Research on Security and Privacy Protection Technology in Cyberspace under Big Data Environment

Ziao Shang

Henan Polytechnic University, Jiaozuo, Henan, 454150, China

Abstract

The widespread application of big data technology has driven profound transformations in data collection, storage, transmission, analysis, and sharing methods, while simultaneously exacerbating cybersecurity risks and personal privacy protection challenges. Although massive data volumes enhance governance efficiency, business decision-making capabilities, and public service quality, they also introduce issues such as data breaches, identity verification, behavioral tracking, and algorithmic misuse. Traditional security models relying on perimeter defense and static access controls struggle to adapt to new environments. This paper analyzes the roles of technologies including data encryption, anonymization, access control, trusted computing, and intelligent monitoring by examining risk evolution patterns, key technologies, and application bottlenecks. It proposes pathways to improve technical frameworks, optimize governance mechanisms, and strengthen collaborative protection strategies, emphasizing the critical importance of integrating technological solutions, institutional frameworks, and scenario-based governance approaches.

Keywords

big data; cyberspace security; privacy protection; data governance; security technology

大数据环境下网络空间安全隐私保护技术研究

尚子傲

河南理工大学，中国·河南 焦作 454150

摘要

大数据技术广泛应用推动了数据采集、存储、传输、分析与共享方式的深刻变革，同时也加剧了网络空间安全与个人隐私保护的风险。海量数据虽提升了治理效率、商业决策与公共服务水平，但也带来数据泄露、身份识别、行为追踪及算法滥用等问题。传统以边界防护和静态权限为主的安全模式难以适应新环境。文章从风险演变、关键技术与应用瓶颈出发，分析数据加密、匿名化、访问控制、可信计算与智能监测等技术作用，提出完善技术体系、优化治理机制和强化协同防护路径，强调技术、制度与场景治理协同的重要性。

关键词

大数据；网络空间安全；隐私保护；数据治理；安全技术

1 引言

在数字经济快速发展背景下，数据已成为重要生产要素。政务平台、社交媒体、电子商务、智慧医疗、在线教育及工业互联网等场景持续产生海量数据，网络空间逐渐成为社会运行的重要基础环境。与传统信息处理方式相比，大数据环境具有数据规模大、来源复杂、流动频繁、关联性强和挖掘深度高等特征，这使网络空间安全问题不再局限于系统入侵和信息窃取，而是延伸到个人隐私暴露、数据画像失控、用户行为预测和算法歧视等更深层次领域。隐私保护已成为网络空间安全治理的重要组成部分。如何在保障数据流通利用的前提下实现隐私边界控制、风险及时识别与全过程安全防护，已经成为学术研究和实践应用共同关注的课题。基于此，系统研究大数据环境下网络空间安全隐私保护技术，具有较强的理论意义和现实价值。

【作者简介】尚子傲（2006–），男，中国河南安阳人，在读本科生，从事网络空间安全研究。

2 大数据环境下网络空间安全隐私保护的现实背景

2.1 数据规模扩张重塑网络空间安全格局

大数据环境最显著的特征在于数据规模持续扩张。用户在网络空间中的搜索记录、消费轨迹、位置变化、社交互动、设备状态及生物识别信息被不断采集和存储，形成了高度细化的数据集合。数据数量的急剧增长，使网络攻击者拥有更多目标资源，也使防护对象由单一系统、单类文件扩展为多平台、多终端和多类型数据资产。攻击方式因此呈现链条化、隐蔽化和持续化趋势。对网络空间而言，数据已不只是被保护的对象，也成为攻击、渗透和操控的重要媒介。由此可见，大数据时代的网络空间安全已经从设备安全、系统安全逐步转向数据安全、关系安全与场景安全并重的综合格局。

2.2 数据关联分析加剧隐私暴露风险

大数据环境中的隐私风险，并不完全源于原始敏感数据的直接泄露，更常见的是多源数据关联分析带来的间接识别。用户即便未主动披露姓名、身份证号等显性身份信息，也可能因消费记录、设备编号、位置轨迹、社交关系和浏览偏好被重新识别。特别是在跨平台数据共享和算法建模广泛应用的条件下，原本分散、碎片化的信息经过整合后，可以勾勒出较为完整的个体画像。此类画像一旦被过度使用，不仅会侵害个人隐私，还可能影响用户在信贷、招聘、保险和平台推荐中的公平权益。隐私风险由“信息是否泄露”转变为“个体是否被过度识别与推断”，这对传统保护理念提出了更高要求。

