网络安全视角下用户数据隐私保护技术路径与实践研究

李丽春
广西壮族自治区贺州市富川瑶族自治县福利镇便民服务中心，广西 贺州 542706
DOI: 10.61369/TACS.2026020047

摘　　要： 在数字化全面渗透的当下，用户数据已成为核心生产要素，而网络安全威胁持续升级，用户数据隐私泄露、滥用问题频发，不仅侵害用户合法权益，也扰乱数字经济秩序，更对网络空间安全构成严峻挑战。本研究以网络安全基础视角为进入研究的点，深度分析用户数据在整个存续周期和常见攻防场景里的核心薄弱点，发掘技术、管理、法律范畴的关键问题点，搭建具有基础防护、核心突破、内控防御、外部阻断、闭环管控的弹性化隐私保护技术体系架构，联合企业平台实践和代表性行业的实施局面，制定可推行的操作方案和推进环节，希望为多方参与者建立数据隐私保护体系从而找到安全防护与价值转化的恰当均衡点，使网络空间安全治理和数字产业协同更好发展。

关 键 词： 网络安全；用户数据；隐私保护

Research on the Technical Path and Practice of User Data Privacy Protection from the Perspective of Cybersecurity

Li Lichun
Convenience Service Center, Fuli Town, Fuchuan Yao Autonomous County, Hezhou City, Guangxi Zhuang Autonomous Region, Hezhou, Guangxi 542706

Abstract: In the current era of comprehensive digital penetration, user data has emerged as a core production factor. However, with the escalating cybersecurity threats, frequent incidents of user data privacy breaches and misuse not only infringe upon users' legitimate rights and interests but also disrupt the order of the digital economy and pose severe challenges to cyberspace security. This study takes a fundamental perspective of cybersecurity as its entry point, thoroughly analyzing the core vulnerabilities of user data throughout its lifecycle and in common attack and defense scenarios. It identifies key issues in the technical, managerial, and legal domains, constructing a resilient privacy protection technical system architecture that encompasses basic protection, core breakthroughs, internal control defenses, external blocking, and closed-loop management. By integrating practical experiences from enterprise platforms and implementation scenarios in representative industries, this study formulates actionable plans and implementation steps. It aims to assist multiple stakeholders in establishing a data privacy protection system, thereby finding an appropriate balance between security protection and value transformation, and fostering better coordination between cyberspace security governance and the digital industry.

Keywords: cybersecurity; user data; privacy protection

引言

依托大数据、云计算、物联网、人工智能等数字技术的急剧拓展，各领域数字化发展进程的加快十分明显，用户数据获取、积累、流通及开发的规模正快速增大，数据的价值愈发有价值，然而在这同时，网络威胁模式越来越精细地分化，数据黑灰产产业链已进入成熟的时期，隐私数据流失事故不断冒出来，从个人认证相关档案、通话明细到消费行踪与面部识别的特性，核心隐私数据所面临的安全风险越来越大。从网络防御维度做相关考量，用户数据隐私防护其实是保障个人权益的核心要点，更是维护网络环境平稳、健全数据交易准则、助力数字经济合规化的根基，我国逐步让《网络安全法》《数据安全法》《个人信息保护法》等基础法律得以实施，为用户数据隐私保护勾勒了法律框架，但技术水平防护有局限、管理结构有缺陷、落实环节有偏差，还是制约隐私保护水平的主要痛点。本论文从网络安全实际应用的相关层面出发，专注于用户隐私数据所遭遇的实际威胁，全方位熟悉关键技术防御的路径，研发贴合实际的运作模式，跨越现有文献理论扎实但实践不充分、技术先进却推广不到位的瓶颈，为各类数据运营方创建能复制的集成化隐私安全路线。

