构化哈希带来额外开销	数据与证明强绑定, 篡改可立即检测	检索效率较低、部署运维复杂、缺乏自动修复能力, 依赖网络	分布式存储、多方数据共享与交换场景

传统的外部校验模式依赖于独立于数据本身的校验机制, 如文件系统的校验[57]或数据库的 MAC[58]. 在这种模式下, 数据与其完整性证明分离, 需要可信的第三方执行和管理校验过程. 而 IPFS 开创了内部自证的新模式, 将完整性验证内嵌于存储结构本身[59]. 其核心机制为内容寻址与结构化哈希验证, 即数据在存储前会被哈希, 生成唯一的内容标识符 (content identifier, CID), 用户通过哈希值定位数据. 数据被拆分为若干块, 组织为默克尔有向无环图 (directed acyclic graph, DAG), 每个节点的哈希值依赖于其子节点, 最终形成可验证的数据结构. 从而实现数据内容与标识的强绑定, 任何微小篡改都会引起哈希值变化, 具备天然的篡改检测能力, 适用于多方协同的去中心化场景. 然而, 该模式也带来了新的挑战. 内容寻址在大规模数据检索时效率较低, 分布式特性也增加了部署与维护的复杂度, 且系统侧重于篡改检测而非数据恢复. 因此, IPFS 虽在完整性保障上有范式优势, 但仍需在性能、系统集成和恢复机制上进一步完善, 以支撑更广泛的数据流通需求.

3.3.3 存储可用性保障

数据存储系统的可用性是保障数据持续流通的基础. 一旦遭受攻击或故障, 数据将难以访问或恢复, 影响数据生命周期. 当前, 主流保障机制主要依靠冗余实现被动容错, 应对存储不可用问题.

董昊文等人[60]指出, 现有云原生数据库通过计算存储分离架构、多副本存储与一致性协议以及高效的故障恢复等技术实现高可用性, 确保即使部分节点失效仍能保证服务连续性, 这也是基于冗余的被动容错这一思想的典型实现, 其本质是通过创建多个副本确保在部分节点或组件失效后, 系统依然能够通过其他副本提供服务. 在具体策略优化方面, Liu 等人[61]针对故障恢复问题构建了一个非线性整数规划模型以在故障问题下最大化数据可用性, 从而降低复制产生的成本, 提高数据可用性并减少一致性维护和存储成本.

虽然上述机制提升了存储可用性, 但仍存在挑战. 一方面, 多副本机制虽具备容错能力, 但资源消耗和维护成本较高; 另一方面, 现有以被动故障响应为主的机制缺乏主动容错能力. 未来可进一步探索高效副本机制和资源调度模型, 并引入机器学习等技术, 实现故障的主动预测与迁移, 从而提升系统在复杂环境下的可用性.

3.3.4 小 结

本节从机密性、完整性和可用性这 3 个方面梳理了数据存储阶段的主要安全挑战与技术进展. 总体来看, 数据存储安全在防护深度和技术手段上不断发展, 但也面临现实困境.

当前防护体系正从单一防线向多层次演进, 数据泄露防护覆盖硬件、算法和物理等多个层面. 数据完整性保护也由外部校验转向内生自证, 标志着分布式可追溯路线的技术思想开始深度影响存储领域, 为多方协同环境下的数据流通提供了新思路.

然而, 现实中仍存在问题. 一方面, 防护体系碎片化, 技术间缺乏统一协调, 整体防护效率有限; 另一方面, 可用性保障依赖多副本冗余和被动容错, 虽提升容错能力, 却带来存储资源浪费和一致性维护成本. 同时, 现有方法多

为故障后的被动响应, 主动预测和智能容错机制尚不成熟, 难以应对复杂动态场景.

综上, 数据存储安全正由分散向系统、由被动向主动转变. 未来研究需关注提升技术融合和整体防护能力, 特别是隐私增强技术与分布式架构的深度协同, 并积极探索基于机器学习和人工智能的主动预测与智能容错机制, 实现更高效、智能和可靠的数据存储安全.

3.4 数据处理阶段

数据处理阶段因需在运行时环境中加载并计算数据, 攻击面较大, 尤其在多租户和跨域协同等复杂场景下, 对机密性、完整性和可用性的保障尤为关键. 本节聚焦数据处理泄露防护、数据处理篡改防护、数据处理可用性保障这 3 类安全目标, 分析主流技术路径与代表性成果, 归纳存在的问题与挑战.

3.4.1 数据处理泄露防护

数据泄露是当今数据处理领域最严重的安全威胁之一, 尤其在云计算和多租户环境下, 敏感数据在内存中的暴露风险显著. 例如, Spectre 攻击利用 CPU 分支预测和推测执行机制, 通过侧信道推测内存中的敏感信息[2]. 当前, TEE 与同态加密 (homomorphic encryption, HE) 是比较具有代表性的两类路径, 分别从硬件隔离与密态计算两个维度出发, 有效降低了敏感数据暴露风险, 如表 4 所示.

表 4 数据处理阶段泄露防护技术对比

技术类型	核心思想	安全性保障	性能	优势	核心挑战	应用场景
可信执行环境 (TEE)	硬件隔离, 受保护的enclave区隔离敏感数据	物理隔离, 防止操作系统/进程访问	高, 计算在明文执行, 硬件加速, 适合实时大规模处理	通用性好, 实时性强, 支持多种数据处理任务	侧信道攻击、内存容量限制、硬件依赖、部署复杂	云计算、边缘计算、隐私保护数据处理
同态加密 (HE)	密态计算, 数据在密文状态下可直接计算	基于数学难题保障, 数据全程不可见	低, 密文计算开销大, 处理速度慢, 难以满足实时要求	强隐私保护, 不依赖专用硬件	计算复杂度高、性能开销大、开发和部署门槛高	隐私计算、医疗、金融等特定场景

TEE 通过在处理器中划定受保护的隔离区 (enclave), 确保数据在其中的处理过程不被高权限软件访问. 典型技术实现包括 Intel SGX[62]、Intel TDX[63]、AMD SEV[64]、ARM TrustZone[65]等, 已在云计算和边缘计算中初步应用. 例如, Li 等人[66]基于 SGX 将网约车的匹配逻辑置于 enclave 中, 有效抵御了服务商与司机的合谋攻击, 且性能远超同态加密等密态计算方案. 然而, 该方案仅适用于单租户环境, 未能解决多租户场景下的隔离问题.

随着 TEE 在云平台和多租户服务中的应用需求增长, 如何在共享硬件资源的前提下仍保障不同用户间的隔离性, 成为实际部署中的关键问题. 为应对云平台中多用户共享 enclave 可能引发的缓存泄露等安全风险, Wang 等人[67]提出了 Liveries 技术, 通过引入轻量级且可验证的 enclave 内部用户隔离机制, 限制线程权限, 并在用户切换时对关键数据进行完整性检查与清理, 从而有效降低了多用户共享 enclave 时的安全风险. 相较于单用户方案, Liveries 解决了安全共享问题, 但也因其复杂的资源调度逻辑而提高了开发部署门槛.

虽然 TEE 技术发展迅速, 但其仍具有难以回避的局限性: 首先, TEE 的内存限制对并发处理能力构成瓶颈; 其次, TEE 可能受到侧信道攻击的威胁, 导致数据泄露; 再次, 这类方案依赖于特定硬件平台, 部署灵活性较差.

与 TEE 不同, 同态加密通过允许数据在密文状态下进行计算, 从根本上避免了敏感数据暴露于处理环境的风险. 以 Gentry 等人[68]提出的全同态加密 (fully homomorphic encryption, FHE) 方案为基础, 近年的研究在计算效率上取得了显著进展[69], 该方向经过算法设计、编程工具与场景落地这 3 个阶段的优化, 逐步走向实用性.

在算法层面, Cheon 等人[70]通过重缩放和批处理技术, 显著提高了部分同态加密的效率, 使得复杂应用例如机器学习推理和数据库查询等场景成为可能.

在编程工具层面, Viand 等人[71]提出的 HECO 编译器能够将高级命令式程序自动转换为高效的 HE 实现. HECO 基于多级中间表示设计, 结合静态分析与自动单指令多数据批处理优化, 显著减少了开发者对底层加密操作与性能调优的依赖. 与 Cheon 等人[70]聚焦于底层同态算法优化不同, HECO 更关注编译层的自动转换与程序表达, 实现了面向开发者友好的通用编程框架.

在具体应用上, Li 等人[48]针对导航问题, 提出一种半约束导航方案, 通过同态加密和混淆电路实现了高效且

安全的导航, 确保用户信息不暴露. 兼顾导航结果正确性与隐私性, 证明了同态机制在实际服务系统中的可行性. 这 3 项工作分别从底层算法、开发工具和应用落地层面推动了 HE 的实用化进程.

尽管 HE 技术取得了显著进展, 但现实挑战依然突出. FHE 本身极高的计算复杂度、专用编译器在跨平台部署上的困难以及现有方案对特定任务结构的依赖, 共同限制了其通用性. 当前 HE 技术虽在特定任务中初具实用性, 但在大规模通用计算方面仍面临算法、编程与系统层面的协同优化挑战.

总体来看, TEE 与 HE 分别代表了当前数据处理阶段防护运行时数据泄露的两大主流技术路线, 二者在安全性、性能和适用范围等方面各有优劣, 未来如何在算法、系统和应用层面实现协同优化, 仍是该领域重要研究方向.

3.4.2 数据处理篡改防护

数据篡改是数据处理阶段另一个重要的安全威胁, 其主要原因包括恶意代码注入、数据处理逻辑被篡改等. 例如, 在 Hadoop、Spark 等大数据框架中, 未经验证的用户可提交恶意作业, 操控处理流程或篡改结果[72]. 针对该问题, 现有防护方案主要包括权限控制、执行隔离和行为检测, 分别从访问授权、执行空间保护和运行时行为约束这 3 个维度防御 (如图 4 所示).

图 4 数据处理完整性的纵深防御体系

权限控制是第 1 道防线, 旨在通过授权确保操作的合法性. 传统的基于角色的访问控制 (role-based access control, RBAC) 为用户分配特定权限角色, 限制其在处理流程中的操作[73]. 具有实现简单、效率较高的特点, 得到广泛应用. 为应对复杂云环境中的细粒度权限管理问题, Ying 等人[74]提出了支持策略隐藏与动态更新的密文策略属性加密 (ciphertext-policy attribute-based encryption, CP-ABE) 机制. 该方案将访问控制逻辑嵌入密文中, 允许数据持有者设定访问策略, 只有满足对应属性的用户才能解密并处理数据, 进一步提升 CP-ABE 在云端数据处理场景中的隐私保护与动态管理能力. 与 RBAC 不同, CP-ABE 将访问策略直接嵌入密文, 实现了加密与权限的强绑定, 更适合云端数据处理模式. 然而, 该路线也引入了新的挑战, 即复杂的密钥管理和高昂的属性撤销开销, 这限制了其在动态权限管理场景下的应用. 为了进一步增强云端数据访问控制的灵活性, Wang 等人[75]提出了具有可更新密文的见证脱密框架, 允许利用更新令牌在不解密的情况下更新密文标签, 从而实现了更细粒度的动态访问策略调整, 有效解决了动态环境下的策略调整难题.

当权限控制被绕过时, 执行隔离作为第 2 层保护, 通过将处理任务置于安全容器中来防止外部干扰. 例如 Mi 等人[76]利用环境隔离技术, 将安全逻辑从管理程序中剥离至受保护的虚拟机, 增强了对数据处理逻辑的保护. 此类方案强调封闭的执行逻辑, 但其高昂的部署成本与资源开销, 尤其是在并发场景下, 限制了其适用范围.

静态的权限控制与执行隔离难以防御运行时的动态攻击, 因此, 基于异常行为的行为检测成为不可或缺的动态补充. 例如, Sharma 等人[77]提出基于无监督学习的用户行为建模方法, 通过分析日志数据来识别内部威胁. 这类方法具备自适应能力, 但其有效性高度依赖高质量的训练数据, 且常面临误报与漏报的挑战. 未来研究方向在于构建一个更整合的防御体系, 包括提升权限控制的动态适应性, 提高执行隔离的效率, 并优化行为检测的准确性与泛化能力.

可以看出, 针对数据处理完整性, 单一技术难以有效应对. 静态的权限控制、执行隔离与动态的行为检测需协同构建防御体系, 但高效整合与统一管理仍是主要挑战.

3.4.3 数据处理可用性保障

数据可用性是数据处理安全的重要维度, 旨在保障处理服务在遭遇攻击或硬件故障时的持续稳定运行. 当前主要威胁包括拒绝服务攻击和资源竞争. 动态资源管理技术是应对可用性问题的常用方法, 通过分析历史负载进行预测和负载均衡. 例如, Saxena 等人[78]提出的资源管理框架能够预测服务器资源利用率并实现动态调度, 尤其适用于具有周期性波动或可预测负载的数据处理场景, 如定期的模型训练任务.

然而, 基于历史数据的预测方法存在固有限制. 首先, 该方法难以应对未知模式, 对于突发任务请求或攻击流量时, 预测模型可能失效, 导致调度响应滞后. 其次, 这类方法仅关注资源利用趋势, 缺乏对任务本身行为特征的安全分析, 无法分辨高资源消耗任务是正常业务还是恶意操作 (如挖矿程序). 因此, 现有机制在识别和防御针对可用性的恶意威胁方面仍有不足. 未来可进一步结合任务行为分析与攻击检测机制, 构建能够感知威胁的弹性资源调度框架, 实现从预测优化到主动防御的演化.

3.4.4 小 结

本节围绕数据处理阶段的机密性、完整性和可用性这 3 大核心安全目标, 系统梳理了当前主流防护技术路径及其代表性进展, 并深入分析了其面临的现实挑战. 总体来看, 数据处理安全具有以下几个特点.

首先, 数据泄露防护主要依赖硬件隔离与密态计算两大技术路线. TEE 通过为计算任务划定隔离区域, 实现高效的运行时安全处理, 适用于对实时性和硬件安全有要求的场景, 但在多用户隔离、侧信道防护及资源受限等方面仍有局限. HE 则支持密文计算, 理论上可实现全密态保护, 但在计算复杂度、系统集成和通用性等方面仍面临挑战. 两者各有优劣, 这两种技术的竞争与互补, 反映了硬件隔离与隐私增强两条路线在计算环节的博弈, 未来的突破口在于二者的协同融合与软硬一体化.

其次, 数据完整性保护已形成多层防御体系, 包括静态的权限控制、执行隔离和动态的行为检测. 权限控制正向细粒度和属性驱动演进, 但随之带来密钥管理和策略一致性难题. 执行隔离和行为检测提升了环境安全性和攻击响应能力, 同时增加了系统复杂性和资源消耗. 如何平衡安全性、灵活性与性能, 亟需进一步探索.

最后, 可用性保障仍以动态资源管理和负载均衡为主, 能够有效应对常规负载波动. 但对异常行为和未知攻击的识别能力有限, 难以防范恶意任务滥用系统资源或发起攻击. 未来需要将安全分析与资源调度深度融合, 构建能够感知威胁、动态应对的智能弹性调度体系.

在应用方面, TEE 与同态加密等技术正在打破数据孤岛, 使多方在不交换明文数据的前提下实现协同计算成为可能, 对组织内部流通和数据共享模式等具有重要意义.

综上, 数据处理安全正向多层协同演进, 但在防护深度、技术融合和主动防御方面仍有不足. 未来应重点推进软硬件一体化安全架构、高效密态计算和智能弹性调度等方向.

3.5 数据发布阶段

数据发布阶段的安全焦点从数据自身的保密性, 转向对数据可控性的维护和对个人隐私的保护. 与数据传输和数据存储阶段相比, 尽管数据机密性与完整性依然重要, 但其技术保障多继承前置阶段 (如数据传输、存储、处理). 相比之下, 如何在数据共享过程中维持发布方对数据的控制权, 以及如何防止敏感信息泄露, 成为本阶段的核心挑战. 本节将结合定向发布和公开发布两种模式, 围绕数据发布可控性维护和隐私保护展开详细讨论.

3.5.1 数据发布可控性维护

数据发布阶段的核心问题之一是数据可控性维护, 即数据发布主体如何保持对数据使用范围、传播路径及操作权限的控制力. 例如, 合法用户虽能获取机密数据, 却可能将其用于非法用途[79], 或因终端设备安全性不足导致数据泄露[80]. 为此, 研究已形成覆盖事前、事中、事后的完整防护链条.

● 事前预防通过权限控制与执行隔离, 从源头限制数据暴露面. 例如, Chen 等人[81]针对触发-动作平台, 通过数据访问最小化解决了过度权限问题. 然而, 权限控制无法约束合法用户获得数据后的复制行为. 为此, TEE 技术被引入, 通过硬件隔离实现可用不可见的数据保护模式, 以减少数据暴露风险. 例如, Chen 等人[82]基于 Intel SGX 提出一种高效的 SQL 查询框架, 可支持多用户对外包数据的安全查询. 然而, TEE 的应用受到硬件兼容性和开发

成本的限制, 难以在所有发布场景中推广. 总体来说, 事前预防机制能限制数据访问, 防止非法访问, 但无法防止合法用户复制或分发数据, 因此还需配合其他后续防护措施.

● 事中防护聚焦于防止合法访问后的数据滥用. 例如, 数据防泄露 (data leakage prevention, DLP)[83]技术通过分析数据内容及其上下文, 结合通知、审计、阻止、加密和隔离等手段保护数据的安全性. 优势在于能够覆盖数据的多种状态, 但其部署和维护成本较高, 且难以防止物理泄露方式 (拍屏、录像等). 一旦数据被非法扩散, 这些机制难以阻止其继续传播, 因此还需要事后追责, 以便追查责任、震慑恶意行为.

● 当泄露发生后, 事后追责成为最后一道防线, 主要包括可证明删除、数字水印和区块链取证这 3 种技术路径. 可证明删除旨在确保数据被有效销毁并提供可验证性. 例如, Hao 等人[84]提出一种基于信任但验证 (trust-but-verify) 机制的可证明删除方案, 利用受信平台模块 (trusted platform module, TPM), 在不完全可信环境中实现数据删除. 该机制的优点是删除操作可被第三方验证, 并作为审计证据, 但它依赖硬件平台和大量加密运算, 可能导致计算延迟, 影响用户体验. 数字水印通过在数据中嵌入可识别标识来溯源泄露者. 值得注意的是, 虽然数字水印在第 3.6 节数据溯源中也扮演重要角色, 但在发布安全阶段, 其核心目标侧重于所有权锚定与泄露源定位, 即作为一种防御性机制, 确保数据流出后的责任可追溯. 例如, Hu 等人[85]提出了一种基于保序加密的可逆水印方案, 通过在密文中嵌入鲁棒性的水印实现了数据追踪与版权保护. 相比可证明删除, 水印技术更适用于防止数据扩散, 但其鲁棒性有限, 易受篡改攻击, 且在频繁交互时嵌入会带来开销. 区块链则通过构建不可篡改的操作日志来实现审计与取证, 例如, Li 等人[86]设计了一种隐私保护的车联网数组取证系统, 结合区块链和数字水印对泄密者追踪. 针对部分泄露数据问题, Li 等人[87]提出了一种匿名且安全的去中心化取证方案 Themis, 兼具可追溯匿名性、隐私访问控制以及高效搜索能力, 能够有效追踪泄密者. 区块链的优势在于其透明性与不可篡改性, 但引入的性能开销、链上存储限制及共识机制复杂性也带来了推广的阻碍.