2.3 数字化场景拓展提高隐私保护复杂程度

网络空间已深度嵌入政务服务、交通出行、医疗健康、智能制造和社会交往等各类场景，隐私保护不再是某一行业或某一平台的局部问题，而是贯穿全社会数字运行过程的系统任务。不同场景的数据类型、敏感程度、流通逻辑和应用目标存在明显差异。医疗数据强调高敏感性和长期保密性，金融数据强调真实性和不可篡改性，社交数据则更加突出行为分析和关系推断风险。场景多元化意味着隐私保护技术必须兼顾通用性与针对性，既要建立统一的基础防护框架，又要结合具体业务形成差异化策略。大数据环境下的隐私保护已经不再是单点技术问题，而是与场景治理深度绑定的综合命题。

3 大数据环境下网络空间安全隐私保护面临的主要问题

3.1 数据采集边界模糊引发过度收集问题

在平台经济和智能服务快速发展的推动下，数据收集行为呈现泛化趋势。部分应用在提供服务过程中超范围索取用户信息，将原本并非必要的数据纳入收集范围，造成隐私边界被不断扩张。用户在复杂条款和默认授权机制下，往往难以准确理解自身数据被收集、使用、共享和保存的具体方式。数据一旦被超量收集，后续即使采取一定安全措施，也难以从源头消除隐私风险。过度收集不仅增加泄露概率，还会使数据处理活动逐渐偏离服务本身，演变为平台画像、精准营销和行为操控的资源基础。由此造成的隐私侵害具有隐蔽性强、持续时间长和影响范围广等特征。

3.2 传统安全防护模式难以适应动态威胁

以往网络安全防护多依赖防火墙、入侵检测、身份认证和边界隔离等技术，这些手段在相对封闭的网络环境中能够发挥较好作用。但在云计算、移动互联网和物联网高度融合的背景下，数据跨端流转和远程调用已成为常态，传统边界日益模糊。隐私风险往往并非发生在单一节点，而是分布在数据生命周期的多个环节，如传输过程中的截获、共享过程中的越权调用、分析过程中的敏感推断、存储过程中的集中泄露等。若仍以静态隔离和单点防护为主，难以及时应对多链路、动态化和场景化的安全威胁。因此，需要由“围绕系统建防线”转向“围绕数据建防线”，形成更加精细、持续和自适应的安全体系。

3.3 技术应用与治理机制之间存在脱节现象

当前许多单位已经部署了数据加密、日志审计、权限管理等技术，但在实际运行中，技术应用效果并不稳定。其原因在于，部分组织对隐私保护的理解仍停留在合规应付层面，缺乏从业务流程重构、数据分类分级、风险评估和责任追溯角度进行系统设计。技术工具与管理机制没有形成闭环，导致安全措施存在碎片化、表面化问题。一些平台虽然采用了脱敏技术，但缺乏对共享对象和使用目的的动态审查；一些系统建立了访问控制规则，却未将岗位变化、权限继承和异常操作纳入实时监测。技术与治理脱节，使隐私保护停留在局部防护层面，难以形成整体效能。

4 大数据环境下网络空间安全隐私保护的关键技术体系

4.1 数据加密与安全传输技术

数据加密是隐私保护最基础也是最核心的技术手段。通过对静态存储数据和动态传输数据进行加密处理，可以有效降低数据被非法窃取后直接暴露的风险。在大数据环境中，加密已不局限于简单的文件级保护，而是需要面向数据库、分布式存储、云端交换和接口调用等多种场景进行协同部署。传输层加密能够保障数据在网络交换过程中不被轻易截获，存储层加密则可强化数据资产的底层安全。随着计算需求提升，如何在保证加密强度的同时兼顾系统性能，成为技术优化的重要方向。围绕密钥管理、分布式加密和可信执行等技术开展改进，能够进一步提升加密体系的实用性。

4.2 匿名化与差分隐私技术

面对大数据环境下强关联分析带来的识别风险，仅依赖删除姓名、电话等直接标识信息已难以实现有效保护。匿名化技术通过泛化、抑制、扰动和分组等方式削弱个体

识别特征，降低数据集在公开、共享或研究使用过程中的隐私泄露概率。差分隐私技术则通过向结果中引入可控噪声，使攻击者难以判断某一特定个体是否参与数据集，从而在一定程度上兼顾数据分析价值与隐私安全。此类技术在公共数据开放、用户行为研究和统计分析中具有较高应用价值。需要注意的是，匿名化并非绝对安全，若缺乏场景评估和参数控制，仍可能被重新识别。因此，匿名化与差分隐私更适合与分类分级管理、访问控制和审计机制协同使用。

4.3 访问控制与智能监测技术

隐私保护不仅要防止外部攻击，更要控制内部滥用。访问控制技术通过设定用户身份、角色权限、数据标签和操作范围，确保不同主体只能在授权条件下接触特定数据。相较于传统静态授权模式，大数据环境更加需要细粒度、动态化的控制机制，以适应岗位变化、业务调整和数据流动场景的持续变化。与此同时，智能监测技术借助日志分析、行为建模、异常识别和风险预警，对数据访问过程进行实时追踪，能够发现越权查询、批量导出、异常下载和高频调用等可疑行为。访问控制与智能监测结合后，可以从“事前限制”和“事中识别”两个维度提升隐私保护能力，形成更加立体的安全防线。