作者简介：李丽春（1977.02-），女，汉族，广西富川人，本科，职称：工程师，研究方向：计算机网络工程。

一、网络安全视角下用户数据隐私面临的核心威胁与风险

（一）数据全生命周期各环节的安全风险

数据从采集、保存、运作、流转、共享到清除的闭环流程，各个流程的节点都有数据泄露方面的风险，而且风险体现出扩散的特点，单个环节的沦陷会很快蔓延成全局性的隐私泄露大事件，刚开始的数据采集阶段，个别数据收集组织背离“最小必要”原则，超出必要范围去采集用户隐私数据，硬性要求非必要权限，不取得用户许可暗地里采集数据，给后续隐私风险埋下基本诱因；众多资料用可读文本混合存储的办法，没有达成数据的分级管控，云技术存储规划不恰当并且数据库防御体系薄弱表现突出，有整体数据外漏的可能性；超出约定界限利用数据、未被授权分析用户特征、算法杀熟情况较多，个别平台以数据串联分析操作反推用户隐私内容，夺走用户知晓信息及做出选择的权利；未使用对数据加密传输的办法，数据经由网络传送存在被截取和修正的问题；数据交互跟完全清除阶段，合作方数据管理方面有漏洞，销毁操作没有达到标准，只是做了形式上的删除仍留存底稿，遗留信息能凭借技术方法重新得到手，使得数据保护存在长期的不足点。

（二）典型网络安全攻击引发的隐私泄露

网络攻击手段的革新直接造成用户隐私数据向外流出，恶意手段一点一点升级强化，抵御的难度逐渐增大，主要的网络攻击类型涉及木马病毒、勒索病毒、SQL 注入、钓鱼攻击、中间人攻击、DDoS 攻击之类的，其中针对数据系统的定向攻击破坏力在众多攻击里最大，侵入者借助 SQL 注入的不足突破数据安全的关卡，非法下载用户核心隐私数据；钓鱼攻击使用伪造的合法网站链接及电子邮件，欺骗用户提供登录用的凭证和个人身份方面信息，有目的地窃取个人数据；中间人攻击对网络数据的流动进行偷听，打破未加密通道窃取核心数据；勒索软件侵入设备之后把文件加密锁定，还会造成资料毁坏，进而威胁公开数据以换来经济上的收益，APT 高级持续性攻击针对主要平台做长期潜伏，几乎没有存在感，若防御关卡被拿下，会造成大范围高敏感特性的用户信息外漏，且之后取证的难度猛然增大，对网络安全体系及隐私数据造成极大的破坏。

（三）技术、管理、法律层面的现存痛点

现时期用户信息隐私保护相关工作，在技术、管理和法律三个核心层面都显露出明显不足，联防联控体系有体系性不足，部分中小微企业技术防御的水平比较低，加密系统、权限划分以及安全检测技术有薄弱点，复杂隐私计算系统实施费用较多协同性不好，技术安全的屏障有明显不足，并且现有防御体系抵抗不了新型网络攻击；许多企业没有设立好完善的数据安全治理机制，数据安全岗位专职人员是空缺的，内部人员权限约束的力度比较弱，违规行为和内部数据泄漏一直禁而不停，欠缺数据安全评估和追责的相关框架；部分主体缺乏法律相关的认知，没有完全落实个人信息保护相关法规，合规体系有名无有效功能，区域性和平台层面的数据隐私法律协同有缺口，打击数据黑灰产的力度要进一步增强，缺乏威慑效果的惩处机制使部分机构冒险行事，进一步造成隐私保护矛盾的加剧。

二、核心技术路径：网络安全驱动的用户数据隐私保护技术体系

（一）数据加密类核心技术（基础防护路径）

数据加密技术作为隐私保护关键支撑，利用密码学方法对信息予以加密，做到让数据“看不见、没法用、改不了”，成为防止外来攻击和内部数据外漏的第一关卡，现代加密体系由对称加密以及非对称加密共同搭建而成，对称加密算法（如 AES）加解密高效且资源占用少，满足大规模数据存储加密方面的需求；非对称加密算法（如 RSA）在安全程度上更占上风，是为密钥传送以及认证环节专门设计。运用哈希算法对数据完整性加以校验，杜绝数据遭未被准许的篡改；开展核心内容的相关处理，把脱敏加密及格式维持加密手段进行融合，基于数据原格式做到对隐私要素的隐藏处理，满足安全防护及功能完好的双重规定，当功能实现的时候，用户登录的凭证、DNA 声纹等生物特征和交易记录等主要数据，运用端到端加密做存储与传输，阻断未处理数据泄露出去的途径，以技术体系阻断核心数据的直接呈现。