总体来看, 数据可控性维护技术分为事前预防、事中隔离和事后追责这 3 层. 权限管理和 TEE 侧重事前防护; DLP 关注事中操作; 可证明删除、数字水印和区块链则用于事后审计. 但这些技术各自独立, 缺乏协同, 且整体上偏向被动补救, 难以主动防止数据泄露.

3.5.2 隐私保护

除了可控性维护, 数据发布还面临隐私保护挑战, 尤其在对外开放场景下, 发布方难以掌控数据流向, 因此必须对数据内容实施隐私保护. 目前已有多种策略, 主要分为两类技术路线, 如表 5 所示.

表 5 数据发布阶段隐私保护技术对比

技术类型	核心思想	保护强度	优势	核心挑战	适用场景
数据脱敏	基于规则的启发式处理, 对敏感信息进行替换、屏蔽等	较弱, 易受关联分析与背景知识攻击	部署灵活、计算开销小、适合结构化数据	依赖敏感信息明确定义, 难以防止推断攻击	结构化数据共享、常规数据发布
差分隐私	基于数学可证明的隐私保护, 通过添加噪声控制泄露上界	强, 可量化, 具备严格的数学保障	保护强度高、可量化、适合统计与机器学习	噪声影响数据精度, 保护强度与可用性需权衡	统计分析、机器学习、分布式场景

(1) 基于规则的启发式脱敏

数据脱敏通过屏蔽、模糊化、伪造或合成等方式对数据进行处理, 其核心思想是根据预先定义的规则, 对数据中的敏感标识符 (如姓名、身份证号) 进行修改或替换. 例如, Yoon 等人[88]提出一种基于生成对抗网络的数据合成方法 ADS-GAN, 用于生成电子健康记录, 在提升数据可用性的同时减少泄露患者隐私的风险. Zhu 等人[89]在私人停车点共享场景下, 提出隐私保护智能停车方案 ASAP, 通过脱敏技术将其真实位置转换为较大的区域范围, 从而实现位置隐私保护. 数据脱敏方法部署灵活、计算开销小, 适用于结构化数据和常规共享. 但其隐私保护依赖于敏感信息的界定, 难以防止关联分析等推测攻击.

(2) 基于数学的可证明隐私

差分隐私通过在数据或查询结果中添加噪声, 在保护隐私的同时保留数据的统计特性和分析价值[90], 其核心思想是通过在查询结果中添加经过精确计算的噪声, 使得攻击者无法判断特定个体是否在该数据集中. 其优点是隐私保障严格, 但引入噪声可能降低数据准确性, 尤其在高敏感的分析任务中. 在分布式场景中, 本地差分隐私

(local differential privacy, LDP) 进一步提升了隐私保护能力, 通过在客户端本地添加噪声, 有效防止敏感信息被窃取. 例如, Wei 等人[91]将 LDP 应用于联邦学习, 通过在客户端本地对模型参数添加噪声后上传, 降低隐私泄露的风险. 差分隐私适用于统计分析和机器学习, 具有可量化和通用的优点. 但其隐私保护与数据可用性存在权衡, 噪声可能降低模型精度和数据效果.

实际应用中, 数据脱敏适合结构化数据共享, 差分隐私更适合统计和建模任务. 两者不是简单替代关系, 而是从规则到可证明隐私的进步. 差分隐私及其变体因其严格隐私保障, 已成为未来隐私保护的发展方向.

3.5.3 小 结

本节围绕数据发布阶段的安全挑战, 重点分析可控性维护和隐私保护两大核心目标. 当前, 数据可控性维护已从单一的事前访问控制, 发展为覆盖事前 (权限控制、执行隔离)、事中 (DLP)、事后 (可证明删除、数字水印、区块链取证) 的多层体系, 但各环节协同不足, 整体以被动补救为主, 主动、一体化的防控机制仍待完善. 这种数据可控性维护在数据交易模式中体现得尤为迫切, 因为它能有效应对所有权转移后的失控风险, 为数据资产化提供必要的安全兜底.

在隐私保护方面, 技术正由基于规则的脱敏向以差分隐私为代表的数学可证明方法转型. 差分隐私实现了严格的隐私量化保障, 但在数据可用性和分析精度上存在权衡. 未来如何实现防控链条协同和高效、可用的严格隐私保护, 是数据发布安全的关键研究方向.

3.6 数据溯源阶段

数据溯源阶段的安全问题主要涉及机密性、完整性和可用性. 系统在该阶段可能遭遇溯源信息泄露、数据篡改及系统可用性受损等威胁, 影响溯源安全. 现有方案包括区块链存证、密态水印和分布式索引等, 但在跨组织流通、恶意篡改和高并发查询等情境下仍有不足. 本节将从溯源数据泄露防护、溯源数据完整性保护和溯源可用性提升这 3 个方面展开分析.

3.6.1 溯源数据泄露防护

数据溯源信息的泄露是数据溯源过程中的安全威胁之一. 为实现溯源, 系统需记录数据流转路径、处理者身份和访问日志等详细信息, 这些内容一旦泄露, 可能导致敏感数据暴露, 甚至被攻击者推测出用户身份. 例如, 在区块链溯源系统中, 攻击者可能通过合谋推测用户的真实身份[92]. 因此, 在保障溯源能力的同时防止溯源信息泄露, 已成为溯源阶段的首要安全挑战, 并推动多样化的技术路径发展.

对溯源记录实施字段级加密与访问控制, 是保障溯源信息机密性的直接手段. 其核心是对结构已知的溯源记录中的敏感字段 (如用户 ID、操作记录) 加密, 并结合密钥管理实现访问控制. 例如, Hasan 等人[93]对敏感的溯源链记录字段进行加密, 并使用基于广播的加密密钥管理方案进行权限控制, 确保了数据机密性. 这类方案适用于字段级保密需求高、访问主体可区分的场景, 技术成熟, 但在动态授权和密钥更新方面存在一定复杂性.

在某些场景下, 需求侧重于验证溯源属性而非读取具体内容. 零知识证明 (zero-knowledge proof, ZKP) 技术可实现在不泄露数据内容的前提下验证特定属性, 例如, Lauinger 等人[94]针对敏感 Web 数据的溯源问题使用 ZKP 技术, 在保护数据机密性的前提下验证数据来源. 此类方法适合内容敏感但验证需求高的场景, 隐私保护能力强, 但计算成本较高, 难以用于高频溯源. 在物联网场景下, Canovas Sanchez 等人[95]结合匿名凭证、非交互式零知识证明和 Idemix 签名技术, 确保溯源数据的机密性, 并允许合法受控解密. 该方案强调对身份隐私的保护, 适用于匿名化溯源需求, 但凭证管理和系统扩展性仍是关键挑战.

与前述方法不同, 数字水印通过在数据本体中嵌入溯源信息, 适用于流数据、图像等多媒体场景. 需要区别的是, 与数据发布中将水印仅作为泄露追踪标识不同, 在溯源阶段, 水印充当了敏感溯源元数据的容器. 因此, 其面临的安全挑战更多是水印内容本身的机密性, 即如何防止攻击者提取并解读水印中携带的敏感信息. 例如, Sultana 等人[96]通过时延水印实现流数据溯源, 该方法依赖水印的隐蔽性. 然而, 水印携带敏感信息, 若设计不当, 可能被攻击者提取, 导致隐私泄露. 为应对这一问题, Li 等人[86]在其提出的数字取证系统中, 将加密后的身份标识嵌入媒体数据作为水印内容, 即使攻击者成功提取出水印, 也无法解密其中的身份信息, 有效增强了水印机制的信息机密

性. 尽管如此, 密钥分发与嵌入容量等问题仍需进一步解决, 实际应用中需权衡系统资源和数据特性.

综上, 数据溯源阶段的机密性保护机制体现出多路径协作的特点, 字段加密和访问控制适用于结构化数据, ZKP 与匿名凭证满足高隐私需求的验证场景, 加密水印机制则适合数据分发等应用. 整体上, 保护目标从静态记录延伸到动态验证和数据载体, 形成纵深防护. 不同技术各有侧重, 但普遍面临性能和管理复杂性挑战. 未来研究可探索多机制融合, 在保障溯源能力的同时提升隐私保护和计算效率.

3.6.2 溯源数据完整性保护

数据溯源系统需持续记录数据流转过程中的操作和状态变化, 记录通常以链式时间序列形式存在, 是责任追溯、行为审计和安全取证的依据. 因此, 任何对溯源记录的篡改、伪造或删除都会破坏溯源链的可信性, 影响数据来源的可验证性. 为此, 研究者提出了多种溯源完整性保障技术, 体现了信任模型的不断演进 (如图 5 所示).

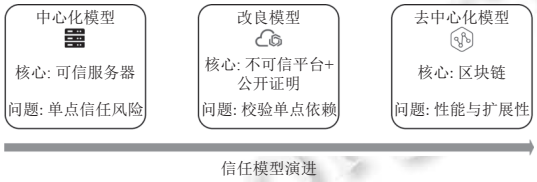

图 5 数据溯源完整性保障技术信任模型演进

● 第 1 阶段是中心化的信任模型. 传统数据溯源完整性方案主要依赖链式结构[97], 其中, Hasan 等人[93]提出的溯源方案是溯源完整性保护的奠基性工作. 在该方案中, 每条溯源记录包含前一条的校验和, 并由用户私钥签名, 保证记录不可篡改. 这种方式具备结构简洁、验证高效的优点, 适用于单域环境下对篡改行为的防范. 但由于其依赖中心化平台管理, 存在明显的信任单点问题, 一旦可信节点被攻破, 整个链条可能被伪造.

● 第 2 阶段是中心化的信任模型面向不可信云的改良. 随着云计算的普及, 研究者开始考虑云服务商自身不可信的场景, Zawoad 等人[98]结合聚合签名以对溯源链进行管理, 并定期发布累加值作为公开证明, 即使云服务提供商恶意, 也无法篡改或伪造可追溯性记录, 从而确保完整性. 该工作将云端的合谋攻击纳入溯源系统威胁建模之中, 为虚拟化环境下的溯源系统设计提供了系统级的安全保障.

● 第 3 阶段是去中心化的信任模型. 随着多组织间数据流转需求增长, 传统中心化结构难以满足跨域完整性保障. 区块链作为去中心化、不可篡改的账本, 被广泛应用于溯源系统, 例如, Liang 等人[99]提出了基于区块链的数据溯源架构 ProvChain, 利用哈希和默克尔树将溯源记录的根哈希上链, 保障不可篡改性并提升数据写入效率. 进一步地, Ruan 等人[100]提出的 LineageChain 引入智能合约, 实现链上动态查询和篡改检测, 支持在线可验证的溯源. 这类方法适用于多方协作、跨组织数据流通场景下的行为可审计需求, 但其链上计算开销与共识延迟仍是系统吞吐能力的制约因素.

综上, 数据溯源系统的完整性保障经历了从信任单点、校验单点到去中心化的演变. 尽管去中心化提升了安全性, 但也带来了性能、成本和可扩展性等新挑战. 未来可进一步研究轻量级链上存证、链下验证和跨链协同等机制, 以在提升系统扩展性与能力的同时保持溯源链的不可篡改性和全生命周期一致性验证.

3.6.3 溯源可用性提升

数据溯源需要实时记录流转行为, 并支持高频、低延迟查询, 以满足审计和追责需求. 随着数据量和并发访问增加, 溯源系统容易出现查询慢、写入阻塞甚至不可用等问题, 影响其可用性和应急响应. 因而, 提升系统可用性、高效写入和快速查询, 是保障溯源系统稳定运行的关键. 然而, 其链式结构和共识机制往往成为性能瓶颈.

在问题表现上, 溯源阶段的可用性问题主要可以分为两类, 一类是查询效率不足, 即在面对复杂溯源路径或高频存在性验证请求时, 系统响应延迟明显. 另一类是写入吞吐受限, 尤其在采用链式结构或区块链结构记录溯源信息的系统中, 写入操作往往受到链结构维护或共识协议性能的瓶颈影响.

由于溯源链结构不利于随机访问, 效率受限, 研究者提出多种结构优化. 例如, Ruan 等人[100]在 LineageChain

中通过 DAG 和追加式跳表提升索引效率, 但在数据频繁更新时维护成本较高, 可能出现索引退化. Zawoad 等人[98]引入布隆过滤器, 实现快速存在性验证, 提高查询效率, 但存在假阳性, 且难以支持数据删除或更新时的一致性维护. 数据溯源系统的写入性能瓶颈可能来源于多种因素, 包括底层存储结构、日志写入策略及一致性共识机制等.

近年来, 随着区块链在溯源系统中的应用, 其写入性能问题日益突出. 与中心化系统相比, 基于区块链的溯源系统需在链上确认每条记录, 写入吞吐受限于共识协议和区块生成速度. 为此, 研究者对共识机制和区块组织进行了优化. 例如, Zhang 等人[101]提出基于哈希链的快速共识协议, 提升了私有链和联盟链的写入速率. 为了提高出块效率, Liu 等人[102]设计了 Dolphin 共识协议, 采用非阻塞并发区块生成机制, 在高延迟环境下显著提升了区块链的交易吞吐量, 使其更加适用于高频数据溯源场景. Zhang 等人[103]提出的 Phantasm 协议增强了系统的鲁棒性, 以应对分裂攻击. 但区块链的高存储成本和扩展性限制仍需关注. 综上所述, 数据溯源系统的可用性保障机制需综合考虑查询效率与写入能力的平衡.

当前研究表明, 溯源系统的可用性保障, 本质上是在确保安全的前提下, 弥补链式结构带来的性能损耗. 目前, 跳表和布隆过滤器可提升查询性能, 轻量级共识协议和并发处理机制有助于提高写入吞吐量. 未来可进一步探索异构链结构、多层缓存和链下验证等技术, 构建高可用的溯源系统.

3.6.4 小 结

数据溯源作为贯穿数据生命周期的审计流程, 其安全技术的发展也呈现出独特的趋势. 综合本节分析, 可以提炼出两大核心特点.

首先, 信任模型由中心化向去中心化演变. 这是溯源技术发展的主线, 也标志着分布式可追溯路线在数据全生命周期安全保障中正式占据了重要地位. 从依赖单一服务器到校验平台再到彻底去中心化, 信任模式的变化推动了溯源系统的演进.

其次, 完整性与可用性之间存在权衡. 不可篡改性是溯源系统的核心价值, 但通过链式结构和共识机制实现时, 往往会降低查询和写入性能, 因此系统设计需在两者间进行平衡.

总体而言, 溯源安全技术正从单纯记录转向实现无需信任、不可篡改且高效的复杂系统. 未来突破将依赖于轻量级密码学协议、高效去中心化共识和创新的链上/链下协同结构.

3.7 总 结

数据要素在流通的各个阶段均面临复杂的安全威胁, 且不同阶段的防护需求与技术瓶颈各异. 本节对 6 个阶段所面临的主要安全挑战、现有研究工作及待解决问题进行了系统性梳理与汇总, 具体如表 6 所示.

表 6 数据要素流通各阶段安全问题、现有研究工作以及待解决问题

流通阶段	问题	研究工作	技术路线	典型时间复杂度	待解决问题
数据采集	设备采集数据泄露及篡改	[26–28]	基于TEE的采集设备保护	进出enclave固定开销O(1)+具体执行开销O($f(n)$), f为TEE中运算	硬件依赖导致适配难成本高, 软件隔离弱易受内核及旁路攻击, 轻量化方案难兼顾性能与安全
		[29]	轻量级加密算法	依赖具体算法, 例如, AES为O(n), n为输入数据长度	在低功耗设备上难以同时满足较高强度算法的算力与能耗需求
	人工录入数据泄露及篡改	[31]	用户认证	依赖具体协议	身份认证影响用户体验, 策略可能误判, 维护成本高
		[32]	采集端环境隔离	非算法, 系统级开销	环境隔离在受限设备上仍需必要的性能与资源开销
	爬虫/接口数据泄露及篡改	[33,34]	数据源认证	依赖协议, 例如文献[34]包括: 生成随机数O(1)+签名O(k^2)+计算MAC O(1)+验签O(k^2), k为密钥长度	系统在复杂异构网络中仍难兼顾高灵活性与通用协议的安全适应性
数据传输	传输数据泄露	[35,37]	加密传输协议	握手O(k^2)+证书链验证O(m)+数据传输O(n), k为密钥长度, m为证书链长度, n为数据长度	协议防护受限于系统复杂性、资源瓶颈及工具可靠性不足
	传输数据篡改	[39,40]	数字签名方案	签名O(k^2)+验证O(k^2), k为密钥长度 (以ECDSA/EdDSA为例)	同时受传统签名的量子风险与后量子方案在性能和适配性上的部署限制

表 6 数据要素流通各阶段安全问题、现有研究工作以及待解决问题 (续)

