 DOI: https://doi.org/10.12349/iser.v6i2.4797

Bank big data privacy protection technology and information security governance

Qinglei Feng

Shenzhen Qianhai WeBank Co., Ltd., Shenzhen, Guangdong, 518063, China

Abstract

With the rapid development of Internet information technology, big data has become an important resource for the banking industry, providing strong support for its business innovation and risk management. However, the application of big data technology also has some disadvantages, which bring great challenges to the privacy protection and information security governance of banks. Based on this, this paper starts from the current situation of bank big data privacy protection technology and information security governance, analyzes the advantages and disadvantages of existing technology and governance methods, and puts forward corresponding suggestions for improvement. Through in-depth research on encryption technology, data desensitization, privacy computing and other technical means, as well as perfect data governance system and information security management system, in order to provide theoretical reference and practical guidance for bank big data privacy protection and information security governance.

Keywords

banking; big data; privacy protection technology; information security governance

银行大数据隐私保护技术与信息安全治理

冯庆磊

深圳前海微众银行股份有限公司，中国 · 广东 深圳 518063

摘　要

随着互联网信息技术的快速发展，大数据成为银行业的重要资源，为其业务创新与风险管理提供了强大支持。然而，大数据技术的运用也存在一定的弊端，给银行的隐私保护和信息安全治理带来了巨大挑战。基于此，本文从银行大数据隐私保护技术和信息安全治理的现状出发，分析现有技术和治理方法的优势与不足，并提出相应的改进建议。通过深入研究加密技术、数据脱敏、隐私计算等技术手段，以及完善的数据治理体系和信息安全管理体系，以期为银行大数据隐私保护和信息安全治理提供理论参考和实践指导。

关键词

银行；大数据；隐私保护技术；信息安全治理

1 引言

信息技术持续发展，数据规模不断扩大，形成了海量的数据资源。银行业作为数据密集型行业，积累了大量的客户信息和业务数据，大量的数据既是银行推动业务创新和服务升级的重要资源，也是其面临的主要安全风险。近年来，个人信息泄露事件频发，引发了社会对数据隐私保护的广泛关注，而黑客攻击、内部人员泄露等信息安全事件也时有发生，给银行的声誉和财产安全带来严重威胁 [1]。银行需要认识到此类问题的严重性，加强大数据隐私保护技术和信息安全治理，以保障银行业务的稳健发展。

【作者简介】冯庆磊（1981–），男，中国山东潍坊人，硕士，从事信息安全领域研究。

2 银行大数据隐私保护与信息安全治理的现状

2.1 数据规模越来越大

随着银行业务的迅猛扩张及客户基数的急剧上升，数据体量正经历着前所未有的爆炸性增长。这一增长趋势不仅显著体现在数据总量的飞跃上，更深层次地反映在数据结构的日益复杂和对实时处理需求的急剧提升。面对如此庞大的数据集，高效且稳定的存储解决方案变得至关重要，而传统存储手段在应对这一挑战时显得捉襟见肘，给数据存储领域带来了新的难题。同时，数据的处理与分析任务也承受着巨大负荷，迅速从海量数据中提炼出有价值的信息，已成为银行业亟待攻克的关键问题。此外，数据规模的急剧膨胀还直接加剧了数据泄露的风险，保障数据在传输、存储及应用全链条中的安全性，已成为银行信息安全管理体系中的核心议题。

2.2 数据种类多样化

银行数据种类繁多，涵盖结构化数据、半结构化数据和非结构化数据等多个领域。结构化数据，诸如客户信息、交易记录等，具备清晰的格式与定义；而半结构化数据，例如日志信息、电子邮件等，其格式则较为灵活多变；至于非结构化数据，则涵盖了图片、音频、视频等多种多媒体形式[2]。各类数据因其独特属性与潜在风险点，为数据隐私防护及信息安全管理工作增添了极大的复杂性。银行需针对各类数据的特性，设计并实施差异化的保护策略，以确保数据的完整无损与高度安全。

2.3 外部风险加剧

近年来，银行遭遇的信息安全事件频发，包括黑客侵袭与内部人员数据泄露等，使其面临的外部风险日益加剧。外部风险不仅源自传统的网络攻击，诸如病毒、木马程序及钓鱼网站等，还涵盖利用大数据与人工智能技术的新型攻击手段，如高级持续性威胁（APT）及勒索软件攻击。这些新型攻击以其高度的隐蔽性、漫长的持续周期及巨大的破坏潜力，给银行的信息安全构成了严峻的挑战。鉴于此，银行亟需不断强化其信息安全防护体系，提升抵御外部威胁的能力。

3 银行大数据隐私保护技术

3.1 加密技术

加密技术是确保数据安全不可或缺的基础防线，在数据的传输与存储流程中，银行采纳先进的加密技术来捍卫数据的机密性和完整性，其中常见的加密算法有 AES（高级加密标准）和 DES（数据加密标准）等。借助加密技术，即便数据在传输途中被拦截，若无相应的解密密钥，也无法窥探其中的内容。此外，银行还运用了文件夹加密技术和数据快照备份机制，以保障数据在存储阶段的安全性。加密技术的应用范畴不仅局限于静态数据，还涵盖动态数据的防护。例如，在客户利用网上银行或手机银行服务时，银行通过 SSL/TLS 协议实现数据的加密传输，有效防止数据在传输过程中被非法获取或篡改。