（二）隐私增强计算技术（核心突破路径）

隐私增强计算技术达成数据“可用不可见”这一核心特性的达成，协调数据分发和隐私维护之间的矛盾之处，同时达成数据价值开发和隐私安全两个诉求，核心技术采用的技术有联邦学习、安全多方计算、差分隐私、同态加密、可信执行环境等，联邦学习使模型游走数据留存下来，多节点联合学习达成数据的去中心化，减小数据集纳所造成的敏感数据暴露程度；安全多方计算使多参与方在不泄露原始数据前提下开展联合计算，防止各参与方隐私数据被泄露；差分隐私以掺杂随机噪声的技术维护隐私，制止攻击者借助结果数据反向破译个人隐私；采用同态加密可以在密文情形下开展计算，解密后的数据结果和明文直接计算的结果一样，运算全程都保证初始数据是加密的，这个技术框架可对数据开放共享、协同运算和机器学习等应用场景起到支撑作用，有力打破数据共享环节的隐私保障屏障，成为作为安全防护和隐私管理双轮驱动的关键技术依靠。

（三）数据访问与权限管控技术（内控防护路径）

数据访问及权限管控技术把防控内部风险作为核心，运用严密的权限分配和整个过程的访问把控，防范内部成员违规访问及越权操作造成的资料泄漏，夯实内部安全的基础，核心机制由 RBAC 访问体系、授权最小化的规则、组合身份验证方法、操作审计与日志追踪网络组成。先根据标准对用户数据做分级归类，界定各级别数据的可访问权限和操作空间大小，扎实落实最低必要权限准则，仅使相关人员拿到工作所需的最少权限；建造组合式身份鉴别的体系，开展多维度的访问鉴权工作，防止不合规权限越界；搭建用于数据操作的审计平台，对数据查阅、变更、转移的全流程各阶段进行监测，收集起操作日志，马上揪出违规操作并保证事后责任精确确定，搭建“权限设定 – 身份核实 – 访问管控 – 审计问责”的闭环管理体系。

（四）网络传输与边界安全技术（外部防御路径）

网络传输与边界安全技术核心工作是抵御外部网络的威胁，

抵御外部网络的攻击、通信窃听及数据被劫持等安全相关隐患，夯实数据在跨域传输以及流程交互中的防护基础，基础技术架构所涉及的包括 SSL/TLS 加密传输协议、防火墙、入侵检测与防御系统（IDS/IPS）、VPN 虚拟专用网络、网络边界隔离技术等。凭借 SSL/TLS 技术框架达成数据传输的整体加密，阻止信息在传输过程当中被第三方非法监听或截获；采用防火墙和入侵检测方案一起用，开展网络流量动态查巡机制，遏制恶意攻击及非法入侵现象，马上察觉并挡住异常数据流动；在网络间远距离数据传输的相关场景，借助 VPN 技术确立安全的私有通信路由，创建网络隔离联合数据加密的双重安全屏障；同时对网络边界开展精细化管理，把内部核心数据系统跟外部网络做物理分隔，减小单一防御边界有缺陷造成的系统级连带风险。

（五）数据销毁与生命周期管控技术（闭环防护路径）

数据销毁及生命周期管控技术使数据处理全流程达成闭环式规范，填补数据销毁阶段的安全缺陷空缺，消除数据残留造成隐私泄露的潜在威胁，达成“起源 – 发展 – 终结”全链路防护的封闭链路，核心能力由数据分级分类的生命周期管理、自动去除信息操作、擦除和物理破坏手段、数据残余的检验办法组成。打造覆盖数据全生命周期的管理办法，定下不同类型数据的采集时限、保存时间和应用领域，保存期限一到的数据自动进行销毁；对于以电子版存在的数据而言，采用迭代式数据销毁之后再重写的技术，把介质上的信息残留全部清除，杜绝利用技术手段使数据复原；在存储介质面临淘汰的时候，利用机械破碎以及磁场销毁的手段，保证数据彻底没法恢复；一并建设数据生命周期管理中心，实时了解数据交换情况，及时对超出期限存储以及非法留存的数据示警，达成数据全流程可监控、可操作、可追溯。