5 大数据环境下网络空间安全隐私保护技术的优化路径

5.1 构建覆盖数据全生命周期的安全防护体系

在大数据环境中，隐私风险呈现出贯穿数据全流程的特征，单一环节的防护已难以有效应对系统性威胁。以数据生命周期为主线构建安全体系，有助于实现从源头到终端的连续治理。在采集阶段，应以合法合规为前提，坚持最小必要与目的限定原则，通过数据筛选与结构化设计减少冗余信息进入系统；在传输过程中，应强化加密协议、接口鉴权与链路完整性校验，降低中间环节被截获与篡改的可能；在存储环节，需结合数据分类分级策略实施差异化加密，并通过多副本备份与物理隔离提升抗风险能力。进入处理阶段后，算法模型对数据的深度挖掘可能引发隐性泄露风险，应通过安全建模、参数保护及过程审计加以约束。数据共享环节则需依托脱敏处理、动态授权与用途约束机制，防止数据在跨域流通中被滥用。最终的数据销毁不仅是技术操作问题，更是合规责任体现，应确保数据不可恢复并具备可验证性。以生命周期为框架的系统性防护，有助于打破分散治理格局，形成闭环管理结构，从而提升整体安全韧性。

5.2 推动隐私计算与可信技术深度融合

数据要素流通的加速，使“数据可用”与“数据安全”之间的张力日益凸显，传统依赖数据隔离的保护方式已难以支撑跨主体协同的现实需求。在此背景下，隐私计算技术为实现数据价值释放提供了新的路径。通过多方安全计算、联邦学习及可信执行环境等机制，不同主体可以在不共享原始数据的前提下完成联合分析，从技术层面实现“可用不可见”。这一模式不仅降低了敏感数据直接暴露的风险，也为跨机构合作创造了条件。然而，单一技术路径难以支撑复杂应用场景，将隐私计算与身份认证、访问控制、区块链存证及安全审计等机制进行协同整合，有助于提升整体可信度与可追溯性。区块链的不可篡改特性能够强化数据使用过程的记录与验证，访问控制机制则保障数据调用的合规边界，安全审计为异常行为识别提供支撑。多技术融合所构建的复合型安全架构，不仅增强了用户对数据处理过程的信任，也为金融风控、智慧医疗及公共治理等领域的数据协同奠定了安全基础。

5.3 完善技术治理协同机制提升应用实效

隐私保护的有效性不仅取决于技术本身，更依赖其与制度安排及组织结构的深度耦合。现实中，部分机构在安全建设中存在“重技术部署、轻治理融合”的倾向，导致技术能力难以转化为实际防护效果。围绕数据治理的整体需求，应建立涵盖数据资产清单、敏感信息目录及风险评估机制的基础制度框架，使数据流转过程具备清晰边界与可控路径。在具体实施层面，技术方案需嵌入业务流程之中，通过事前评估、事中控制与事后审计形成闭环管理结构。对关键数据处理活动，应设置审批授权、操作留痕与责任追溯机制，强化组织内部的约束力与透明度。与此同时，复合型人才的培养同样不可或缺，研发人员需理解安全约束，管理人员应具备技术认知，一线运营人员则需掌握基本的隐私保护操作规范。通过制度、技术与人员能力的协同推进，隐私保护才能从静态配置转化为动态治理能力，在复杂多变的网络环境中持续发挥效用。

6 结语

大数据环境下，网络空间安全与隐私保护已经成为数字社会稳定运行的重要基础。数据规模扩张、跨域流动加速和智能分析深化，使隐私风险呈现出更强的关联性、隐蔽性和持续性，传统安全防护模式面临明显局限。围绕这一变化，数据加密、匿名化处理、访问控制、智能监测、隐私计算和可信技术等构成了当前隐私保护的重要技术支撑。与此同时，技术应用必须与数据治理、制度建设和场景管理相结合，才能真正回应复杂多变的网络空间风险。未来，应继续推动安全技术创新、优化全生命周期治理体系、完善协同防护机制，在保障数据价值合理释放的同时守住隐私安全底线，为数字经济健康发展和网络空间治理现代化提供坚实保障。

参考文献

[1] 付文伟.大数据环境下用户隐私保护与网络安全策略研究[J].中国电信业,2025,(08):54-57.

[2] 张璁,倪弋.筑牢网络空间安全屏障——党的十八大以来网络安全工作综述[J].平安校园,2026,(Z1):70-73.

[3] 杨军.网络空间中数字身份认同与个人隐私保护[J].数字通信世界,2025,(01):181-183.