流通阶段	问题	研究工作	技术路线	典型时间复杂度	待解决问题
数据传输	传输中断	[42]	多路径数据传输	非算法, 系统级开销	并发多路径在大规模场景下仍受调度复杂性与维护开销制约
数据存储	存储数据泄露	[44]	硬件安全模块(HSM)	依赖具体协议	系统集成复杂度高, 硬件成本增加
		[45–52]	加密存储协议	数据加解密O(n), n为数据长度	加密查询结构复杂导致计算开销高
		[54,55]	物理介质销毁	不适用 (物理销毁无算法时间复杂度)	稳定性与效率难以平衡
	存储数据篡改	[59]	基于IPFS的存储完整性保护	文件添加O(n)+文件查找O(log$N$+n)+DHT查找O(log$N$)+内容发布O(log$N$), n为数据长度, N为节点数量	内容寻址在大规模场景下检索低效且系统集成复杂, 导致存储与性能开销偏高
	数据存储不可用	[61]	高可用存储技术	非算法, 系统级开销	多副本与被动容错方案仍受高存储与计算资源消耗限制
数据处理	处理数据泄露	[62–67]	TEE保护的数据处理	进出enclave固定开销O(1)+具体执行开销O(f(n)), f为TEE中运算	TEE受内存与硬件限制及侧信道风险制约, 多租户场景下的隔离与部署灵活性仍不足
		[48,68–71]	同态加密	加密O(n^3)+解密O(n^3)+加法O(n^3)+乘法O(n^4), n为数据长度	受噪声累积、参数膨胀与电路深度限制所导致的结构性计算瓶颈制约
	处理数据篡改	[74,75]	访问控制机制	O(1)–O(m), m为权限数量	在动态场景下受密钥更新与属性撤销成本高的限制
		[76]	环境隔离	非算法, 系统级开销	受容器与虚机隔离带来的资源与调度开销限制
		[77]	行为检测	依赖检测模型	受误漏报与延迟导致的准确性和实时性不足制约
	数据处理不可用	[78]	计算负载均衡	非算法, 系统级开销	基于历史预测难以应对突发与未知模式, 导致防护响应不及时
数据发布	发布数据可控性	[81]	最小化授权	代码分析O(n), n为代码长度	难以限制合法用户在获取数据后再分发与扩散行为
		[82]	TEE保护的安全数据查询	进出enclave固定开销O(1)+具体执行开销O(f(n)), f为TEE中运算	在发布场景中受硬件兼容性、侧信道风险与开发部署成本限制
		[83]	数据防泄露系统	依赖策略复杂度	成本较高, 难应对拍屏等物理层面的泄露方式
		[84]	可证明删除	依赖密码学协议	面临较高的存储与计算开销
		[85–87]	数据泄露追踪	嵌入O(n)+提取O(n), n为数据长度	链上存储与共识带来性能限制
	发布数据隐私保护	[88,89]	数据脱敏	O(n), n为数据长度	难以抵御关联分析等推断攻击, 仍存在隐私泄露风险
		[90,91]	基于差分隐私的隐私保护	噪声添加O(1)+查询O(n), n为数据长度	在高噪声需求下易导致精度下降, 难以兼顾隐私保护与数据效用
数据溯源	溯源数据泄露	[93–95]	加密溯源数据保护	数据加密O(n)+数据解密O(n), n为数据长度	使用密码学机制时易产生较高的计算与管理开销
		[86,96]	水印信息防护	水印加密O(m)+水印嵌入/提取O(n), m为水印长度, n为数据长度	受密钥管理复杂与水印容量有限的制约
	溯源数据篡改	[93,98]	中心化溯源	依赖协议, 例如文献[93]中, 数据写入: 签名O(k^2)+广播加密O(log$n$); 验证O(L), k为密钥长度, n为审计员数量, L为溯源链长度	依赖中心化体系, 存在单点故障和过强信任假设
		[99,100]	区块链溯源	写入O(共识); 查询O(L), L为链长度	受链上存储成本高与共识吞吐低的限制
	数据溯源不可用	[98,100]	查询结构优化	依赖协议, 例如文献[98]中, 数据查询O(log$_b$$N$), b为跳表基数, N为版本数	动态数据更新带来高维护开销, 布隆过滤器存在假阳性问题
		[101–103]	高效共识协议	依赖协议, 例如文献[101]中, 共识O(n), n为共识节点数量	受共识延迟与状态膨胀双重制约, 仍难以在高频溯源场景下保持吞吐

4 数据要素流通可信问题

在数据要素流通过程中, 可信性是保障数据安全流通和高效利用的关键. 可信问题与安全问题相关但有所不同. 安全主要关注数据是否被窃取、篡改或破坏, 而可信更关注数据内容和来源的真实性、可靠性. 可信性贯穿数据流通的各个阶段, 直接影响流通效率和应用效果, 如图 6 所示.

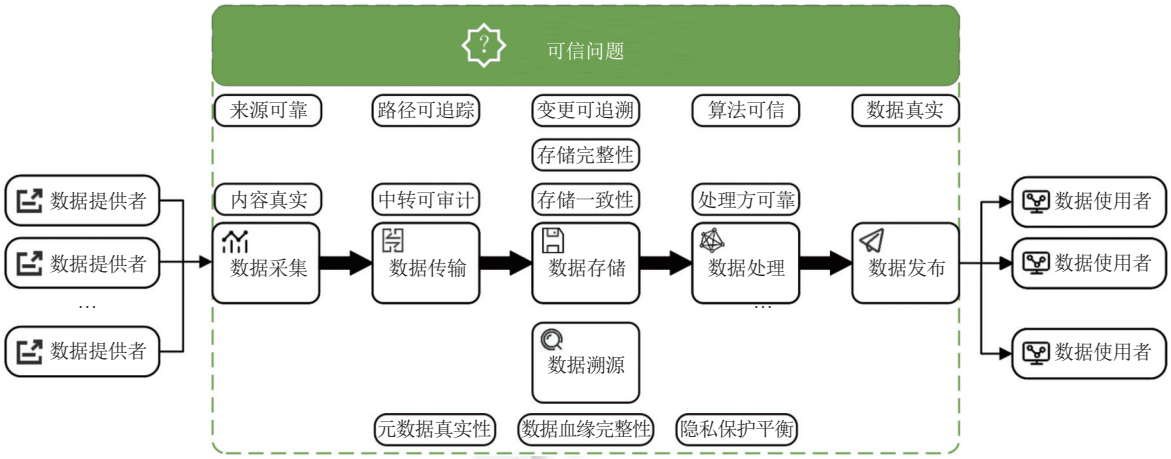

图 6 数据要素流通各阶段可信问题

4.1 数据采集阶段

数据采集阶段的可信问题主要包括数据来源的可靠性和数据内容的真实性, 来源不透明或偏差会损害数据的信任基础. 现有方案虽能提升采集可信性, 但普遍存在计算和存储开销大、难以适应复杂场景等问题. 本节将针对不同采集场景, 分析其可信性挑战及应对方法.

4.1.1 自动化设备采集

在自动化采集中, 数据来源的可靠性主要体现在采集设备可靠性和采集数据真实性两个方面. 例如, 攻击者可能伪造合法设备并上传伪造数据[104], 或因设备故障导致数据失真[105]. 为此, 形成了两类不同的信任机制.

针对设备身份伪造问题, 基于硬件物理特性的方案从物理层面为每个设备赋予不可复制的标识. 例如, Guin 等人[106]利用静态随机存储器产生的随机物理偏差作为设备指纹, 构建物理不可克隆函数 (physical unclonable function, PUF), 实现低成本、高可靠的硬件身份认证, 适用于边缘设备环境. 但在大规模分布式场景下, 设备部署和认证管理仍面临挑战. 且 PUF 方案仅能保证设备身份真实性, 无法防止设备因故障或被攻击上传虚假数据.

基于分布式共识的信任机制通过群体共识替代对单一设备的信任, 构建了动态、全局的信任体系. 基于区块链的信任管理是其主流实现. 例如, Liu 等人[107]提出基于区块链的半集中式信任管理架构, 动态评估物联网设备信任值, 能够抵御异常或恶意设备上传失真数据, 适用于大规模异构设备协同, 但对链上写入频率和计算资源有较高要求. 针对车联网, 刘代东等人[108]提出分层区块链信誉管理系统, 将事件数据分层存储, 并结合贝叶斯推理模型和改进共识算法, 实现高效、上下文相关的信誉评估, 适合动态和不确定性高的场景. 这类方案可持续评估设备行为, 具备可审计性和动态识别能力, 但同样对计算和通信资源有较高要求.

从机制上看, 硬件可信根侧重静态身份认证, 方案轻量, 适合设备端应用, 但功能有限; 分布式信任 (如区块链结合动态模型) 侧重动态行为, 具备强可审计性和全局一致性, 但对资源要求较高, 难以直接在资源受限设备上部署. 现有研究多关注设备行为结果, 未来可进一步对行为过程进行建模, 提升动态可验证性.

4.1.2 人工录入

人工录入数据的可信性既受无意失误影响, 也面临恶意伪造威胁, 因此治理需从内外两个层面入手. 自动化清洗等内部治理方法是提升数据质量的重要手段, 常通过领域知识和规则模型识别、修正异常数据. 例如, Shi 等人[109]

提出了一种适用于医疗场景的数据自动化清洗方法, 能够以高度自动化的方式处理大规模数据. 该方法具备较高自动化程度, 但其依赖专家经验和领域规则, 难以适应跨领域场景, 且对恶意伪造数据缺乏鲁棒性.

外部治理侧重于记录和追踪数据录入行为, 如“谁在何时何地提交了数据”, 而不仅关注数据内容本身. 例如, Li 等人[86]针对车联网场景, 通过区块链记录数据提供者的元数据以确保数据变动可追溯, 防止虚假数据上传和篡改. 但这种方法在写入性能和隐私保护方面存在挑战, 一是在高频交互场景下易出现性能瓶颈, 二是在涉及敏感身份信息时, 链上记录可能导致隐私泄露.

综上, 自动清洗与行为追踪构成了保障数据可信的双重体系, 前者提升数据质量, 后者明确责任归属. 针对自动清洗依赖领域知识、泛化能力不足的问题, 未来可引入跨领域迁移学习等方法提升适应性. 针对区块链方案, 可采用链下索引、ZKP 等机制, 在保障可审计性的同时降低链上负载与隐私风险.

4.1.3 第三方接口调用与网络爬虫

当数据来自不可控的第三方时, 可信性风险显著增加. 若未充分验证数据源, 容易引入不可靠数据, 甚至遭遇投毒攻击, 进一步降低数据可信性[110,111]. 相关研究主要有面向采集过程和面向数据内容两种思路.

- 面向采集过程的方法通过提升采集流程的安全性来增强数据可信性. 例如, Zhang 等人[112]提出的 Town Crier 系统, 通过多数据源比对和 SGX 硬件隔离, 确保数据在采集和验证过程中的完整性, 并为智能合约提供可验证的数据来源. 该方法保障了采集过程的可信, 但无法验证数据内容的真实性. 如果所有数据源被同一攻击者控制, TEE 也无法防御. 此外, 对硬件的依赖限制了其应用范围.
- 面向数据内容的方法侧重识别外来数据中的异常或恶意部分. 例如, Tran 等人[113]发现中毒样本在特征空间中具有谱特征的规律, 并据此利用统计工具识别并剔除异常数据, 以减轻数据投毒攻击的影响. 但相关研究[114]指出, 对于经过对抗性构造的数据, 该类方法易出现误判与漏检, 难以提供稳定的防御保障.

总体来看, TEE 方案和异常检测分别针对采集过程和数据内容提供防御. TEE 适合对数据链路完整性要求高的场景, 可信性强; 异常检测适合作为动态防御机制嵌入采集流程. 现有研究缺乏对外部数据源质量的系统建模, 未来可引入数据源声誉管理和历史行为建模等方法, 以提升外部数据可信性评估的可解释性和动态适应性.

4.1.4 小 结

本节围绕 3 类典型数据采集场景, 分析了其可信性挑战与应对策略. 总体来看, 不同场景下的数据采集可信保障有不同的技术路径和治理重点. 自动化设备采集主要依赖两类信任根: 一是以 PUF 为代表的硬件可信根, 实现静态身份认证; 二是基于区块链的分布式共识机制, 实现对设备动态行为的持续评估. 从可信演进的视角来看, 这代表了数据采集阶段正从单一的身份可验证向初步的行为可验证层级跨越.

在人工录入和第三方数据源场景, 治理逻辑从内容质量延展至行为责任和过程可验证性. 人工录入数据既要依靠自动化清洗等内容保障, 也需结合行为记录完善责任追溯. 第三方数据源则通过异常检测提升内容可信度, 同时加强过程完整性保护, 实现内容与过程的双重防护. 这种从源头建立的信任机制, 不仅是组织内部流通进行数据质量治理的基础, 也常被用于在数据交易场景以生成可验证的数据资产凭证.

综上, 数据采集阶段的可信保障, 本质是在数据流通起点建立可靠门槛. 未来应整合各类静态与动态技术, 构建覆盖设备、行为、内容等多维度的协同可信评估体系, 为数据流通和共享提供坚实基础.

4.2 数据传输阶段

在数据传输阶段, 核心问题包括传输路径的可追踪性和中转节点行为的可审计性. 前者要求能够还原数据流向, 后者需验证各节点操作, 防止篡改、丢弃或恶意转发. 现有方案多采用区块链、TEE 和 ZKP 等技术, 但在性能、开销及复杂环境适应性等方面仍有挑战. 同时, 提升传输透明性和可验证性虽然增加了信息记录, 但会带来用户隐私风险. 因此, 如何在保障系统可信性的同时保护用户隐私, 成为当前研究的关键, 本节围绕这些问题进行讨论.

4.2.1 传输路径追踪与行为审计

数据在传输时会经过多个中转节点, 其可信性不仅依赖于传输路径记录, 还取决于中转节点是否按协议正确操作. 这对于金融交易、医疗等高敏感场景尤为重要, 有助于审计、溯源和责任追溯. 然而传统网络协议缺乏对路

径和节点行为的结构化记录, 难以满足这些需求. 为此, 目前主要提出了如下两种不同的传输可信保障模式.

● 基于分布式共识的全局审计模式. 该模式利用区块链记录每次数据传输的路径, 例如, Dwivedi 等人[115]基于区块链, 利用智能合约对数据在各节点的传输操作进行记录, 并通过共识机制保障记录不可篡改, 实现数据完整性验证、节点认证与过程审计等功能, 提升整体传输系统的透明度与安全性, 适合需要多方协作、互不信任的场景. 但在高频数据传输下, 区块链在路径记录和节点行为验证方面可能面临性能和扩展性瓶颈.

● 基于硬件隔离的节点级证明模式. 该模式采用 TEE 技术, 使每个中转节点在受硬件保护的环境中操作, 并生成可验证的行为证明. 例如, Liu 等人[116]提出的 TEE 可验证传输记录系统, 通过节点间相互记录形成服务记录链, 实现操作合规性共识, 提升系统效率和扩展性. 相比区块链, 该模式延迟更低、实时性更强, 适合高吞吐量和高效率场景, 但高度依赖特定硬件平台, 且部署与维护成本较高, 在面对侧信道攻击等安全威胁时仍存在风险.

对比来看, 区块链和 TEE 都能实现数据传输的可审计性, 但侧重点不同. 区块链强调全局一致性和可溯源性, 适合多方协作场景; TEE 关注节点级行为证明, 兼顾效率和实时性, 更适合对性能要求较高的系统. 两者在扩展性和性能上差异明显. 未来可探索将区块链的审计能力与 TEE 的高效执行相结合, 构建链下执行、链上验证的混合架构, 实现性能与可审计性的平衡.

4.2.2 隐私保护矛盾

虽然区块链和 TEE 提升了传输路径的可追踪性和节点行为的可审计性, 但在记录和验证过程中不可避免涉及用户敏感信息, 存在隐私泄露风险. 因此, 如何在实现可审计性的同时保护用户隐私仍是关键挑战. 现有研究提出多种技术路径, 本节主要介绍两类典型机制: 匿名可审计机制和链上隐私增强机制.

● 匿名可审计机制. 该机制旨在在实现可追责和行为验证的同时, 最大限度隐藏用户身份或数据内容. 例如, Li 等人[92]在供应链场景中结合联盟区块链、零知识证明和 TEE 智能合约, 实现了数据传输的隐私保护与可审计性, 适合隐私和合规要求高的场景, 但系统复杂度和性能开销较大. 另一方面, Li 等人[117]提出的去中心化门限签名方案, 通过动态追踪和零知识证明, 实现隐私保护下的动态可追责, 适用于政务、金融等重视身份保护和行为可控的场景, 但对密钥管理和系统同步要求较高.

● 链上隐私增强机制. 部分研究尝试从链上结构层面提升隐私性, 例如, Guo 等人[118]设计了一种基于图生成网络的隐蔽交易保护方法, 有效公开区块链下的隐私保护交易. 该类机制具有轻量化、无需额外硬件的优势, 适用于区块链场景, 但在通用性等方面存在一定局限.

从身份和数据的角度来看, 匿名可审计机制强调在保护用户敏感信息的同时保留系统审计能力, 是重要研究方向; 而从系统层面的角度来看, 链上隐私增强机制则提供了一种轻量化的补充路径. 未来研究可探讨两类机制的融合与互补, 以进一步兼顾可验证性和隐私保护.

4.2.3 小 结

在传输路径追踪和行为审计方面, 当前研究主要包括基于分布式共识的全局审计模式 (区块链方案) 和基于硬件隔离的节点级证明模式 (TEE 方案). 区块链方案适用于多方协作、互不信任的场景, 强调全局可追溯和不可篡改; TEE 方案侧重本地操作可验证性和高效处理, 更适合对性能和实时性要求高的应用. 两者各有优劣, 需结合实际需求进行权衡和集成. 这两种机制虽然实现方式不同, 但本质上都是为了解决中转节点的行为可验证问题, 确保数据流通过程的透明与合规.

在隐私保护方面, 零知识证明、门限签名和链上结构优化等方法在兼顾可审计性和用户隐私方面取得一定进展, 但在系统复杂性、性能和通用性上仍有挑战. 不同机制侧重点不同, 目前尚无统一技术路线.

总体来看, 数据传输阶段的可信保障正逐步走向融合多种安全机制的复杂系统, 未来研究需进一步提升性能和隐私保护的平衡能力, 不断完善混合架构和适应复杂网络环境的可用性.

4.3 数据存储阶段

数据存储阶段的可信性, 主要关注存储数据的生命周期记录和状态正确性, 具体包括 3 个方面: 一是数据变更可追溯性, 确保每次修改都有记录可查; 二是存储内容完整性, 防止数据被篡改或丢失; 三是分布式环境下的数据

一致性, 确保各副本状态同步. 针对这些问题, 已有多种解决方案被提出, 但在性能优化、存储开销和系统复杂性等方面仍存在挑战. 本节分析当前主要的可信性问题及其对应的解决方案.

4.3.1 数据变更可追溯性

在存储系统中, 数据通常会经历多次修改, 因此变更的可追溯性是保障数据可信性的重要要求. 实现可追溯性需要记录数据内容的修改记录以便后续审计和责任追踪. 然而, 一些存储系统本身不直接支持版本追踪和修改记录. 为应对这一挑战, 一种有效的设计思想是将数据存储平面与行为审计平面进行解耦和分层.

在这种分层架构下, 研究者利用区块链技术构建独立且不可篡改的审计平面. 例如, Nyaletey 等人[119]将文件内容存储在 IPFS 等系统中, 将文件操作和变更记录写入区块链, 形成可追溯的审计链, 实现了对存储全过程的追踪. 区块链的核心价值在于记录和验证数据写入、修改、删除等操作, 生成可验证、不可篡改的日志, 适用于对透明性要求高的场景. 然而, 该方法面临存储膨胀和吞吐瓶颈等问题, 尤其在高频更新或大规模存储下, 性能成为主要挑战. 未来可通过链下记录和分层结构等方式优化其在大规模系统中的适用性.

4.3.2 存储内容完整性

在数据存储阶段, 数据完整性是可信存储的重要因素. 分布式和云环境下, 用户无法直接验证服务商是否正确存储数据, 存在数据被篡改或丢失的风险. 当前相关研究主要基于如下两类不同的信任根探索可验证存储问题.

