大数据信息安全保护策略研究

赖一阳
全域数据信息安全重点联合实验室，北京 100021

DOI: 10.61369/TACS.2026010005

摘　　要： 在数字经济快速发展的背景下，大数据技术的广泛应用推动了各领域转型升级，同时也带来严峻的信息安全与隐私保护挑战。大数据具有海量性、多样性、高速性和价值性等特征，其信息安全保护已成为保障数字经济健康发展、维护个人合法权益和社会公共利益的关键。基于此，本文针对大数据信息安全保护策略展开研究，分析当前大数据信息安全与隐私保护的主要挑战，梳理相关关键技术，探讨数据安全防护、数据备份与恢复等核心技术的理论内涵，提出针对性保护策略，为构建完善的大数据信息安全防护体系提供理论参考。

关 键 词： 大数据；信息安全；隐私保护；防护技术；保护策略

Research on Information Security Protection Strategies for Big Data

Lai Yiyang
Key Joint Laboratory for Global Data and Information Security, Beijing 100021

Abstract: Against the backdrop of the rapid development of the digital economy, the widespread application of big data technology has driven the transformation and upgrading of various sectors, while also posing severe challenges to information security and privacy protection. Characterized by volume, variety, velocity, and value, big data information security protection has become a key element in safeguarding the healthy development of the digital economy, protecting individuals' legitimate rights and interests, and upholding social public interests. Based on this, this paper conducts a focused study on big data information security protection strategies. It analyzes the major challenges currently facing big data information security and privacy protection, sorts out relevant key technologies, discusses the theoretical connotations of core technologies such as data security defense and data backup and recovery, and proposes targeted protection strategies, thereby providing theoretical references for constructing a comprehensive big data information security defense system.

Keywords: big data; information security; privacy protection; defense technology; protection strategy

引言

随着信息技术迭代升级，大数据已渗透到社会生产、生活、治理各领域，成为驱动数字经济发展的核心生产要素。大数据技术可实现海量异构数据的采集、存储、分析与挖掘，为企业决策、公共服务优化、科技创新等提供有力支撑。但大数据的海量性、多样性、高速性、去中心化等特征，打破了传统信息安全防护边界，使信息安全风险呈现扩散化、复杂化、隐蔽化特点。因此，加强大数据信息安全保护研究，构建适配大数据特征的防护体系，具有重要理论意义和现实价值。

一、大数据信息安全与隐私保护挑战

（一）数据隐私泄漏风险突出

大数据应用环境下，数据采集涉及个人身份信息，财产情况以及行为轨迹等敏感领域数据，获取数据呈现隐蔽性、覆盖范围广且成本较低等特点，部分主体在未严格履行告知义务及用户授权程序的情况下，非法采集、存储甚至是泄露隐私数据的现象屡有发生，造成了更为突出的数据安全风险与侵权隐患。基于大数据关联性特征，分散的非敏感数据经关联分析后能提炼出用户隐私信息并构建“数据画像”，隐私泄漏风险会大幅增加。存储安全漏洞、传输加密缺失、访问权限管控不足等问题都会使隐私数据面临被非法获取、滥用或传播等威胁，个人合法权益会受到侵害。

（二）数据安全防护难度加大

大数据的海量性使存储规模持续扩大，传统的硬件设备和架构设计已经无法满足实际应用场景的需求，在这种情况下，分布式存储以及云计算等创新技术开始逐渐兴起，并且在一定程度上增加了信息安全防护的技术难度和复杂程度。在分布式环境中，数据被分散在不同的节点之中，各个节点的安全防御水平存在较大差异，任何一个节点的安全漏洞都有可能对整个系统造成威

胁。大数据存在多种属性，结构化、半结构化、非结构化的混合数据形式，不同种类的数据防护需求和技术达成路径存在差异，单一的安全保障方式难以应对复杂局面的现状。

（三）安全管理体系不完善与

当前多数组织在大数据应用中，缺乏完善的信息安全管理体系，未建立健全管理制度、责任体系和流程规范，存在权责不清、流程混乱、监管缺位等问题。部分机构觉得数据安全不重要，没有专业的技术支持人员或者专职管理人员，没法有效地实施风险评判和危险探查任务，进而让存在的安全威胁更加广泛。