三、实践落地：根据场景来的隐私保护实施办法与操作环节

（一）企业 / 平台层面的整体实践框架

企业跟平台作为信息处理的核心方面，要建设“技术 + 管理 + 合规”三位一体的综合工作架构，达成隐私保护无缺失实施，基于现有的数据规模以及业务样式，按层次落实加密、权限管理和传输防护等基础技术，资源充裕的主体当慢慢采纳隐私增强计算技术；创建专门的数据安全工作队伍，制定完善的数据安全条例和岗位操作办法，按时组织网络安全及隐私保护专题学习，增强从业人员防泄密的警觉意识；切实履行《个人信息保护法》等相关法规提出的要求，对用户授权体系进行改良，拟定一目了然的隐私说明，进行数据合规检查和风险管理，接受监管机关进行的检查及指导，一并推行个人隐私泄露应急管控相关机制，制定泄露预警方案设计、应急响应操作流程、溯源追查责任流程、通知用户情况、风险补救办法等程序，切实减少隐私泄露事件所产生的不良后果。

（二）典型应用场景实践方案

基于各行业场景所提出的隐私保护要求，设定灵活的实施办法，做到场景贴合度和安全实效的统一，网购及线上服务所涉及的平台场景，着重加强对用户个人消费记录和支付相关数据的保护，推进属性级脱敏协同加密存储，做好权限差异化的管控措施，杜绝差异化定价以及隐私侵犯；理财投资相关行业，针对用户支付账户、交易的买卖记录、信用相关资料等保密数据，借助深度加密办法、组合式认证和隐私保护计算的技术，增强交易数据在传输及存储过程中的防护程度，避免金融凭证失窃以及虚假交易发生；智慧医疗实施相关场景，保障患者诊疗记录检验结果及生理特征等敏感信息，运用联邦学习方案来开展医疗数据的联合挖掘，同时开展脱敏和加密工作，不允许任何样子的医疗数据违规转送；物联网相关的数据采集场景，针对互联装置所收集的个人活动轨迹和场所标记，加大终端设备数据加密方面措施，对数据采集权限分配予以规范，把好数据传输的安全门槛，阻挡设备安全隐患造成的隐私损失。

（三）隐私保护技术落地实施步骤

为让技术有序开展下去，规避冒进采用造成预算超支和安防隐患，利用标准工作流程逐步开展，进行数据安全隐患的梳理以及级别界定，全方面核查企业数据存量，审查数据处理活动合规方面的问题，按安全级别对数据的层级进行分类，选定核心的防护要点；开展安全方案筛选和平台搭建，按风险分级结论和实施的要求，选用相称的技术防护体系，先开展基础加密措施、权限管理机制和边界防护技术的实施，之后逐步完成对隐私计算高端技术的引入；开展配套制度实施及人才培养，同步强化制度在各方面的约束，确切明确岗位权责的限度，进行企业全员的风险防范相关培训，提升技术使用与风险应对本事；对防御体系进行评估并修复漏洞，对上线的防护系统做承压测试、缺陷探查和攻防模拟，找出防护问题，整治系统潜在的不足；第五步，常态化运维与迭代升级，安排专人负责系统运维，实时监控安全状态，根据新型网络攻击与业务变化，及时更新技术与防护策略，保障隐私保护长效性。

四、结束语

网络安全视角下的用户数据隐私保护，是一项系统性、长期性工程，关乎个人权益、产业发展与网络空间安全。在数字技术持续迭代、网络威胁不断升级的背景下，单一防护手段难以满足隐私保护需求，必须构建全生命周期、多层级、技术与管理协同的防护体系。本文梳理的核心风险、技术路径与实践方案，立足行业实际，兼顾实用性与合规性，可为各类数据处理主体提供参考。

参考文献

[1] 王林，魏嘉贺 . 数字经济时代下网络安全情报共享与协同防控策略研究 [J]. 情报杂志，2025(11).

[2] 任昊 . 新型网络环境下的数据安全与隐私保护关键技术研究 [D]. 电子科技大学，2020.

[3] 张益锋，秦云，朱先德 . 云计算下网络安全技术实现的路径分析 [J]. 计算机产品与流通，2019(6):2.DOI:CNKI:SUN:WXXJ.0.2019-06-020.

[4] 邱宝强 . 面向云计算平台的数据安全问题和保护策略研究 [J]. 数字通信世界，2023(3):11-13.