- 基于数学难题的密码学证明. 这是一类常见的可验证存储方法, 通过密码学协议, 用户或第三方可以向存储服务器发起挑战, 服务器需生成有效凭证以证明数据完整性. 例如, Anthoine 等人[120]提出了一种基于有限域上随机线性代数验证方案的新型动态可检索性证明方法, 这一方法具有公开可验证性, 能够确保用户和任意第三方能够验证数据在存储过程中是否被篡改. 该方案安全性较强、无需信任第三方, 但计算与通信开销较大.
- 基于物理隔离的硬件证明. 该方案利用 TEE 将数据完整性验证逻辑放在受硬件保护的 enclave 中, 简化了设计并提升性能. 例如, Zhou 等人[121]利用 TEE 的硬件安全特性实现高效的数据完整性验证, 并降低了用户侧的计算负担. 该方法在保障存储可验证的同时显著降低了用户侧计算负担, 并简化了协议设计. 然而, TEE 本身存在潜在的硬件漏洞风险, 且对部署条件要求较高, 难以在大范围异构硬件环境下推广.

总体来看, 可验证存储能有效保障数据完整性, 适用于不可信云环境. 密码学方案安全性强, 无需信任第三方; 硬件方案在性能和易用性方面有优势. 未来可探索软硬件协同机制, 在保证验证能力的同时降低资源消耗.

4.3.3 分布式环境下的数据一致性

在多节点的分布式存储系统中, 数据一致性是实现可信保障的基础, 如果系统在节点故障、网络分区或并发访问时无法确保各副本最终状态一致, 任何可信性保障都无从谈起.

为解决这一问题, 以 Paxos[122]、Raft[123]等为代表的一致性协议被广泛应用, 这类协议通过选举主节点和日志复制等机制, 以保证分布式存储系统的强一致性[124]. 一致性协议是分布式存储可信的核心技术, 理论成熟、应用广泛. 然而, 如何兼顾一致性保障与系统性能, 仍是核心挑战. 未来可关注协议的轻量化和模块化设计, 实现高效且可信的数据一致性.

4.3.4 小 结

本节从数据变更可追溯性、存储内容完整性和分布式环境下的数据一致性这 3 个方面分析了数据存储阶段面临的可信挑战. 总体来看, 现有技术主要展现出以下 3 个特点.

1) 分层与解耦的系统架构成为应对复杂可信需求的重要设计方向. 通过划分独立的审计平面与数据平面, 实现功能上的分工与协作, 有助于提升系统的灵活性和可维护性.

2) 关于信任根的选择, 不同方案在数据完整性保障上分为依赖数学证明和依赖硬件证明两类路径. 信任根的不同, 直接影响系统的安全性、性能表现及实际部署方式, 是该领域方案设计时的重要权衡因素.

3) 以数据一致性协议为核心的分布式系统基础理论, 为可信存储提供了坚实支撑. 相关协议的工程化实现与优化, 直接决定了上层机制的可信性与可用性.

综上, 可信存储正逐渐从单一技术手段演进为多技术协同、层次分明的系统工程, 推动该领域向更高水平发展.

4.4 数据处理阶段

数据处理阶段的可信性问题包括算法可信性和参与方行为可信性. 前者关注算法在偏见、干扰或不透明情况下的稳定性与可解释性, 后者关注多方协作中如何防止恶意方行为. 如果这些问题无法有效解决, 不仅会影响处理结果的正确性, 还会削弱用户对系统的信任. 目前, 研究主要通过算法可解释性、零知识证明和区块链等方法应对, 但在实际应用中仍面临性能开销大和实现复杂等难题.

4.4.1 算法可信性

数据处理算法, 尤其是复杂的机器学习模型, 其可信性主要面临两大挑战. 一是黑盒问题, 即模型决策过程不透明, 难以获得信任; 二是脆弱性问题, 模型在特定输入下可能输出严重错误. 例如, Hendrycks 等人[125]提出了一种对抗性过滤技术, 通过筛选真实样本, 揭示了计算机视觉模型在自然场景中的脆弱性, 这种脆弱性导致模型在特定输入下输出错误结果. 为此, 研究者从可解释性与鲁棒性两个角度出发, 提出多种可信性增强方案.

在提升可解释性方面, 相关技术致力于揭示算法的决策依据, 增强模型的透明度. 例如, Nohara 等人[126]提出了一种基于公平利益分配理论的 Shapley 加性解释方法, 解释了梯度提升决策树模型, 揭示了特征与结果之间的潜在关系, 提高算法可信性. 针对模型脆弱性, 研究者聚焦于提升算法的鲁棒性, 即抵御对抗性攻击的能力. 例如, Levi 等人[127]提出了一种通用方法, 能够在分类器自然精度几乎不受影响的情况下大幅提升鲁棒性.

虽然相关理论和工具不断进步, 但在实际应用中, 可解释性、鲁棒性和性能三者往往难以兼顾. 提升可解释性通常需要更简单但性能较低的模型, 而增强鲁棒性的方法往往也会增加计算开销, 还可能会降低正常情况下的模型性能, 未来, 如何根据不同场景需求按需平衡, 构建可信的数据处理框架, 将是算法可信性研究的重要方向.

4.4.2 参与方行为可信性

● 在数据处理的协作场景中, 参与方之间可能存在恶意行为, 威胁数据处理的正确性和公平性. 例如, 恶意的计算方可能通过篡改计算逻辑或伪造计算结果, 直接干扰协作结果的正确性, 从而损害其他参与方的利益. 为应对这一挑战, 现有研究提出并应用了多种先进技术. 根据其核心验证目标的不同, 这些技术方案主要分为针对计算结果正确性、计算环境可信性以及协作历史不可篡改性的不同方向, 其对比如表 7 所示.

表 7 多方协作中处理行为可信保障技术对比

技术类型	验证目标	信任根	隐私保护能力	性能与成本	优势	核心挑战	适用场景
零知识证明	计算结果正确性	数学难题	高, 可在不泄露输入的前提下验证结果	计算和通信开销高, 生成与验证耗时, 难以满足高频实时场景	强隐私保护, 数学可证明, 适用多种计算验证	适用范围受限、性能瓶颈、复杂电路难表达	复杂计算外包、隐私计算、深度学习等
可信执行环境	计算环境完整性	硬件厂商	中, 依赖硬件隔离, 明文计算, 外部不可见	需专用硬件, 硬件成本高, 计算性能较好但受内存等资源限制	支持实时处理, 易于集成, 适用多用户云环境	依赖硬件、受侧信道攻击威胁、部署复杂	云计算、边缘计算、数据处理服务
区块链	协作历史不可篡改	分布式共识	低, 仅记录操作流程, 需结合额外隐私技术	共识延迟高, 链上存储成本大, 吞吐有限, 难适应高频操作	全流程透明、不可篡改、支持审计与追责	性能瓶颈、隐私保护依赖外部机制、可扩展性受限	过程审计、多方协作等

● 针对计算结果的正确性验证, ZKP 和可验证计算 (verifiable computation, VC) 技术被广泛使用, 它们允许数据持有方在不泄露隐私数据的情况下, 向其他方证明计算结果的正确性. 例如, Sun 等人[128]利用 ZKP 验证深度学习训练的正确性, 实现在保护数据和模型隐私的同时, 证明神经网络训练过程的合法性. 然而 ZKP 的计算和通信开销较大, 生成和验证证明耗时较长, 且通用性受限于电路表达能力, 难以满足高频或实时场景需求. VC 进一步扩展了 ZKP 的能力, 允许数据持有方验证计算方是否按照约定的逻辑正确执行了计算. 例如, Fiore 等人[129]通过引入支持非确定性计算的同态签名, 实现了在流式认证数据上的隐私保护可验证计算, 其性能在滑动窗口统计等场景下显著优于现有方法. 相比 ZKP, 该方法在数据更新频繁的场景下表现更加高效. 但 VC 也存在局限, 如预处理步骤带来额外开销, 同时在处理动态参与方和复杂协作逻辑时的灵活性有待提升.

● 针对计算环境的可信性问题, TEE 技术为保障计算环境可信提供了根本手段. 例如, Chen 等人[130]提出了一种机密计算即服务 (confidential computing as a service, CCaaS) 方案, 通过硬件隔离机制确保计算逻辑未被篡改, 并

利用被遗忘证明机制, 在任务完成后证明服务提供商已清除用户数据, 从而增强用户隐私保护. 该方法实际可部署性较高, 适用于多用户云计算环境. 针对数据处理服务结果的真实性, 张溯等人[131]提出了一种基于远程证明的处理服务完整性验证方法, 使用 TEE 对代码、执行过程和结果进行度量与验证, 保障了计算环境的可信性. 然而这类方法依赖于硬件平台, 且易受侧信道攻击等威胁.

● 为实现协作历史的不可篡改性, 多方协作体系引入区块链技术. 区块链通过记录每一步协作操作, 实现全过程的透明和不可篡改, 支持计算处理的全流程审计, 有效防止计算方的恶意行为. 例如, Peng 等人[132]提出了一种基于区块链系统的可验证和可审计联邦学习框架, 通过委员会聚合模型以及在区块链上记录可验证证明, 实现模型训练过程的可验证性和可审计性, 为联邦学习系统提供可信保障. 该框架适用于模型更新不频繁、节点可信度可控的场景, 但在节点频繁变更或高频模型更新时, 链上记录会遇到性能瓶颈. 此外, Zhang 等人[133]通过结合基于同态加密的投标比较电路、ZKP 以及密码学承诺, 提出一种基于区块链的密封投标方案, 确保了投标过程的可信性. 但该方案设计复杂, 涉及多种密码组件, 难以在通用数据处理场景中直接复用. 针对复杂多方交互中的公平性与原子性难题, 张明武等人[134]提出基于国密 SM2 算法的多方链式适配器签名方案, 通过预适配签名算法将授权与秘密值绑定, 并在链式结构下实现了安全传递与交互. 在保障多方协作公平性的同时, 具备更高的计算效率与可扩展性, 为跨链交易和协作审计提供了自主可控的技术支撑.

综上所述, 不同验证技术针对参与方行为提供各自特定的安全保障, 从计算结果、计算环境到协作历史, 形成了多层次的可信体系. 这些机制在可信性、隐私保护和性能开销之间存在明显权衡. 未来研究应关注于提升机制的集成、适配性和可配置性方面, 构建灵活配置信任的协同计算系统, 以适应复杂多变的参与方和协作逻辑.

4.4.3 小 结

本节围绕数据处理的可信性问题, 从算法与处理参与方两个层面进行分析, 相关研究主要具有以下两大特征.

1) 在算法可信性方面, 针对黑盒和脆弱性问题, 可解释性和鲁棒性提升技术被广泛探索. 但这两者与算法性能之间常存在难以平衡的权衡, 如何根据应用场景实现合理取舍, 成为重要议题.

2) 在参与方行为的可信保障方面, 呈现出分层验证体系. 从计算结果的正确性、计算环境的完整性到协作历史的不可篡改记录, 各类方案根据不同目标协同应用, 展现出深度融合趋势. 这种分层体系映射出验证深度的递进, 即环境完整性保障了行为可信, 而结果正确性验证则进一步实现了内容可信的核心.

综上, 数据处理阶段的可信保障正逐步从关注单一维度演进为多目标、多层次, 且充满复杂权衡的系统工程. 未来的研究突破依赖于在降低系统开销的前提下, 实现算法可信性和参与方行为可信性的协同提升.

4.5 数据发布阶段

数据发布阶段的核心可信问题在于证明发布数据的真实性. 发布过程中, 数据可能因伪造、篡改或来源不明而降低可信度, 不仅影响数据使用者的信任, 还可能对下游任务造成误导. 为解决这一问题, 现有研究主要有两种路径: 一是利用密码学机制直接验证数据发布者身份和数据属性; 二是借助外部可信源进行验证.

4.5.1 直接验证机制

直接验证机制旨在不依赖任何外部实体, 仅通过密码学协议来完成数据真实性的自证. 其中又可以细分为对发布者身份和发布内容属性这两个维度的证明.

● 针对发布者身份的验证, 数字签名技术已成为解决数据发布者身份验证问题的成熟手段. 通过为数据附加数字签名, 能够确保数据来源的可靠性, 还能防止篡改. 作为可信数据发布体系的基础, 数字签名已获得广泛应用.

● 针对发布内容属性的验证, ZKP 技术为证明数据属性提供了有力手段, 使数据发布者能在不泄露具体内容的情况下证明数据的某些属性, 提升真实性验证的便利性. 例如, Wan 等人[135]提出基于扩展 Zk-SNARK 协议的 Zk-AuthFeed, 实现了零知识认证的链下数据输入, 保障了区块链应用中的数据隐私和真实性. 但在大规模或数据频繁更新、属性复杂的场景下, 生成和验证开销较高, 系统性能成为瓶颈. 未来可进一步探索轻量化 ZKP 协议与可配置属性证明技术, 以提升其在通用数据发布场景中的实用性与灵活性.

4.5.2 外部验证机制

当直接验证机制不足以建立信任时, 引入外部实体进行验证成为一种重要补充. 这一路径清晰地展现了信任

模型从中心化向去中心化的演进.

可信第三方 (trusted third party, TTP) 认证是一种中心化的认证机制, 依赖权威机构或可信平台提供数据真实性的第三方证明, 为数据的真实性背书. 例如, 可信时间戳技术通过向数据添加时间戳并签名, 证明数据在特定时间点的存在性和完整性[136]. 然而 TTP 的可信性高度依赖于认证机构, 缺乏透明性, 一旦认证机构遭受攻击或面临利益冲突, 其认证结果的可靠性可能会受影响. 去中心化预言机技术旨在解决区块链场景中链外数据的真实性问题. 由于区块链本身无法直接访问链外数据 (如天气、市场价格等), 预言机系统通过引入外部数据源, 提供了一种可信的数据输入方式.

随着区块链技术的发展, 为解决链上智能合约如何安全地与链下真实世界数据交互的问题, 预言机应运而生. 它旨在用一个去中心化的节点网络, 来取代单一的 TTP. 早期的工作例如 Zhang 等人[137]允许用户在无需可信硬件或服务器端修改的情况下, 证明通过 TLS 协议访问的数据确实来自某个特定网站, 而不暴露数据的具体内容. 而以 Chainlink 2.0[138]为代表的目前应用较为广泛的去中心化预言机网络, 利用多指标信誉系统和押金机制管理网络中的预言机, 并且支持可信执行环境的接入, 从而提升了链上数据输入的可信性. 然而去中心化预言机涉及多个节点的共识, 导致其验证性能不足, 尤其在需要高频数据的场景中.

总而言之, 外部验证机制经历了从信任单一权威到信任密码学证明与共识的深刻模式转变, 如图 7 所示. 未来研究可进一步探索融合去中心化机制与轻量化共识协议, 以缓解预言机在非区块链环境中的适配难题, 并提升其在高频、实时数据发布场景下的验证效率与通用性.

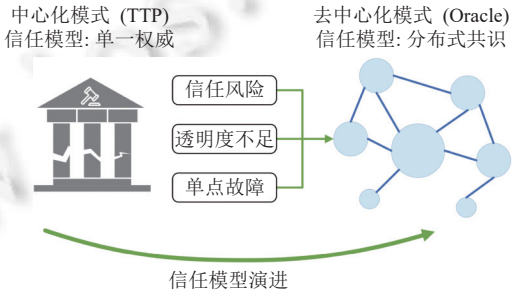

图 7 外部数据真实性验证机制演进

4.5.3 小 结

本节围绕数据发布阶段的核心可信问题进行了系统梳理. 目前, 相关技术主要聚焦于两类代表性方案, 分别为直接验证机制和外部验证机制, 各自展现出不同的发展重点.

直接验证机制方面, 技术实现已经从传统的身份认证扩展到对数据内容属性的隐私保护验证. 这类方案不仅能够明确数据的发布主体, 还可以在不泄露原始数据的前提下, 证明数据满足特定属性, 这意味着可信技术已突破了身份与行为的范畴, 迈入数据内容可验证的阶段, 从而提升可信发布体系的完整性和灵活性.

外部验证机制方面, 基于第三方的验证机制则经历了从中心化权威到去中心化共识机制的重要转变. 这种信任模型的变革增强了数据发布的公开性和抗篡改能力, 重构了以数据交易与数据共享为代表的弱信任场景下的信任模型, 使得接收方无需完全信任发布主体即可验证数据真实性, 但同时也带来了性能开销和系统复杂性等新的挑战, 成为当前研究需要重点突破的瓶颈.

综上, 数据发布阶段的可信保障正向着更全面、更去中心化的方向发展, 同时也面临着更高的复杂性和成本压力. 未来, 高级密码学技术与高效共识机制的创新, 将成为推动该领域进一步发展的关键动力.

4.6 数据溯源阶段

数据溯源阶段通过记录元数据, 追踪数据的起源、流通和变换过程, 其可信性对数据流通安全至关重要. 此阶段的核心问题不再是数据本身, 而是元数据的可信性, 主要包括 3 大挑战: 一是元数据真实性, 即如何防止操作历史被伪造; 二是数据血缘完整性, 确保复杂变换后血缘链不断裂; 三是隐私保护与溯源透明度的冲突, 既要实现可

追责, 又要保护敏感信息. 本节围绕这 3 方面综述研究进展, 并探讨未来方向.

4.6.1 元数据真实性保障

作为描述数据属性和操作历史的关键载体, 元数据的真实性是数据溯源可信性的基础. 在数据流通中, 攻击者可通过伪造操作者身份、篡改时间戳或解耦元数据与数据实体的关联, 导致溯源记录失效. 因此, 如何确保元数据与实体操作行为的强关联性成为关键挑战. 现有研究主要采用两种技术路线来实现元数据真实性保障.

一种技术路线是基于密码学协议构建逻辑可信路径, 通过数学可验证方式保障元数据的生成和关联安全. 例如, Yang 等人[139]提出 Dasein 验证框架, 利用改进的默克尔树进行内容验证、可信时间戳保证时间、多层签名实现主体认证, 支持全流程可信溯源. 但该方法依赖多层签名和时间戳协调, 计算与管理开销大, 跨平台扩展性较差. 在数据交易场景中, Liu 等人[140]基于 ZKP 构建数据可用性验证体系, 允许买方在交易前验证数据真实性. 但 ZKP 的生成和验证成本较高, 尤其在数据结构复杂或频繁更新时, 系统响应能力成为瓶颈. 此外, 这类密码学方案还面临高计算开销、量子威胁和跨系统互操作性差等局限.

另一种技术路线是基于可信硬件的环境可信路径, 侧重于通过物理隔离和硬件安全特性, 保证元数据生成环境的可信性. 例如 Weng 等人[141]针对机器学习中的被遗忘权问题, 在 SGX 可信执行环境中用认证数据结构追踪数据并生成可验证证明, 但部署成本高且存在侧信道攻击风险. Aman 等人[142]采用 PUF 作为可信根构建认证协议, 实现可信溯源, 该方法硬件开销低、唯一性强, 但长期稳定性易受噪声干扰, 存在工程化难题.

综上, 基于密码学的逻辑可信和基于 TEE 的环境可信从不同层面提供支持. 前者灵活但计算开销大, 后者高效但依赖硬件, 未来可进一步协同设计密码学与硬件机制, 提升真实性验证的安全性、性能与适应性.