二、大数据信息安全保护的关键技术

（一）数据安全防护技术

1. 加密技术

作为大数据安全的重要技术保障，加密技术借助特定加密算法，将原本的信息转变为难以轻易解读的内容，唯有合法持有密钥的主体方可借助密钥逆向还原，其核心功能是防止数据遭受非法访问和篡改。在大数据时代背景之下，加密技术主要分为对称和非对称这两种基本形式，对称加密依靠一个密钥就可以实现对数据的高效传输，由于操作起来非常简便并且计算开销比较小的缘故，对称加密被大量应用在大规模数据处理的场景当中，像DES、AES这种经典算法就属于典型代表；而相对而言，非对称加密依靠公私钥配对的形式提供更为优良的安全性能，而且在管理密钥方面也显得更加简便，在数字签名和安全通信等场景里展现出显著优势，像RSA、ECC这样各种主流方案都有所涵盖。此外，同态加密算法以及差分隐私技术正快速地向实际应用场景推进，同态加密算法通过执行对密文的算术运算的方式，在保证数据安全的同时提高数据的利用效率；差分隐私技术通过在原始数据中加入随机扰动的方式，将个体的特征信息进行模糊处理，达到隐私保护和数据分析的协同作用[1]。

2. 访问控制技术

访问控制技术通过准确设置主体权限，阻止非法操作，保证数据只被获准使用者获取和使用，传统自主访问控制（DAC）和强制访问控制（MAC）难以应对大数据环境下动态性与多样性带来的问题。大数据时代背景下，访问控制技术正朝着精细化，动态化方向发展，RBAC凭借职能划分实施权限划分，简化管理环节，提升运营效率，适用于权限等级清晰的组织；ABAC依靠主体、客体、环境要素创建实时授权模型，表现出更加强大的安全防护能力，而且在大规模分布式数据环境当中，在适应多样化安全需求方面表现得更为高效[2]。

3. 防火墙与入侵监测技术

作为网络安全基础设施的核心组成部分，防火墙肩负筛选并管控网络数据流的重要职能，依靠预先设定的安全策略，防火墙可以精准分辨合法的通信行为以及隐藏的威胁，有效阻挡外部恶意攻击对大数据系统造成的侵害[3]。传统的防火墙在应对新型的安全问题时弊端明显，下一代防火墙（NGFW）整合了入侵检测，应用识别等功能模块，大幅提高了数据分析能力，在对异常流量的特征进行实时监控之后及时作出反应，显著提升了整体的防护水准。入侵监测技术（IDS）与防火墙相互配合，实时监测网络流量、系统日志等，发现异常和入侵行为并报警，管理人员可以及时进行处理。IDS主要分为基于特征监测和基于异常监测两种，基于特征监测（识别已知攻击）和基于异常监测（建立正常模型、识别未知攻击）。

4. 安全审计与监控技术

安全审计与监控技术对系统操作和数据传输过程实时追踪并全面记录，形成对数据安全状态的动态监测，为事故后续调查提供精准数据。在大数据背景下，安全审计最主要的作用就是为处理海量数据提供支持，安全审计对数据全生命周期的操作轨迹进行全程记录，通过对安全审计的相关信息进行深度解析，以识别其中潜藏的风险因素，为决策提供精准依据。安全监控与安全审计相比更偏向于对数据进行实时动态的监测，通过对设备运行状态、网络流量变化情况进行实时动态监测，使用完善的系统架构进行数据信息的实时监控，一旦出现异常变化立即发出警报信号，从而达到最优的安全防护效果，提高监控系统的响应速度和准确率[4]。

（二）数据备份与恢复技术

1. 数据备份技术

数据备份作为保障大数据安全的重要技术手段，是将信息同步到其他的存储载体上，进行冗余保存，在原始数据出现破坏或丢失的时候，通过已经建立的副本就可以进行数据恢复，从而保证数据的完整性和持续可用性。在大数据技术的支持下，传统备份架构主要包含全量、增量和差异这三种基本模式。全量备份能够保证数据的完整性，但是备份的时间比较长，存储空间的需求也比较大，比较适合对关键业务的周期性数据进行保存。增量备份则是关注新增或修改信息的变化特征，具有高效低资源占用的特点，在高频操作场景下，它被广泛应用于日常的运维管理[5]。差异备份会针对自上次全量备份之后发生的变动内容予以记录，既保证了全面覆盖又提升了执行效率。

2. 数据恢复技术

数据恢复技术与备份策略相互依存，基本目标是通过冗余存储或其他方式补偿数据丢失的现象，保证信息的持续可用性，面对大规模数据环境的还原需求，重点应放在提高系统处理性能和减少损失上[6]。数据恢复技术包含即时、快速、完全三种，即时恢复以高效见长，适合对数据实时性要求高的场景；快速恢复兼顾完整性和效率，大规模数据集重建时优势明显；完全恢复致力于精准还原受损信息至初始状态，在核心业务系统里应用广泛。智能化转型持续深入，利用人工智能算法设计自动化修复流程成为可能，操作便利性提升，效能和运维成本优化。