4.6.2 数据血缘完整性验证

数据血缘记录了数据全生命周期的变换轨迹, 是追溯数据问题的重要依据. 但在数据流通过程中, 聚合、脱敏、特征提取等非线性操作会导致传统哈希或水印技术难以追踪变换后的血缘关系. 例如, 在 AI 训练中, 若无法验证训练数据与模型的关联, 就难以溯源模型偏见. 因此, 如何验证复杂流通场景下的血缘完整性, 成为数据溯源可信性的关键难题. 目前主流数据血缘技术分为两类: 侵入式追溯技术和非侵入式分析技术, 对比如表 8 所示.

表 8 数据血缘追踪技术对比

技术类型	核心原理	对原始数据影响	应用部署依赖	优势	核心挑战	适用场景
侵入式追溯	直接修改数据本身, 植入难以察觉的标识	有损, 对原始数据进行微小修改, 可能影响效用	部署灵活, 无需依赖特定平台或代码	鲁棒性强, 支持可验证追溯	数据效用损失与溯源强度需权衡	数据外包、社交网络、AI训练数据溯源
非侵入式分析	观测系统行为、静态分析或运行时监控推断数据关系	无损, 并不改变原始数据	依赖中心化平台或完整代码访问, 需要系统支持	无损、部署成本低、适应性强	依赖中心化平台、难适应跨域分布式环境	分布式计算、云数据平台等

● 侵入式追溯技术: 对数据本身进行微小且难以察觉的修改, 实现可追溯性. 与发布阶段利用水印追踪泄露不同, 此处的水印具有更复杂的语义, 旨在携带数据变换历史或逻辑证明, 以验证数据在多跳流转后的血缘完整性. 例如, Backes 等人[143]提出的 LIME 框架, 利用鲁棒水印来保证数据即使经过非线性变换仍可提取标识, 并结合不经意传输和签名协议, 实现在恶意环境下接收方的不可抵赖性, 适用于数据外包和社交网络等场景. Sablayrolles 等人[144]提出的放射性数据技术, 通过对训练样本进行不可感知的修改, 使模型在训练后携带可识别特征, 即使只标记少量训练数据, 也能高置信度检测模型是否使用过目标数据, 对数据增强和模型变化具有鲁棒性. 这类方法的共同挑战是对数据修改可能影响数据效用, 因此, 如何平衡溯源鲁棒性与数据价值是其核心难题.

● 非侵入式分析技术: 不修改数据本身, 通过观测和分析系统行为间接推断数据血缘. 例如, Chen 等人[130]在机密计算服务框架中, 利用 Rust 静态分析工具 MIRAI 分析数据标签, 追踪机密数据在系统内的流通, 无需修改数据, 但依赖控制流分析, 可能遗漏部分路径. Tang 等人[145]通过监听分布式平台的运行时事件, 粗粒度捕获数据与处理过程的关联, 基于系统行为构建血缘图谱, 追踪数据流通路径, 具有部署成本低、适应性强的优点. 这类方法的主要局限在于对中心化平台或特定环境的依赖. 静态分析需要完整源代码, 运行时监听通常要求中心化、可观

测的平台, 难以适用于跨组织、异构的分布式场景.

当前数据血缘技术主要分为侵入式和非侵入式两类. 侵入式方案溯源鲁棒性和可验证性强, 但可能带来数据效用损失; 非侵入式方案对原始数据无损、部署灵活, 但依赖中心化平台或运行时分析, 难以适应跨域和动态环境. 未来, 侵入式方案可探索可调控扰动强度和低损鲁棒标识, 以兼顾溯源能力和数据价值; 非侵入式方案可探索跨平台和去中心化机制, 提升跨域流通环境下的血缘完整性验证能力.

4.6.3 隐私保护与可控溯源

数据溯源过程中, 隐私保护与溯源透明度存在矛盾. 一方面, 《中华人民共和国个人信息保护法》等法律法规要求数据匿名化, 但可能导致溯源信息丢失; 另一方面, 完整的溯源记录又可能泄露敏感信息. 因此, 如何在隐私增强技术下实现可控溯源, 成为平衡数据价值与安全的关键. 针对这一矛盾, 学界探索了隐私保护的数据溯源机制.

早期的隐私保护溯源机制主要通过密码学协议实现严格隐私保护. 例如, Li 等人[86]通过结合密码学承诺与不经意传输将用户私钥嵌入数据, 仅授权实体能够提取解密, 实现隐私保护的溯源. Canovas Sanchez 等人[95]采用匿名凭证和非交互式零知识证明, 既保护隐私信息, 又允许授权实体依法解密追溯. 这类方案能提供强有力的隐私安全保障. 但由于保护策略静态预设, 灵活性不足, 难以适应复杂、动态的溯源需求.

一些研究探索了更为灵活的治理模式, 通过量化方式平衡隐私保护与溯源透明度. 例如 Deutch 等人[146]形式化了溯源信息效用与查询隐私泄露的权衡, 提出溯源抽象化方法, 利用匿名技术评估隐私强度, 从而在数据可用性与隐私保护之间找到最优平衡. 该模型首次对溯源效用和隐私泄露的权衡进行量化, 为理论研究提供了基础. 但该类方案多基于静态、理想化假设, 在动态数据、多跳查询等复杂场景下支持有限, 实际应用较少.

总体来看, 隐私保护与可控溯源的治理正从静态、刚性走向动态、弹性权衡. 未来应围绕动态策略和最小披露原则, 结合隐私-溯源权衡分析, 构建支持跨主体和多跳查询的可控溯源, 促进隐私保护与可控溯源深度融合.

4.6.4 小 结

本节分析了数据溯源阶段的 3 大可信挑战. 首先, 在元数据真实性保障方面, 现有技术分为基于密码学协议的逻辑可信和依赖可信硬件的环境可信, 两者在信任基础、性能和部署灵活性上各具优劣, 未来有望通过融合实现更优的安全性和适应性.

在数据血缘追踪上, 研究主要包括侵入式和非侵入式两种方式. 侵入式提升溯源鲁棒性, 但可能影响数据效用; 非侵入式对数据无损, 但受限于实现环境. 如何平衡鲁棒性和适用性是该领域的关键难题. 在隐私保护方面, 随着溯源透明性与隐私矛盾加剧. 研究从静态、刚性的访问控制转向动态、可量化的隐私-效用权衡模型, 推动隐私保护成为系统性、全局性的问题. 这种全流程的溯源体系, 既能支撑数据跨境流通中的合规审计, 也是解决数据交易中确权与纠纷仲裁难题的关键手段.

总体来看, 数据溯源的可信保障正成为密码学、硬件安全、数据科学和治理理论等多领域交叉的研究前沿. 未来突破将依赖于在保障强安全性的同时, 实现高效、灵活、智能的协同溯源体系设计.

4.7 总 结

本节将数据采集、传输、存储、处理、发布和溯源这 6 个阶段的可信性挑战、现有技术方案及尚待解决问题汇总于表 9. 在各阶段的可信技术中, 部分手段具备一定的溯源能力, 但仅用于本阶段自身, 不构成跨阶段的完整溯源体系. 而本文所定义的溯源阶段是面向全链路的统一追踪, 与这些局部机制在范围与作用上均不同.

表 9 数据要素流通各阶段可信问题、现有研究工作以及待解决问题

流通阶段	问题	研究工作	技术路线	典型时间复杂度	待解决问题
数据采集	采集设备可靠性	[106]	设备防伪造	PUF响应O(1)	大规模场景下受指纹稳定性与跨设备认证同步限制
		[107,108]	区块链信任评估	信任值计算O(1)+区块链O(共识)+信任值查询O(1)	受共识开销与设备行为暴露导致的隐私与性能瓶颈制约
	采集数据真实性	[109]	数据校验	依赖校验方法, 通常为O(n), n为数据长度	依赖专家经验, 跨场景适配性不足

表 9 数据要素流通各阶段可信问题、现有研究工作以及待解决问题 (续)

流通阶段	问题	研究工作	技术路线	典型时间复杂度	待解决问题
数据采集	采集数据真实性	[86]	区块链数据存证	存证O(共识), 证据取回O(1)	高频写入下易出现链上吞吐瓶颈
		[112]	TEE保护的多数据源对比	进出enclave固定开销O(1)+具体执行开销O($f(n)$), f为TEE中运算	适用范围受限, 且TEE技术存在侧信道攻击和高成本问题
		[113]	数据异常检测	依赖检测模型, 例如SVM为O(nd), n为数据长度, d为特征维度	难以抵御经对抗性构造的恶意数据
数据传输	传输路径追踪与中转节点审计	[115]	区块链传输审计	写入O(共识)+审计O(k), k为相关链上记录数量	在高频传输下存在链上写入瓶颈与扩展性不足
		[92,116]	TEE保护的中转节点行为记录	进出enclave固定开销O(1)+具体执行开销O($f(n)$), f为TEE中运算	易受侧信道攻击、硬件漏洞影响, 高部署成本
数据存储	数据变更可追溯性	[119]	区块链审计	写入O(共识)+审计O(k), k为文件相关链上记录数量	高频数据变更场景下链上写入开销显著
	存储完整性验证	[120]	密码学数据完整性证明	读操作O(log$n$)+写操作O(log$n$)+审计O(n), n为数据长度	计算与通信开销较高, 高频审计场景网络负担显著
		[121]	TEE保护的存储完整性验证	进出enclave固定开销O(1)+具体执行开销O($f(n)$), f为TEE中运算	受硬件依赖与潜在侧信道风险限制, 难以在异构环境中大规模推广
	分布式存储一致性	[122,123]	强一致性共识协议	依赖协议, 例如Raft/Paxos (单次) O(n), n为节点数	受多轮通信与日志复制限制, 难以支撑高并发扩展
数据处理	处理算法可信性	[126]	算法可解释性提升	依赖具体方法, 与被解释模型的复杂度相关	解释结果受特征相关性与模型复杂度限制, 且可解释性与鲁棒性、性能难以兼顾
		[127]	算法鲁棒性提高	依赖具体方法, 显著增加模型训练时长, 而非一次性开销	在提升鲁棒性的同时难以避免对模型精度与开销的影响
	处理行为可信性	[128,129]	基于ZKP的计算结果正确性证明	通常, 生成O(n)+验证O(1) (例如Groth16), n为电路约束数量	计算与通信开销高, 难支撑高频或实时验证
		[130]	基于TEE的处理过程完整性保护	进出enclave固定开销O(1)+具体执行开销O($f(n)$), f为TEE中运算	易受侧信道攻击、硬件漏洞影响, 高部署成本
		[132–134]	基于区块链的可验证证明	写入O(共识)+验证O(1)	链上记录在高频协作下存在吞吐瓶颈, 方案复杂度高, 潜在隐私问题
数据发布	发布数据真实性证明	[135]	基于ZKP的数据真实性证明	通常, 生成O(n)+验证O(1) (例如Groth16), n为电路约束数量	生成与验证开销高, 难适应大规模与高频更新场景
		[136]	基于TTP的外部真实性证明	进出enclave固定开销O(1)+具体执行开销O($f(n)$), f为TEE中运算	中心化依赖强, 单点信任问题与透明性不足
		[137,138]	基于预言机的外部真实性证明	依赖预言机网络共识	多节点共识导致验证延迟高, 难以支撑高频数据输入
数据溯源	数据真实性验证	[139,140]	基于密码学的数据真实性验证	证明生成O(log$n$)+验证O(log$n$) (例如Merkle tree), n为已记录数据条数	多轮签名与证明带来高计算与管理开销, 跨系统扩展性受限
		[141,142]	基于硬件的真实性验证	远程证明O(n)+签名O(k^2)+验证O(k^2), n为测量数据长度, k为密钥长度(以TEE为例)	易受侧信道攻击、硬件漏洞影响, 高部署成本以及指纹稳定性问题
	数据血缘完整性验证	[143,144]	侵入式追溯	水印嵌入O(n)+水印提取O(n), n为数据长度	对数据侵入式修改可能影响效用, 难以平衡鲁棒性与数据价值
		[130,145]	非侵入式分析	依赖具体分析工具	依赖特定平台或完整代码, 可观测性受限、跨组织适用性不足
	隐私保护平衡	[86,95]	硬性隐私保护机制	数据加密O(n)+数据解密O(n), n为数据长度	静态策略难以应对复杂动态的溯源需求
		[146]	隐私-溯源平衡调控	O(($h\times l$)$^n\times q$), h为抽象树高度, l为叶节点数, n为被抽象的血缘变量数, q为判定复杂度	基于理想化假设, 难适应动态与多跳复杂场景

5 总结与展望

数据要素流通的安全与可信问题贯穿其全生命周期, 涉及数据采集、存储、传输、处理、发布和溯源这 6 个阶段. 本文围绕数据要素流通的不同阶段, 系统分析了各阶段的安全与可信性问题以及现有的研究进展和待解决问题. 综合第 1–4 节的分析, 多种关键技术在保障数据要素流通安全与可信中发挥着核心作用, 但它们在计算复杂度、通信开销及核心优势上各有侧重. 为直观展现其内在权衡, 表 10 对这些技术进行了横向对比总结. 本节进一步提炼数据要素流通的宏观发展路线, 剖析当前仍待解决的关键挑战, 并对未来研究方向进行展望.

表 10 安全与可信关键技术横向对比

技术类型	核心操作	计算复杂度	通信开销	主要瓶颈	优势与趋势
数字签名	密钥生成、签名、验证	低	低	密钥的安全管理; 后量子算法带来的签名尺寸和性能开销	提供基础性保障; 后量子密码、聚合/门限签名等是趋势
访问控制	策略定义、权限验证、访问决策	较低	低	静态策略难以适应动态需求; 复杂策略的管理和一致性维护	广泛适用性; 趋势是向动态、细粒度、情景感知的架构演进
同态加密	密文上的运算(加法/乘法)	极高	较低	密文计算、重加密/自举、噪声管理	强隐私保障; 算法优化和硬件加速是未来方向
联邦学习	本地模型训练、模型更新的安全聚合	高	高	通信效率、模型投毒、隐私推断等问题	实现隐私保护的协同机器学习; 与其他技术结合增强安全性是趋势
可信执行环境	硬件隔离区内的明文计算	低	较低	进出enclave的I/O、内存容量限制	性能高, 支持通用计算; 防御侧信道攻击是关键
物理不可克隆函数	基于物理特征生成唯一的设备标识	低	低	响应稳定性受环境影响 (温度、老化)	为物联网设备提供轻量级、低成本的防伪和身份认证; 提升稳定性是关键
零知识证明	生成/验证证明	高 (生成) 较低 (验证)	中	证明生成过程的计算与内存消耗	强隐私性与可验证性; 轻量化等是研究热点
可验证计算	外包计算、生成正确性证明、验证证明	高 (计算方) 低 (验证方)	较低	证明生成的开销较大; 协议设计通常针对特定计算类型	保证外包计算结果的可信性; 向更通用的计算场景发展
安全多方计算	多方间分布式加密协议交互	高	极高	多轮网络通信延迟、参与方数量	不依赖中心化可信方; 降低通信轮次是优化重点
区块链	共识算法、交易验证、智能合约执行	中	高	共识延迟、交易吞吐量瓶颈	去中心化信任、不可篡改; 分层、链下结合是扩展方向
可验证数据存储	标签生成、完整性证明	中	低	初始标签生成开销大; 仅保证完整性, 不保证机密性	高效验证远程数据完整性, 无需下载; 支持动态数据更新、与去中心化存储集成是趋势
差分隐私	对查询结果或数据添加噪声	低	较低	隐私预算分配、噪声与可用性的平衡	数学可证明的隐私; 提升可用性是重点方向
数字水印	水印嵌入/提取	较低	低	鲁棒、不可感知性和容量之间的平衡	为数据提供可追溯的身份标识; 抗攻击能力是研究热点
预言机	获取、验证并向链上提交外部数据	中	中	如何信任外部数据源; 去中心化带来的延迟和成本	连接区块链与现实世界的关键桥梁; 去中心化预言机网络是主流趋势
数据防泄漏	内容识别、行为监控、策略阻断	中	低	误报率和漏报率高; 难以防御物理泄露和精心设计的规避手段	工业界主流内部威胁和合规性解决方案; 结合AI提升检测精度是趋势

5.1 数据要素流通安全发展路线

基于对现有安全技术的系统性梳理, 本文验证了第 1 节提出的“三线分化、协同融合”的安全技术演进模型. 揭示了数据流通安全保障从传统密码学的单一基础防线开始, 为应对动态处理过程中的挑战, 逐步分化出隐私增强路线、硬件隔离路线以及分布式可追溯路线. 这 3 条主线并行发展, 各有侧重, 而未来的核心趋势是这 3 条路线的深度交叉与协同融合, 最终形成一体化的全链路安全保障体系 (如图 8 所示).

(1) 基础: 传统密码学与数据安全

这类技术是保障数据流通安全的基础, 主要解决数据在存储和传输过程中的机密性与完整性, 如对称/非对称

加密、哈希、数字签名和 TLS 等协议, 构成了数据安全的第 1 道防线. 但这些技术难以保障数据在计算和处理等动态环节中的安全, 因此推动了新技术的发展.

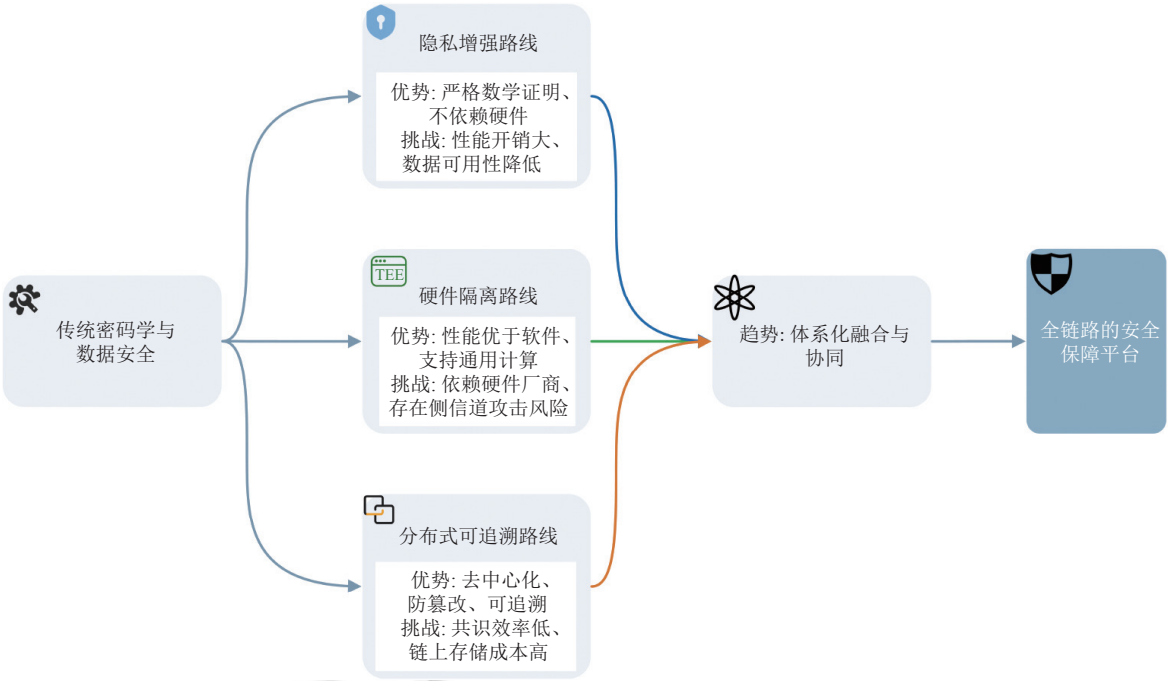

图 8 数据要素流通安全发展路线

(2) 并行路线: 从静态保护到动态保护

为了实现安全的数据流通, 发展出 3 条核心技术路线, 分别从不同维度应对动态流通过程中的安全挑战.

1) 隐私增强路线 (软件层面): 该路线以 HE、安全多方计算、ZKP 等密码学方法以及差分隐私等方法为代表, 实现数据的安全计算和分析. 其优点是严格的安全性且不依赖特定硬件, 但通常存在计算性能开销大或数据可用性降低的问题.

2) 硬件隔离路线 (硬件层面): 以 TEE 为代表, 通过建立物理隔离的安全区, 保障代码和数据的机密性与完整性. 性能优于纯软件方法, 并支持通用计算, 但安全性依赖于硬件厂商, 且存在侧信道攻击等风险.

3) 分布式可追溯路线 (架构层面): 以区块链、IPFS、数字水印等技术为代表, 利用去中心化等特性为跨主体、多环节的数据流通提供防篡改和防滥用能力, 解决多方协作下的信任问题. 但面临共识效率和链上存储成本等挑战.

(3) 发展趋势

未来的发展趋势是将多种技术路线深度融合, 构建覆盖数据全生命周期的协同安全体系. 例如, 软硬结合 (如在 TEE 中运行隐私计算协议, 兼顾性能与安全)、多技术协同 (如结合区块链溯源与加密水印泄露取证) 等. 最终目标是将各类安全能力整合, 形成全链路的数据流通安全保障平台. 现有研究已呈现出明显的融合特征, 具体表现为以下 3 个方面.

1) 区块链+TEE 实现链下计算与链上验证的融合: 针对区块链存储成本高、计算效率低的问题, 现有研究 (如区块链数据供给[112]、基于 TEE 的可验证传输记录[116]) 利用 TEE 在链下高效隐私地处理数据或验证数据源, 仅将计算结果或证明上链. 这种融合既保留了区块链的不可篡改性, 又利用 TEE 解决了性能瓶颈和隐私保护问题.

2) 联邦学习+隐私计算/区块链实现协同与隐私的融合: 单一的联邦学习仍面临梯度泄露风险, 而 Wei 等人[91]结合差分隐私与联邦学习, 在本地模型更新中添加噪声以防止隐私推断; Peng 等人[132]则结合区块链与联邦学习, 利用链上智能合约记录模型更新过程, 解决了中心服务器不可信及协作过程不可审计的问题.

3) 数字水印+密码学实现主动溯源与被动防御的融合: 针对传统水印易被移除、明文水印信息泄露的问题, 文献 [86] 将高级密码学技术与数字水印结合, 在数据中嵌入加密身份标识, 既保证了水印信息的机密性, 又实现了数据泄露后的责任追溯.

这些案例表明, 单一技术路线已难以应对复杂挑战, 技术融合正在成为解决性能-安全-隐私矛盾的主流路径. 然而, 这一融合过程必须克服异构技术间在信任假设、安全模型及性能开销上的内在冲突, 通过架构创新实现不同技术路线的优势互补而非简单的功能堆砌.

5.2 数据要素流通可信发展路线

针对可信问题, 通过对具体技术方案的纵深剖析, 本文进一步确证了第 1 节提出的“验证深度递进”发展模型, 揭示了数据流通中的可信需求遵循从表层到核心的演进路径, 即: 1) 身份可验证, 解决“你是谁”的问题, 是可信的基石; 2) 行为可验证, 解决“行为是否合规”的问题, 是过程透明的保障; 3) 内容可验证, 解决“数据本身及其声明是否为真”的问题, 是价值实现的最终要求. 如图 9 所示, 这 3 个阶段层层递进, 不仅描绘了技术发展的历史轨迹, 也为未来构建深度可信体系指明了方向.

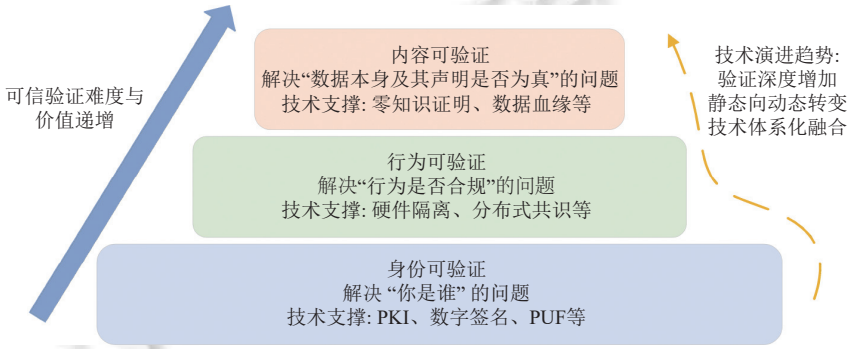

图 9 数据要素流通可信发展路线

(1) 身份可验证阶段

这一阶段的核心在于确保数据流通参与方 (如人、设备、系统) 的身份可信, 即解决“你是谁”的问题. 技术上主要依赖数字签名等密码学工具, 并通过可信第三方集中管理身份. PUF 等技术将身份认证延伸到物理层, 为物联网设备等提供更难伪造的硬件指纹.

但该阶段高度依赖中心化机构, 存在单点故障和信任风险, 且验证能力仅限于静态身份, 无法保障主体在动态交互中的行为可信, 难以满足复杂数据流转场景的需求.

(2) 行为可验证阶段

随着数据进入处理、发布等环节, 可信的焦点从静态身份扩展至动态行为, 核心问题转变为“行为是否合规”. 为解决这一问题, 发展出了两条主流技术路线.

● 基于硬件隔离的路线. 以 TEE 为代表, 通过隔离的安全区确保数据处理行为和逻辑严格按预定代码执行, 并可通过远程证明机制对外证实其行为的完整性. 该路线将行为的可信性锚定在硬件厂商提供的可信根上.

● 基于分布式共识的路线. 以区块链技术为代表, 将数据的关键操作记录在分布式账本上, 实现去中心化的过程审计, 并通过智能合约约束各方行为. 该路线将行为的可信性建立在多数参与者的共识和密码学保障之上.

此阶段显著提升了流通过程的透明度与可追溯性. 然而, TEE 面临硬件平台依赖与侧信道攻击等安全风险, 而区块链路径则受制于性能、可扩展性和治理复杂性等固有挑战.

(3) 内容可验证阶段

在身份与行为可信的基础上, 可信技术进一步发展到验证数据内容本身及相关声明的真实性, 尤其是在保护数据隐私的前提下. 零知识证明和可验证计算等前沿密码学技术, 使数据持有方能在不泄露隐私的情况下, 证明数

据来源、计算结果正确或满足特定属性. 数据血缘等溯源技术通过记录和追踪数据全生命周期的流转、处理与变换路径, 为数据内容真实性验证和溯源提供支持.

该阶段大幅提升了数据内容真实性的保障能力, 但仍面临挑战. 一方面, ZKP 和 VC 通常开销较大, 影响大规模或实时应用. 另一方面, 数据血缘等溯源系统需维护复杂链路, 易受链条冗长、存储压力和查询效率等问题影响. 提升验证效率、优化可扩展性, 并确保全链路可信, 是当前和未来的研究重点.

(4) 发展趋势

随着数据流通场景日益丰富和信任需求提升, 可信验证技术正向多层次、智能化和协同化方向发展. 未来, 这些技术将融合身份、行为和内容的多维验证能力, 构建高效、智能、自适应的数据可信流通协同体系, 更好地支撑复杂多变的数据流通环境.

5.3 安全与可信的协同与权衡

尽管本文第 3、4 节分别阐述了数据要素流通过程中的安全与可信技术, 但在数据要素流通的实际运行中, 二者呈现出依存互补与矛盾权衡并存的复杂辩证关系.

安全机制往往是构建可信系统的必要前提, 例如, 若缺乏加密与访问控制的保护, 数字签名便极易被伪造, 导致身份可信崩塌; 若缺乏 TEE 的内存隔离, 运行其中的验证逻辑便可能被篡改, 致使行为可信失效. 反之, 可信机制则是验证安全策略有效性的关键手段. 通过全链路溯源可以审计数据是否在非授权环境下被解密, 从而形成对安全防护的闭环验证. 二者在理想状态下应当形成安全保障可信、可信验证安全的良性循环.

然而, 在实现安全和可信的同时, 不同技术路线的融合却面临底层的冲突与权衡, 这种深层次的痛点主要体现在以下 3 个维度.

(1) 异构信任根的冲突

例如, 分布式可追溯路线 (如区块链) 的核心假设是去中心化信任, 通过多方共识消除对单一实体的依赖; 而硬件隔离路线 (如 TEE) 的信任根则锚定在硬件制造商这一中心化实体上. 当区块链与 TEE 结合 (如 TEE 预言机或链下计算) 时, 系统的整体安全性将发生木桶效应降级, 即原本去中心化的系统可能因 TEE 硬件层面的单点漏洞而导致全局信任崩塌. 如何在引入硬件效率的同时, 不破坏分布式系统的去中心化信任假设, 是融合架构设计的首要难题.

(2) 安全模型与功能目标的互斥

安全技术中的隐私增强路线往往采用概率性或模糊化模型, 而监管溯源路线则要求确定性的精确记录. 在数据发布阶段, 若采用差分隐私添加噪声来保护隐私, 可能会破坏数据水印或数字指纹的完整性, 导致溯源机制失效. 反之, 强可追溯性要求记录详尽的元数据, 这又可能与最小化披露的隐私原则相冲突. 这种隐私-溯源的博弈, 使得单一融合方案难以同时满足高强度的隐私保护与高精度的溯源.

(3) 实时要求与较低性能的矛盾

数据流通对实时性要求极高, 而高强度的安全技术往往伴随巨大的计算或通信开销. 例如, 同态加密和零知识证明虽然理论完备, 但其计算复杂度比明文计算高出数个数量级. 若将其直接通过智能合约集成到区块链上, 链上有限的计算能力与昂贵的 Gas 费用将成为不可逾越的瓶颈, 导致系统吞吐量急剧下降, 无法支撑大规模数据要素的高频流转.

5.4 关键挑战与未来研究方向

在安全可信的数据要素流通过程中, 仍然存在以下亟需关注和解决的主要挑战.

(1) 安全性与处理效率之间存在显著矛盾. 一方面, 基于密码学的方案难以在安全性与计算性能之间取得平衡; 另一方面, 区块链等可信保障技术在高吞吐量场景下面临性能瓶颈, 限制其实际应用.

(2) 现有方案仍面临安全攻击风险. 例如, TEE 虽然应用广泛, 但依然易受侧信道攻击和硬件漏洞影响, 威胁数据流通安全. 传统密码学算法受到量子计算的威胁, 而基于深度学习的数据异常检测、数据脱敏等方案也可能遭受对抗性攻击, 导致算法失效.

(3) 隐私保护技术在数据流通中面临隐私性与可用性之间的矛盾. 差分隐私、数据脱敏等方法虽然能保护隐私, 但往往会降低数据可用性. 区块链等技术在隐私保护方面也存在局限. 同时, 数据泄露后的追溯和责任界定较难, 现有泄密追踪机制还存在性能瓶颈.

(4) 现有数据可信性验证技术在适用性和透明性方面仍有挑战. 数据真实性验证常依赖专家经验或增加计算成本, 适用性不足; 算法和数据处理的可信性验证也受限于性能和硬件成本. 此外, 基于第三方的验证缺乏透明性, 难以完全满足可信需求; 基于预言机的验证则存在额外性能开销, 并需探索区块链以外的应用场景. 随着数据流通场景日益复杂, 参与实体不断增加, 安全与可信问题的解决方案需要具备更高的性能和适应能力, 并应进一步探索二者的协同机制.

未来研究可以从以下 5 个方向展开.

(1) 突破高开销密码学原语的计算与通信瓶颈

现有全同态加密在进行非线性运算时面临密文膨胀和计算复杂度呈指数级增长的问题, 导致其远比明文计算慢, 难以支撑实时数据流通. 同时, 安全多方计算在大规模节点协同中存在高昂的通信轮次开销. 未来研究需聚焦于基于硬件加速的 FHE 优化、通信量最小化的 MPC 协议设计等, 以解决高频交易和实时分析场景下的性能不可用问题.

(2) 防御新型侧信道与量子计算威胁

尽管 TEE 被广泛应用, 但 Spectre、Meltdown 及其变种攻击证明了基于微架构的侧信道攻击可穿透硬件隔离; 同时, 当前广泛使用的 RSA、ECC 等公钥体系面临量子计算 Shor 算法的威胁. 未来研究应重点关注抗量子密码算法在数据流通协议中的轻量化适配,以及基于非易失性内存和内存加密技术的抗侧信道 TEE 架构设计.

(3) 解决隐私保护技术的隐私-效用权衡量化难题

现有差分隐私机制在处理高维数据或长尾分布数据时, 为保证隐私预算往往引入过多噪声, 导致数据可用性急剧下降. 未来需探索基于数据分布感知的自适应噪声添加机制以及细粒度的隐私度量模型, 在数学层面精确刻画并优化隐私保护强度与数据效用之间的边界, 而非单纯依赖经验性的参数调整.

(4) 构建跨域、异构环境下的可信性验证体系

当前可信验证呈现碎片化, 区块链难以直接验证链下物理世界数据的真实性, TEE 难以跨异构芯片厂商建立互信. 未来需研究去中心化预言机网络的高效共识机制, 以及跨 TEE 架构的统一远程证明协议, 以消除数据在跨域流通过程中的信任断层.

(5) 实现全流程的协同优化

未来的研究需要从全流程的角度出发, 设计贯穿数据采集、传输、存储、处理、发布和溯源的统一安全与可信保障框架, 解决阶段割裂和协作不足的问题, 形成全生命周期的安全可信闭环体系.

References

[1] Draft expert group on definitions in the data field. Interpretations of common terminology in the data field (first edition). 2024 (in Chinese). https://www.nda.gov.cn/sjj/zwgk/zcfb/1230/ff808081-93de5a43-0194-1b18a0c6-037e.pdf

[2] Kocher P, Horn J, Fogh A, Genkin D, Gruss D, Haas W, Hamburg M, Lipp M, Mangard S, Prescher T, Schwarz M, Yarom Y. Spectre attacks: Exploiting speculative execution. In: Proc. of the 2019 IEEE Symp. on Security and Privacy. San Francisco: IEEE, 2019. 1–19. [doi: 10.1109/SP.2019.00002]

[3] Bates A, Hassan WU. Can data provenance put an end to the data breach? IEEE Security & Privacy, 2019, 17(4): 88–93. [doi: 10.1109/MSEC.2019.2913693]

[4] Li JH, Yin Y, Li SY, Lin X. Review of big data security and privacy computing technologies. Journal of Cybersecurity, 2024, 2(6): 1–15 (in Chinese with English abstract). [doi: 10.20172/j.issn.2097-3136.240601]

[5] Zhong ZY, Zhu CH, Li JZ, Zhang MH. A survey on blockchain-based trusted data elements circulation. Frontiers of Data and Computing, 2023, 5(5): 46–62 (in Chinese with English abstract). [doi: 10.11871/jfdc.issn.2096-742X.2023.05.005]

[6] Wang LP, Guan Z, Li QS, Chen Z, Hu MS. Survey on blockchain-based security services. Ruan Jian Xue Bao/Journal of Software, 2023, 34(1): 1–32 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6402.htm [doi: 10.13328/j.cnki.jos.006402]

[7] Zhang YF, Zeng D, Luo JL, Xu ZL, King I. A survey of trustworthy federated learning with perspectives on security, robustness and privacy. In: Proc. of the 2023 ACM Web Conf. Austin: ACM, 2023. 1167–1176. [doi: 10.1145/3543873.3587681]

[8] Jing XY, Yan Z, Pedrycz W. Security data collection and data analytics in the Internet: A survey. IEEE Communications Surveys & Tutorials, 2019, 21(1): 586–618. [doi: 10.1109/COMST.2018.2863942]

[9] Shan ZH, Ren K, Blanton M, Wang C. Practical secure computation outsourcing: A survey. ACM Computing Surveys, 2018, 51(2): 31. [doi: 10.1145/3158363]

[10] Hong QA, Yu RD, Yu SB, Long XY. A review of data element circulation for intelligent connected vehicles. Information and Communications Technology and Policy, 2024, 50(3): 27–34 (in Chinese with English abstract). [doi: 10.12267/j.issn.2096-5931.2024.03.004]

[11] Hou JW, Qu LL, Shi WC. A survey on Internet of Things security from data perspectives. Computer Networks, 2019, 148: 295–306. [doi: 10.1016/j.comnet.2018.11.026]

[12] Liu LW, Fu CH, Sun ZK, Zhou Y, Ruan N, Jiang CJ. Privacy key technologies in whole stages of data circulation: Current situation, challenges, and prospects. Ruan Jian Xue Bao/Journal of Software, 2026, 37(1): 301–325 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/7478.htm [doi: 10.13328/j.cnki.jos.007478]

[13] State Administration for Market Regulation, Standardization Administration of the People's Republic of China. GB/T 37988—2019 Information security technology—Data security capability maturity model. Beijing: Standards Press of China (in Chinese).