三、大数据信息安全保护策略

（一）构建完善的大数据信息安全管理体系

构建完善的管理体系是大数据安全管理的重要依托。首先，构建起一个完善的系统性安全管控机制，详细规定安全管控在数

据生命周期各个时段的具体要求与操作标准，还要判定部门与人员在数据安全中肩负的职能界限，创建一个权利责任明确、步骤仔细无遗漏并具备监督力度的系统架构[7]。其次，完备全员化安全责任网络，做好各工作岗位的细致分工并执行动态监测试点，保证信息防护在全过程持续有效。此外，加强安全风险管理的重点是创建常态化的风险监控和评价体系，全方位地摸排潜藏的系统性隐患，依照预先认定的高危点制订有针对性的防范策略；要巩固应急管理的机制，规划编制流程，并规范负责部分和处置步骤，以便在突发情况出现的时候实现有效的处理行动，在处理过一段时间后结合实际予以反馈，争取后续的一些巩固和改善[8]。

（二）强化大数据信息安全技术创新与应用

技术创新是增强防护效能的主要动力，要加大研发投入，促使安全技术不断演进，要重点关注新式加密算法，访问控制模型以及入侵检测系统的研发设计。要加快同态加密，差分隐私等前沿技术的应用进程，还要深入优化传统权限管理机制的功能，从而全方位改善安全保障水平。此外，亟须推进安全技术的集成化应用，把多源关键技术要素融合起来，形成事前预警，实时监控，事后响应的全链条防护体系，健全完善协同联动的安全保障机制[9]。

（三）健全大数据信息安全法律法规与合规管理

健全的法律法规体系是信息安全的重要保障，需完善大数据安全领域的立法架构和政策标准，弄清楚数据处理主体所具有的权利义务界限；细化具体职责范围，设置专门针对新型安全威胁和隐私侵权行为的条款，明确清晰的法律责任划分和处罚规则，加大违法行为的成本压力。同时，应形成包含数据安全技术标准、组织架构设置、评估体系在内的综合性标准体系，为企事业单位的实践工作提供依据。企业要增强合规管控职能，严格依照法律法规和行业准则，创建系统化的内部监督体系，定时开展全面审计，找出潜在的风险并及时处理，以此避免违规行为产生的安全和法律问题[10]。

四、结语

综上所述，大数据技术为数字经济注入强大动力，但也带来严峻的信息安全与隐私保护挑战。在大数据信息安全保护工作中，数据安全防护、备份与恢复技术是核心支撑，应构建完善管理体系、强化技术创新应用、健全法律法规与合规管理，提升防护能力。大数据信息安全保护是系统性、长期性工作，需多方协同发力，构建多元协同的保护格局。在后续工作中，需持续加强理论研究和实践探索，适配大数据技术迭代需求，不断提升安全防护能力。

参考文献

[1] 陶海敏 . 大数据时代的隐私保护和信息安全管理 [J]. 山西电子技术 ,2024,(06):71-72+109.

[2] 张萍 . 大数据背景下档案管理信息安全与隐私保护策略研究 [C]// 延安市教育学会 . 第五届创新教育与发展学术会议论文集（一）. 中共陕西省委党校（陕西行政学院）;,2023:623-630.DOI:10.26914/c.cnkihy.2023.090658.

[3] 安博 , 李敏杰 , 陈宏伟 . 学生信息安全与隐私保护：大数据时代的关切 [J]. 数字通信世界 ,2024,(10):217-219.

[4] 李春生 . 基于区块链技术的医疗信息安全与隐私保护研究 [J]. 电脑编程技巧与维护 ,2024,(10):59-61+65.DOI:10.16184/j.cnki.comprg.2024.10.049.

[5] 邱蕾 . 情报视角下科技论文出版数据信息安全风险与管控 [J]. 科技与出版 ,2024,(10):113-118.DOI:10.16510/j.cnki.kjycb.20241014.006.

[6] 晏庆 , 崔浩贵 , 刘冰 , 等 . 大数据时代下计算机信息网络安全问题研究 [J]. 无线互联科技 ,2024,21(17):102-104+115.

[7] 徐来凤 , 邱辉 . 基于大数据的公共政策制定中隐私权保护的行政法研究 [J]. 法制博览 ,2024,(24):25-27.

[8] 梁晓强 . 基于大数据技术的网络信息安全防护策略分析 [J]. 电子技术 ,2024,53(08):316-317.

[9] 唐桥 . 检察视角下的数据知识产权保护问题研究 [C]// 第五届全国检察官阅读征文活动获奖文选 - 优秀奖 . 四川省巴中市巴州区人民检察院 ;,2024:221-228.DOI:10.26914/c.cnkihy.2024.009062.

[10] 王钰婷 , 廖周宇 , 覃琪 , 等 . 大数据信息安全背景下数据库课程教学改革研究 [J]. 信息与电脑（理论版）,2024,36(13):130-132.