[14] Lyu GX, Liu P, Lu YM, Wang TY, Kang XG. A data middle platform architecture based on microservice serving power grid business. In: Proc. of the 8th IEEE Int'l Conf. on Cyber Security and Cloud Computing (CSCloud)/ the 7th IEEE Int'l Conf. on Edge Computing and Scalable Cloud (EdgeCom). Washington: IEEE, 2021. 219–224. [doi: 10.1109/CSCloud-EdgeCom52276.2021.00047]

[15] Li BS, Hu QG, Chen XF, Gao BQ. Research and design of data platform for power grid enterprise. Electric Power Information and Communication Technology, 2019, 17(7): 29–34 (in Chinese with English abstract). [doi: 10.16543/j.2095-641x.electric.power.ict.2019.07.006]

[16] Liu K, Wang SL, Cheng W, Yang WB, Yang SZ. Research on middle platform construction and large data analysis of power enterprises based on Aliyun. In: Proc. of the 2022 Int'l Seminar on Computer Science and Engineering Technology (SCSET). Indianapolis: IEEE, 2022. 326–329. [doi: 10.1109/SCSET55041.2022.00080]

[17] Lu X, Zhang ZJ, Zhou T, Niu T, Li M, Guan ZT, Ma T, Zhu LH. Decentralized fair IoT data trading via searchable proxy re-encryption. IEEE Internet of Things Journal, 2024, 11(11): 19485–19499. [doi: 10.1109/JIOT.2024.3365832]

[18] Hu DH, Li YF, Pan LX, Li M, Zheng SL. A blockchain-based trading system for big data. Computer Networks, 2021, 191: 107994. [doi: 10.1016/j.comnet.2021.107994]

[19] Lyu QY, Zhou YL, Ren YZ, Wang Z, Guo YC. Toward personal data sharing autonomy: A task-driven data capsule sharing system. IEEE Trans. on Information Forensics and Security, 2024, 19: 9760–9774. [doi: 10.1109/TIFS.2024.3472529]

[20] Lu YL, Huang XH, Zhang K, Maharjan S, Zhang Y. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of vehicles. IEEE Trans. on Vehicular Technology, 2020, 69(4): 4298–4311. [doi: 10.1109/TVT.2020.2973651]

[21] Chatziantoniou D, Kantere V, Antoniou N, Gantzia A. Data virtual machines: Simplifying data sharing, exploration & querying in big data environments. In: Proc. of the 2022 IEEE Int'l Conf. on Big Data. Osaka: IEEE, 2022. 373–380. [doi: 10.1109/BigData55660.2022.10020508]

[22] Peng S, Sun D, Zhu LK, Zhou HT, Zhang XS, Cui CC. Enhancing cross-border data sharing in blockchain networks: A compliance-centric approach ensuring anonymity and traceability. In: Proc. of the 3rd Int'l Conf. on Computer Science and Blockchain. Shenzhen: IEEE, 2023. 200–204. [doi: 10.1109/CCSB60789.2023.10398873]

[23] Rahman MS, Al Omar A, Bhuiyan MZA, Basu A, Kiyomoto S, Wang G. Accountable cross-border data sharing using blockchain under relaxed trust assumption. IEEE Trans. on Engineering Management, 2020, 67(4): 1476–1486. [doi: 10.1109/TEM.2019.2960829]

[24] Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of Things: Evolution, concerns and security challenges. Sensors, 2021, 21(5): 1809. [doi: 10.3390/s21051809]

[25] Huang JY, Bai JX, Zhang X, Liu Z, Feng YH, Liu JC, Sun X, Dong MX, Li M. KeystrokeSniffer: An off-the-shelf smartphone can eavesdrop on your privacy from anywhere. IEEE Trans. on Information Forensics and Security, 2024, 19: 6840–6855. [doi: 10.1109/TIFS.2024.3424301]

[26] Guan L, Liu P, Xing XY, Ge XY, Zhang SZ, Yu M, Jaeger T. TrustShadow: Secure execution of unmodified applications with ARM TrustZone. In: Proc. of the 15th Annual Int'l Conf. on Mobile Systems, Applications, and Services. Niagara Falls: ACM, 2017. 488–501. [doi: 10.1145/3081333.3081349]

[27] Han S, Jang J. MyTEE: Own the trusted execution environment on embedded devices. In: Proc. of the 2023 Network and Distributed

System Security Symp. San Diego: Internet Society, 2023. [doi: 10.14722/ndss.2023.23041]

[28] Du DD, Yang BC, Yu Y, Xia YB, Ding ZH, Zhao YW, Zhang L, Zang BY, Chen HB. SegTEE: Trusted execution environment for lightweight edge devices. Chinese Journal of Computers, 2025, 48(1): 188–209 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2025.00188]

[29] Khan MN, Rao AS, Camtepe S. Lightweight cryptographic protocols for IoT-constrained devices: A survey. IEEE Internet of Things Journal, 2021, 8(6): 4132–4156. [doi: 10.1109/JIOT.2020.3026493]

[30] Hazum A, Mana O, Wernik I, Melnykov B, Efrati C. COVID-19 goes mobile: Coronavirus malicious applications discovered. 2020. https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered

[31] Gavazzi A, Williams R, Kirda E, Lu L, King A, Davis A, Leek T. A study of multi-factor and risk-based authentication availability. In: Proc. of the 32nd USENIX Security Symp. Anaheim: USENIX Association, 2023. 2043–2060.

[32] Song WN, Ming J, Jiang L, Xiang Y, Pan XC, Fu JM, Peng GJ. Towards transparent and stealthy Android OS sandboxing via customizable container-based virtualization. In: Proc. of the 2021 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2021. 2858–2874. [doi: 10.1145/3460120.3484544]

[33] Hong SM, Xu L, Huang JW, Li HD, Hu HX, Gu GF. SysFlow: Toward a programmable zero trust framework for system security. IEEE Trans. on Information Forensics and Security, 2023, 18: 2794–2809. [doi: 10.1109/TIFS.2023.3264152]

[34] Karapanos N, Capkun S. On the effective prevention of TLS man-in-the-middle attacks in Web applications. In: Proc. of the 23rd USENIX Security Symp. San Diego: USENIX Association, 2014. 671–686.

[35] Rescorla E. The transport layer security (TLS) protocol version 1.3. 2018. https://www.rfc-editor.org/rfc/rfc8446 [doi: 10.17487/RFC8446]

[36] MITRE. CVE-2014-0160. 2014. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

[37] Maehren M, Nieting P, Hebrok S, Merget R, Somorovsky J, Schwenk J. TLS-Anvil: Adapting combinatorial testing for TLS libraries. In: Proc. of the 31st USENIX Security Symp. Boston: USENIX Association, 2022. 215–232.

[38] Lenovo caught installing adware on new computers. 2015. https://thenextweb.com/news/lenovo-caught-installing-adware-new-computers

[39] Rao V, Prema KV. Light-weight hashing method for user authentication in Internet-of-Things. Ad Hoc Networks, 2019, 89: 97–106. [doi: 10.1016/j.adhoc.2019.03.003]

[40] Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehlé D. CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR Trans. on Cryptographic Hardware and Embedded Systems, 2018, 2018(1): 238–268. [doi: 10.46586/tches.v2018.i1.238-268]

[41] The Guardian. Fastly says single customer triggered bug that caused mass outage. 2021. https://www.theguardian.com/technology/2021/jun/09/fastly-says-single-customer-triggered-bug-that-caused-mass-outage

[42] Zheng L, Zhang X, Zhang SJ, Chen XH. Research on multi-path network in cloud computing based on SCTP. In: Proc. of the 8th IEEE Int'l Conf. on Cyber Security and Cloud Computing (CSCloud)/ the 7th IEEE Int'l Conf. on Edge Computing and Scalable Cloud (EdgeCom). Washington: IEEE, 2021. 30–35. [doi: 10.1109/CSCloud-EdgeCom52276.2021.00016]

[43] Winder D. Microsoft security shocker as 250 million customer records exposed online. 2020. https://www.forbes.com/sites/daveywinder/2020/L01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/

[44] Dauterman E, Corrigan-Gibbs H, Mazières D. SafetyPin: Encrypted backups with human-memorable secrets. In: Proc. of the 14th USENIX Symp. on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2020. 1121–1138.

[45] Li M, Chen YF, Zheng SL, Hu DH, Lal C, Conti M. Privacy-preserving navigation supporting similar queries in vehicular networks. IEEE Trans. on Dependable and Secure Computing, 2022, 19(2): 1133–1148. [doi: 10.1109/TDSC.2020.3017534]

[46] Li M, Zhu LH, Zhang ZJ, Lal C, Conti M, Alazab M. User-defined privacy-preserving traffic monitoring against n-by-1 jamming attack. IEEE/ACM Trans. on Networking, 2022, 30(5): 2060–2073. [doi: 10.1109/TNET.2022.3157654]

[47] Li M, Zhu LH, Lin XD. Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing. IEEE Trans. on Services Computing, 2021, 14(6): 1902–1913. [doi: 10.1109/TSC.2019.2903060]

[48] Li M, Chen YF, Gao JB, Wu JY, Zhang ZJ, He JL, Zhu LH, Conti M, Lin XD. Accurate, secure, and efficient semi-constrained navigation over encrypted city maps. IEEE Trans. on Dependable and Secure Computing, 2025, 22(3): 2642–2658. [doi: 10.1109/TDSC.2024.3521396]

[49] Li M, Zhang MW, Zhu LH, Zhang ZJ, Conti M, Alazab M. Decentralized and privacy-preserving smart parking with secure repetition and full verifiability. IEEE Trans. on Mobile Computing, 2024, 23(12): 11635–11654. [doi: 10.1109/TMC.2024.3397687]

[50] Li M, Gao JB, Zhu LH, Zhang ZJ, Lal C, Conti M. Time-restricted, verifiable, and efficient query processing over encrypted data on

cloud. IEEE Trans. on Services Computing, 2024, 17(3): 1239–1251. [doi: 10.1109/TSC.2023.3311586]

[51] Wang Q, Hu DH, Li M, Yang GM. Secure and flexible wildcard queries. IEEE Trans. on Information Forensics and Security, 2024, 19: 7374–7388. [doi: 10.1109/TIFS.2024.3430056]

[52] Shen H, Yu CG, Susilo W, Chen YT, Zhang MW. An efficient graph encryption scheme supporting shortest path fuzzy queries. IEEE Trans. on Information Forensics and Security, 2025, 20: 8687–8700. [doi: 10.1109/TIFS.2025.3599388]

[53] Kyodo News. Japan local gov't hard drives with personal info sold in online auction. 2019. https://english.kyodonews.net/news/2019/12/e4d56ade9dd3-local-govt-hard-drives-with-personal-info-sold-in-online-auction.html

[54] Kissel R, Regenscheid A, Scholl M, Stine K. Guidelines for media sanitization. National Institute of Standards and Technology, NIST SP 800–88r1, 2014. [doi: 10.6028/NIST.SP.800-88r1]

[55] China Association of Communication Enterprises. T/CAICI 80-2024 Data security requirements and evaluation methods for Data Destruction in storage media. 2024 (in Chinese). https://www.cssn.net.cn/cssn/productDetail/0751693eb1eb67025c4d2ddba83b952a

[56] Reardon J, Basin D, Capkun S. SoK: Secure data deletion. In: Proc. of the 2013 IEEE Symp. on Security and Privacy. Berkeley: IEEE, 2013. 301–315. [doi: 10.1109/SP.2013.28]

[57] Ma A, Dragga C, Arpaci-Dusseau AC, Arpaci-Dusseau RH, Mckusick MK. Ffsck: The fast file-system checker. ACM Trans. on Storage, 2014, 10(1): 2. [doi: 10.1145/2560011]

[58] Mykletun E, Narasimha M, Tsudik G. Authentication and integrity in outsourced databases. ACM Trans. on Storage, 2006, 2(2): 107–138. [doi: 10.1145/1149976.1149977]

[59] Shi RZ, Cheng RZ, Fu YQ, Han B, Cheng Y, Chen SQ. Centralization in the decentralized Web: Challenges and opportunities in IPFS data management. In: Proc. of the 2025 ACM Web Conf. Sydney: ACM, 2025. 4068–4076. [doi: 10.1145/3696410.3714627]

[60] Dong HW, Zhang C, Li GL, Feng JH. Survey on cloud-native databases. Ruan Jian Xue Bao/Journal of Software, 2024, 35(2): 899–926 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6952.htm [doi: 10.13328/j.cnki.jos.006952]

[61] Liu JW, Shen HY, Chi HM, Narman HS, Yang YY, Cheng L, Chung W. A low-cost multi-failure resilient replication scheme for high-data availability in cloud storage. IEEE/ACM Trans. on Networking, 2021, 29(4): 1436–1451. [doi: 10.1109/TNET.2020.3027814]

[62] McKeen F, Alexandrovich I, Berenzon A, Rozas CV, Shafi H, Shanbhogue V, Savagaonkar UR. Innovative instructions and software model for isolated execution. In: Proc. of the 2nd Int'l Workshop on Hardware and Architectural Support for Security and Privacy (HASP). Tel-Aviv: ACM, 2013. 10. [doi: 10.1145/2487726.2488368]

[63] Intel®. Intel® Trust Domain Extensions. 2022. https://www.intel.com/content/dam/develop/external/us/en/documents/tdx-whitepaper-final9-17.pdf

[64] Kaplan D, Powell J, Woller T. AMD memory encryption. 2021. https://docs.amd.com/api/khub/documents/ZcsCCmeL80dbtuf_VlGpvw/content

[65] Pinto S, Santos N. Demystifying ARM TrustZone: A comprehensive survey. ACM Computing Surveys, 2019, 51(6): 130. [doi: 10.1145/3291047]

[66] Li M, Chen YF, Lal C, Conti M, Martinelli F, Alazab M. Nereus: Anonymous and secure ride-hailing service based on private smart contracts. IEEE Trans. on Dependable and Secure Computing, 2023, 20(4): 2849–2866. [doi: 10.1109/TDSC.2022.3192367]

[67] Wang WH, Liu WJ, Chen HB, Wang XF, Tian HL, Lin DD. Trust beyond border: Lightweight, verifiable user isolation for protecting in-enclave services. IEEE Trans. on Dependable and Secure Computing, 2023, 20(1): 522–538. [doi: 10.1109/TDSC.2021.3138427]

[68] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proc. of the 41st Annual ACM Symp. on Theory of Computing (STOC). Bethesda: ACM, 2009. 169–178. [doi: 10.1145/1536414.1536440]

[69] Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 2019, 51(4): 79. [doi: 10.1145/3214303]

[70] Cheon JH, Kim A, Kim M, Song Y. Homomorphic encryption for arithmetic of approximate numbers. In: Proc. of the 23rd Int'l Conf. on the Theory and Applications of Cryptology and Information Security. Hong Kong: Springer, 2017. 409–437. [doi: 10.1007/978-3-319-70694-8_15]

[71] Viand A, Jattke P, Haller M, Hithnawi A. HECO: Fully homomorphic encryption compiler. In: Proc. of the 32nd USENIX Security Symp. Anaheim: USENIX Association, 2023. 4715–4732.

[72] MITRE. CVE-2018-8009. 2018. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8009

[73] Zhang YH, Deng RH, Xu SM, Sun JF, Li Q, Zheng D. Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys, 2021, 53(4): 83. [doi: 10.1145/3398036]

[74] Ying ZB, Jiang WJ, Liu XM, Xu SM, Deng RH. Reliable policy updating under efficient policy hidden fine-grained access control framework for cloud data sharing. IEEE Trans. on Services Computing, 2022, 15(6): 3485–3498. [doi: 10.1109/TSC.2021.3096177]

[75] Wang YZ, Zhang MW. Witness encryption with updatable ciphertexts. Science China Information Sciences, 2025, 68(3): 132109. [doi: 10.1007/s11432-024-4214-0]

[76] Mi ZY, Li DJ, Chen HB, Zang BY, Guan HB. (Mostly) exitless VM protection from untrusted hypervisor through disaggregated nested virtualization. In: Proc. of the 29th USENIX Security Symp. USENIX Associatio, 2020. 1695–1712.

[77] Sharma B, Pokharel P, Joshi B. User behavior analytics for anomaly detection using LSTM autoencoder—Insider threat detection. In: Proc. of the 11th Int'l Conf. on Advances in Information Technology. Bangkok: ACM, 2020. 5. [doi: 10.1145/3406601.3406610]

[78] Saxena D, Singh AK, Buyya R. OP-MLB: An online VM prediction-based multi-objective load balancing framework for resource management at cloud data center. IEEE Trans. on Cloud Computing, 2022, 10(4): 2804–2816. [doi: 10.1109/TCC.2021.3059096]

[79] Kiayias A, Tang Q. Traitor deterring schemes: Using bitcoin as collateral for digital content. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. Denver: ACM, 2015. 231–242. [doi: 10.1145/2810103.2813698]

[80] NBC News. Stolen NASA laptop had space station control codes. 2012. https://www.nbcnews.com/id/wbna46591267

[81] Chen YA, Alhanahnah M, Sabelfeld A, Chatterjee R, Fernandes E. Practical data access minimization in trigger-action platforms. In: Proc. of the 31st USENIX Security Symp. Boston: USNEIX Association, 2022. 2929–2945.

[82] Chen YX, Zheng QH, Yan Z, Liu D. QShield: Protecting outsourced cloud data queries with multi-user access control based on SGX. IEEE Trans. on Parallel and Distributed Systems, 2021, 32(2): 485–499. [doi: 10.1109/TPDS.2020.3024880]

[83] Alneyadi S, Sithirasenan E, Muthukkumarasamy V. A survey on data leakage prevention systems. Journal of Network and Computer Applications, 2016, 62: 137–152. [doi: 10.1016/j.jnca.2016.01.008]

[84] Hao F, Clarke D, Zorzo AF. Deleting secret data with public verifiability. IEEE Trans. on Dependable and Secure Computing, 2016, 13(6): 617–629. [doi: 10.1109/TDSC.2015.2423684]

[85] Hu DH, Wang Q, Yan S, Liu XJ, Li M, Zheng SL. Reversible database watermarking based on order-preserving encryption for data sharing. ACM Trans. on Database Systems, 2023, 48(2): 5. [doi: 10.1145/3589761]

[86] Li M, Chen YF, Lal C, Conti M, Alazab M, Hu DH. Eunomia: Anonymous and secure vehicular digital forensics based on blockchain. IEEE Trans. on Dependable and Secure Computing, 2023, 20(1): 225–241. [doi: 10.1109/TDSC.2021.3130583]

[87] Li M, Shen YZ, Ye GX, He JL, Zheng X, Zhang ZJ, Zhu LH, Conti M. Anonymous, secure, traceable, and efficient decentralized digital forensics. IEEE Trans. on Knowledge and Data Engineering, 2024, 36(5): 1874–1888. [doi: 10.1109/TKDE.2023.3321712]

[88] Yoon J, Drumright LN, van Der Schaar M. Anonymization through data synthesis using generative adversarial networks (ADS-GAN). IEEE Journal of Biomedical and Health Informatics, 2020, 24(8): 2378–2388. [doi: 10.1109/JBHI.2020.2980262]

[89] Zhu LH, Li M, Zhang ZJ, Qin Z. ASAP: An anonymous smart-parking and payment scheme in vehicular networks. IEEE Trans. on Dependable and Secure Computing, 2020, 17(4): 703–715. [doi: 10.1109/TDSC.2018.2850780]

[90] Dwork C, Roth A. The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 2014, 9(3–4): 211–487. [doi: 10.1561/0400000042]

[91] Wei K, Li J, Ding M, Ma C, Yang HH, Farokhi F, Jin S, Quek TQS, Poor HV. Federated learning with differential privacy: Algorithms and performance analysis. IEEE Trans. on Information Forensics and Security, 2020, 15: 3454–3469. [doi: 10.1109/TIFS.2020.2988575]

[92] Li M, Chen YF, Zhu LH, Zhang ZJ, Ni JB, Lal C, Conti M. Astraea: Anonymous and secure auditing based on private smart contracts for donation systems. IEEE Trans. on Dependable and Secure Computing, 2023, 20(4): 3002–3018. [doi: 10.1109/TDSC.2022.3204287]

[93] Hasan R, Sion R, Winslett M. Preventing history forgery with secure provenance. ACM Trans. on Storage, 2009, 5(4): 12. [doi: 10.1145/1629080.1629082]

[94] Lauinger J, Ernstberger J, Finkenzeller A, Steinhorst S. Janus: Fast privacy-preserving data provenance for TLS. In: Proc. of the 2025 Privacy Enhancing Technologies. Washington: PETS, 2025. 511–530. [doi: 10.56553/popets-2025-0028]

[95] Canovas Sanchez JL, Bernabe JB, Skarmeta AF. Towards privacy preserving data provenance for the Internet of Things. In: Proc. of the 4th IEEE World Forum on Internet of Things (WF-IoT). Singapore: IEEE, 2018. 41–46. [doi: 10.1109/WF-IoT.2018.8355229]

[96] Sultana S, Shehab M, Bertino E. Secure provenance transmission for streaming data. IEEE Trans. on Knowledge and Data Engineering, 2013, 25(8): 1890–1903. [doi: 10.1109/TKDE.2012.31]

[97] Pan BF, Stakhanova N, Ray S. Data provenance in security and privacy. ACM Computing Surveys, 2023, 55(14s): 323. [doi: 10.1145/3593294]

[98] Zawoad S, Hasan R. SECAP: Towards securing application provenance in the cloud. In: Proc. of the 9th IEEE Int'l Conf. on Cloud Computing (CLOUD). San Francisco: IEEE, 2016. 900–903. [doi: 10.1109/CLOUD.2016.0132]

[99] Liang XP, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proc. of the 17th IEEE/ACM Int'l Symp. on Cluster, Cloud and Grid Computing (CCGRID). Madrid: IEEE/ACM, 2017. 468–477. [doi: 10.1109/CCGRID.2017.8]

[100] Ruan PC, Dinh TTA, Lin Q, Zhang MH, Chen G, Ooi BC. LineageChain: A fine-grained, secure and efficient data provenance system for blockchains. The VLDB Journal, 2021, 30(1): 3–24. [doi: 10.1007/s00778-020-00646-1]

[101] Zhang ZJ, Liu XY, Li M, Yin H, Zhu LH, Khoussainov B, Gai KK. HCA: Hashchain-based consensus acceleration via re-voting. IEEE Trans. on Dependable and Secure Computing, 2024, 21(2): 775–788. [doi: 10.1109/TDSC.2023.3262283]

[102] Liu XY, Feng KY, Zhang ZJ, Li M, Chen X, Lai WQ, Zhu LH. Dolphin: Efficient non-blocking consensus via concurrent block generation. IEEE Trans. on Mobile Computing, 2024, 23(12): 11824–11838. [doi: 10.1109/TMC.2024.3399772]

[103] Zhang ZJ, Liu XY, Feng KY, Wan MC, Li M, Dong J, Zhu LH. Phantasm: Adaptive scalable mining toward stable BlockDAG. IEEE Trans. on Services Computing, 2024, 17(3): 1084–1096. [doi: 10.1109/TSC.2023.3322203]

[104] Khan F, Al-Atawi AA, Alomari A, Alsirhani A, Alshahrani MM, Khan J, Lee Y. Development of a model for spoofing attacks in Internet of Things. Mathematics, 2022, 10(19): 3686. [doi: 10.3390/math10193686]

[105] BBC. Energy smart meter issues creating north-south divide. 2023. https://www.bbc.com/news/articles/cq52382zd1no

[106] Guin U, Singh A, Alam M, Canedo J, Skjellum A. A secure low-cost edge device authentication scheme for the Internet of Things. In: Proc. of the 31st Int'l Conf. on VLSI Design and the 17th Int'l Conf. on Embedded Systems (VLSID). Pune: IEEE, 2018. 85–90. [doi: 10.1109/VLSID.2018.42]

[107] Liu Y, Zhang C, Yan Y, Zhou X, Tian ZH, Zhang J. A semi-centralized trust management model based on blockchain for data exchange in IoT system. IEEE Trans. on Services Computing, 2023, 16(2): 858–871. [doi: 10.1109/TSC.2022.3181668]

[108] Liu DD, Jin R, Wei SJ. Distributed Internet of vehicles node reputation management system based on consortium chain. Computer Engineering, 2025, 51(10): 191–202 (in Chinese with English abstract). [doi: 10.19678/j.issn.1000-3428.0069457]

[109] Shi X, Prins C, van Pottelbergh G, Mamouris P, Vaes B, de Moor B. An automated data cleaning method for electronic health records by incorporating clinical knowledge. BMC Medical Informatics and Decision Making, 2021, 21(1): 267. [doi: 10.1186/s12911-021-01630-7]

[110] BBC. Tay: Microsoft issues apology over racist chatbot fiasco. 2016. https://www.bbc.com/news/technology-35902104

[111] Gao MN, Chen W, Wu LF, Zhang BL. Survey on backdoor attacks and defenses for deep learning research. Ruan Jian Xue Bao/Journal of Software, 2025, 36(7): 3271–3305 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/7364.htm [doi: 10.13328/j.cnki.jos.007364]

[112] Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town Crier: An authenticated data feed for smart contracts. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. Vienna: ACM, 2016. 270–282. [doi: 10.1145/2976749.2978326]

[113] Tran B, Li J, Madry A. Spectral signatures in backdoor attacks. In: Proc. of the 32nd Int'l Conf. on Neural Information Processing Systems. Montréal: Curran Associates Inc., 2018. 8011–8021.

[114] Whang SE, Roh Y, Song H, Lee JG. Data collection and quality challenges in deep learning: A data-centric AI perspective. The VLDB Journal, 2023, 32(4): 791–813. [doi: 10.1007/s00778-022-00775-9]

[115] Dwivedi SK, Amin R, Vollala S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. Journal of Information Security and Applications, 2020, 54: 102554. [doi: 10.1016/j.jisa.2020.102554]

[116] Liu LF, Li J, Yuan TT. TEE-based mutual proofs of transmission services in decentralized systems. In: Proc. of the 2020 IEEE INFOCOM Conf. on Computer Communications Workshops. Toronto: IEEE, 2020. 754–759. [doi: 10.1109/INFOCOMWKSHPS50562.2020.9162764]

[117] Li M, Ding HN, Wang Q, Zhang MW, Meng WZ, Zhu LH, Zhang ZJ, Lin XD. Decentralized threshold signatures with dynamically private accountability. IEEE Trans. on Information Forensics and Security, 2024, 19: 2217–2230. [doi: 10.1109/TIFS.2023.3347968]

[118] Guo ZY, Li X, Liu JM, Zhang ZJ, Li M, Hu JJ, Zhu LH. Graph-based covert transaction detection and protection in blockchain. IEEE Trans. on Information Forensics and Security, 2024, 19: 2244–2257. [doi: 10.1109/TIFS.2023.3347895]

[119] Nyaletey E, Parizi RM, Zhang Q, Choo KKR. BlockIPFS—Blockchain-enabled interplanetary file system for forensic and trusted data traceability. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain. Atlanta: IEEE, 2019. 18–25. [doi: 10.1109/Blockchain.2019.00012]

[120] Anthoine G, Dumas JG, de Jonghe M, Maignan A, Pernet C, Hanling M, Roche DS. Dynamic proofs of retrievability with low server storage. In: Proc. of the 30th USENIX Security Symp. USENIX Association, 2021. 537–554.

[121] Zhou WC, Cai YF, Peng YQ, Wang S, Ma K, Li FF. VeriDB: An SGX-based verifiable database. In: Proc. of the 2021 Int'l Conf. on Management of Data. ACM, 2021. 2182–2194. [doi: 10.1145/3448016.3457308]

[122] Lamport L. Paxos made simple. ACM SIGACT News (Distributed Computing Column), 2001, 32(4): 51–58.

[123] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm. In: Proc. of the 2014 USENIX Annual Technical Conf. Philadelphia: USENIX Association, 2014. 305–319.

[124] Howard H, Mortier R. Paxos vs Raft: Have we reached consensus on distributed consensus? In: Proc. of the 7th Workshop on Principles

and Practice of Consistency for Distributed Data (PaPoC). Heraklion: ACM, 2020. 8. [doi: 10.1145/3380787.3393681]

[125] Hendrycks D, Zhao K, Basart S, Steinhardt J, Song D. Natural adversarial examples. In: Proc. of the 2021 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Nashville: IEEE, 2021. 15257–15266. [doi: 10.1109/CVPR46437.2021.01501]

[126] Nohara Y, Matsumoto K, Soejima H, Nakashima N. Explanation of machine learning models using Shapley additive explanation and application for real data in hospital. Computer Methods and Programs in Biomedicine, 2022, 214: 106584. [doi: 10.1016/j.cmpb.2021.106584]

[127] Levi M, Kontorovich A. Splitting the difference on adversarial training. In: Proc. of the 33rd USENIX Security Symp. Philadelphia: USENIX Association, 2024. 3639–3656.

[128] Sun HC, Bai TH, Li J, Zhang HY. zkDL: Efficient zero-knowledge proofs of deep learning training. IEEE Trans. on Information Forensics and Security, 2025, 20: 914–927. [doi: 10.1109/TIFS.2024.3520863]

[129] Fiore D, Tucker I. Efficient zero-knowledge proofs on signed data with applications to verifiable computation on data streams. In: Proc. of the 2022 ACM SIGSAC Conf. on Computer and Communications Security. Los Angeles: ACM, 2022. 1067–1080. [doi: 10.1145/3548606.3560630]

[130] Chen HB, Chen HH, Sun MS, Li K, Chen ZF, Wang XF. A verified confidential computing as a service framework for privacy preservation. In: Proc. of the 32nd USENIX Security Symp. Anaheim: USENIX Association, 2023. 4733–4750.

[131] Zhang S, Zhang Y, Zhang W, Huang G. Method of data service integrity verification based on remote attestation. Ruan Jian Xue Bao/Journal of Software, 2024, 35(11): 4949–4972 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/7001.htm [doi: 10.13328/j.cnki.jos.007001]

[132] Peng Z, Xu JL, Chu XW, Gao S, Yao Y, Gu R, Tang YZ. VFChain: Enabling verifiable and auditable federated learning via blockchain systems. IEEE Trans. on Network Science and Engineering, 2022, 9(1): 173–186. [doi: 10.1109/TNSE.2021.3050781]

[133] Zhang ZJ, Lu X, Li M, An JC, Yu Y, Yin H, Zhu LH, Liu Y, Liu JM, Khoussainov B. A blockchain-based privacy-preserving scheme for sealed-bid auction. IEEE Trans. on Dependable and Secure Computing, 2024, 21(5): 4668–4683. [doi: 10.1109/TDSC.2024.3353540]

[134] Zhang MW, Fan TY, Wang YZ, Zhu TQ, Yang B. Multiparty chained adaptor signatures based on the SM2 algorithm. Scientia Sinica Informationis, 2025, 55(6): 1406–1427 (in Chinese with English abstract). [doi: 10.1360/SSI-2025-0009]

[135] Wan ZG, Zhou Y, Ren K. Zk-AuthFeed: Protecting data feed to smart contracts with authenticated zero knowledge proof. IEEE Trans. on Dependable and Secure Computing, 2023, 20(2): 1335–1347. [doi: 10.1109/TDSC.2022.3153084]

[136] Adams C, Cain P, Pinkas D, Zuccherato R. Internet X.509 public key infrastructure time-stamp protocol (TSP). 2001. https://datatracker.ietf.org/doc/html/rfc3161

[137] Zhang F, Maram D, Malvai H, Goldfeder S, Juels A. DECO: Liberating Web data using decentralized oracles for TLS. In: Proc. of the 2020 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2020. 1919–1938. [doi: 10.1145/3372297.3417239]

[138] Breidenbach L, Cachin C, Chan B, Coventry A, Ellis S, Juels A, Koushanfar F, Miller A, Magauran B, Moroz D, Nazarov S, Topliceanu A, Tramèr F, Zhang F. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. Chainlink Labs, 2021, 1: 1–136.

[139] Yang XY, Wang S, Li FF, Zhang Y, Yan WY, Gai FY, Yu BQ, Feng LK, Gao Q, Li YZ. Ubiquitous verification in centralized ledger database. In: Proc. of the 38th IEEE Int'l Conf. on Data Engineering. Kuala Lumpur: IEEE, 2022. 1808–1821. [doi: 10.1109/ICDE53745.2022.00181]

[140] Liu ZW, Hu CQ, Xia H, Xiang T, Wang BL, Chen JJ. SPDTS: A differential privacy-based blockchain scheme for secure power data trading. IEEE Trans. on Network and Service Management, 2022, 19(4): 5196–5207. [doi: 10.1109/TNSM.2022.3181814]

[141] Weng JS, Yao SL, Du YF, Huang JJ, Weng J, Wang C. Proof of unlearning: Definitions and instantiation. IEEE Trans. on Information Forensics and Security, 2024, 19: 3309–3323. [doi: 10.1109/TIFS.2024.3358993]

[142] Aman MN, Basheer MH, Sikdar B. Data provenance for IoT with light weight authentication and privacy preservation. IEEE Internet of Things Journal, 2019, 6(6): 10441–10457. [doi: 10.1109/JIOT.2019.2939286]

[143] Backes M, Grimm N, Kate A. Data lineage in malicious environments. IEEE Trans. on Dependable and Secure Computing, 2016, 13(2): 178–191. [doi: 10.1109/TDSC.2015.2399296]

[144] Sablayrolles A, Douze M, Schmid C, Jegou H. Radioactive data: Tracing through training. In: Proc. of the 37th Int'l Conf. on Machine Learning. JMLR.org, 2020. 8326–8335.

[145] Tang MJ, Shao SS, Yang WQ, Liang YB, Yu YY, Saha B, Hyun D. SAC: A system for big data lineage tracking. In: Proc. of the 35th IEEE Int'l Conf. on Data Engineering. Macao: IEEE, 2019. 1964–1967. [doi: 10.1109/ICDE.2019.00215]

[146] Deutch D, Frankenthal A, Gilad A, Moskovitch Y. On optimizing the trade-off between privacy and utility in data provenance. In: Proc. of the 2021 Int'l Conf. on Management of Data. ACM, 2021. 379–391. [doi: 10.1145/3448016.3452835]

附中文参考文献

[1] 数据领域名词解释起草专家组. 数据领域常用名词解释 (第一批). 2024. https://www.nda.gov.cn/sjj/zwgk/zcfb/1230/ff808081-93de5a43-0194-1b18a0c6-037e.pdf

[4] 李建华, 银鹰, 李思源, 林夕. 大数据安全与隐私计算技术综述. 网络空间安全科学学报, 2024, 2(6): 1–15. [doi: 10.20172/j.issn.2097-3136.240601]

[5] 钟子岳, 朱长昊, 李浚哲, 张美慧. 基于区块链的数据要素可信流通技术综述. 数据与计算发展前沿, 2023, 5(5): 46–62. [doi: 10.11871/jfdc.issn.2096-742X.2023.05.005]

[6] 王利朋, 关志, 李青山, 陈钟, 胡明生. 区块链数据安全服务综述. 软件学报, 2023, 34(1): 1–32. http://www.jos.org.cn/1000-9825/6402.htm [doi: 10.13328/j.cnki.jos.006402]

[10] 洪启安, 于润东, 于胜波, 龙翔宇. 智能网联汽车数据要素流通综述. 信息通信技术与政策, 2024, 50(3): 27–34. [doi: 10.12267/j.issn.2096-5931.2024.03.004]

[12] 刘立伟, 傅超豪, 孙泽堃, 周耘, 阮娜, 蒋昌俊. 数据要素流通全流程隐私关键技术: 现状、挑战与展望. 软件学报, 2026, 37(1): 301–325. http://www.jos.org.cn/1000-9825/7478.htm [doi: 10.13328/j.cnki.jos.007478]

[13] 国家市场监督管理总局, 国家标准化管理委员会. GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型. 北京: 中国标准出版社, 2019.

[15] 李炳森, 胡全贵, 陈小峰, 高秉强. 电网企业数据中台的研究与设计. 电力信息与通信技术, 2019, 17(7): 29–34. [doi: 10.16543/j.2095-641x.electric.power.ict.2019.07.006]

[28] 杜冬冬, 杨璧丞, 余炀, 夏虞斌, 丁佐华, 赵永望, 张磊, 臧斌宇, 陈海波. SegTEE: 面向小型端侧设备的可信执行环境系统. 计算机学报, 2025, 48(1): 188–209. [doi: 10.11897/SP.J.1016.2025.00188]

[55] 中国通信企业协会. T/CAICI 80-2024 存储介质数据销毁安全要求和测试方法. 2024. https://www.cssn.net.cn/cssn/productDetail/0751693eb1eb67025c4d2ddba83b952a

[60] 董昊文, 张超, 李国良, 冯建华. 云原生数据库综述. 软件学报, 2024, 35(2): 899–926. http://www.jos.org.cn/1000-9825/6952.htm [doi: 10.13328/j.cnki.jos.006952]

[108] 刘代东, 金睿, 魏松杰. 基于联盟链的分布式车联网节点信誉管理系统. 计算机工程, 2025, 51(10): 191–202. [doi: 10.19678/j.issn.1000-3428.0069457]

[111] 高梦楠, 陈伟, 吴礼发, 张伯雷. 面向深度学习的后门攻击及防御研究综述. 软件学报, 2025, 36(7): 3271–3305. http://www.jos.org.cn/1000-9825/7364.htm [doi: 10.13328/j.cnki.jos.007364]

[131] 张溯, 张颖, 张伟, 黄罡. 基于远程证明的数据服务完整性验证方法. 软件学报, 2024, 35(11): 4949–4972. http://www.jos.org.cn/1000-9825/7001.htm [doi: 10.13328/j.cnki.jos.007001]

[134] 张明武, 范恬媛, 王玉珠, 朱天清, 杨波. 基于 SM2 的多方链式适配器签名. 中国科学: 信息科学, 2025, 55(6): 1406–1427. [doi: 10.1360/SSI-2025-0009]

作者简介

陈毅飞, 博士生, CCF 学生会员, 主要研究领域为数据安全, 隐私保护.

李萌, 博士, 教授, CCF 高级会员, 主要研究领域为数据流通, 数据安全, 隐私保护.

乔焰, 博士, 副教授, CCF 高级会员, 主要研究领域为网络测量, 时间序列表示学习, 异常检测.

汪青, 博士生, CCF 学生会员, 主要研究领域为应用密码学, 可搜索加密.

张子剑, 博士, 教授, CCF 高级会员, 主要研究领域为认证与识别, 共识机制, 隐私计算.

祝烈煌, 博士, 教授, CCF 杰出会员, 主要研究领域为密码学, 协议安全, 物联网安全.