3.2 数据脱敏

数据脱敏技术是一种在数据处理流程中专门用于保护数据隐私的手段，其核心目标是在不干扰数据分析流程及结果的前提下，确保数据的隐私安全。在客户数据的收集、存储及处理各个环节，银行需对敏感数据实施脱敏处理，以规避数据泄露所引发的潜在风险。数据脱敏通常依赖于数据屏蔽、数据替换及数据加密等多种策略来实现。举例来说，在数据分析的实践中，银行可以对客户的姓名、身份证号码、银行卡号等敏感信息进行替换或加密，从而在保持数据分析价值的同时，确保无法直接追溯至具体的个人身份信息。此外，银行亦可采用数据扰动技术，对原始数据进行随机化处理，以此进一步削弱数据泄露可能带来的风险[3]。

3.3 数据分区

数据分区策略是一种将数据分割为多个独立存储部分的方法，旨在隔离不同数据类型间的关联，进而提升数据的安全防护水平。借助数据分区策略，银行能够有效地将敏感数据与非敏感数据分别存储，并配置差异化的访问权限，从而规避未授权访问的风险。实施数据分区通常涉及数据分割、数据隔离以及数据加密等技术手段。

3.4 隐私计算

隐私计算技术旨在保护数据隐私的同时，促进数据的安全共享与协同计算能力。利用隐私计算技术，银行能够无需泄露原始数据，即可有效处理与分析数据，挖掘其内在价值，该技术领域主要包括多方安全计算、同态加密以及差分隐私等关键技术。具体而言，在多方安全计算的框架下，银行能够与其他机构合作处理和分析数据，无需直接共享原始数据。同态加密技术则赋予了银行在加密数据上直接进行计算的能力，输出加密结果而无需解密过程。差分隐私技术则通过向数据中引入噪声的手段，在保护数据隐私的同时，保留其统计特性。隐私计算技术在银行大数据隐私保护领域展现出广泛的应用潜力，比如在反欺诈与风险管理等场景中，银行能借助隐私计算技术与其他机构合作，共同分析挖掘数据，以提升反欺诈与风控的效能。

4 银行大数据隐私保护与信息安全治理的应对策略

4.1 构建完善的数据治理架构

在银行大数据隐私保护与信息安全治理的规划之中，构建以数据为核心的管理体系发挥着重要作用。数据治理体系的构建，不仅对于银行数据资源的有效利用至关重要，更是确保数据安全、提升业务决策精确度的关键所在。为此，银行需从组织架构、职责划分以及决策机制三个维度出发，为数据治理工作提供清晰的导向和坚实的基础。其一，银行需确立清晰的数据治理组织架构，确保各部门在数据管理领域能够各司其职、协同配合。数据管理部门应作为核心力量，承担起数据治理工作的整体规划与实施重任，同时，银行还需明确其他部门在数据管理中的角色定位与职责范围，从而汇聚数据治理的强大合力。其二，银行应制定详尽的数据管理职责分工方案，确保各部门在数据管理的各个环节中均能各尽其责、发挥所长。其三，银行应当构建涵盖数据采集、存储、加工、分析及使用等各个方面的科学决策机制，确保决策过程的公开性、透明性和高效性，还要明确决策流程、决策依据及决策结果等内容，从而实现对数据管理工作的全面把控，确保数据治理工作的稳健运行[4]。在构建完善的数据治理架构的过程中，银行还需高度重视数据质量监控机制的建立，数据质量作为数据管理的生命线，直接关乎数据治理工作的实际效果，定期对数据进行质量检查和评估，通过数据清洗、校验及修复等手段，提升数据的准确性和完整性，

是银行数据质量的持续优化与提升的重要手段。

4.2 强化信息安全防护体系

在数字化转型的背景下，信息安全防护是银行大数据隐私保护与信息安全治理的重要组成部分，银行面临着前所未有的信息安全挑战。为应对挑战，银行需采用先进的信息安全技术，构建全方位的信息安全防护体系。银行数字化转型背景下，应合理利用现代化信息技术，防护体系的强化需要借助防火墙技术、入侵检测技术、身份认证技术等。其一，银行应部署高性能的防火墙设备，对外部网络攻击进行有效防御，通过合理运用防火墙技术，可以实现对内部网络的全面保护，防止外部恶意攻击对银行数据资源的破坏和窃取。其二，银行应构建入侵检测系统，实时监控网络流量和异常行为，入侵检测技术的有效运用，可以及时发现并处置潜在的安全威胁，减少安全事件的发生和蔓延。其三，银行应采用先进的身份认证技术，如多因素认证、生物识别认证等，确保只有授权用户才能访问敏感数据和系统资源，进一步实现对用户访问权限的精准控制，防止数据泄露和非法访问的发生。除技术手段的合理有效运用外，银行还需建立完善的信息安全管理制度和操作规程，明确信息安全工作的目标和原则，规范员工的信息安全行为。同时还需定期对信息系统进行安全评估和漏洞扫描，及时发现并修复潜在的安全隐患，确保信息系统的安全性和稳定性。

4.3 实施严格的数据访问控制

数据访问控制机制是捍卫数据安全、预防泄露的核心策略，在银行大数据隐私保护及信息安全管理体系中占据着举足轻重的地位。银行需依据数据的敏感级别与重要性，划分不同的安全层级并采取相应的防护措施，以保障数据的机密性与完整性不受侵害。首要的是，银行必须严格限定对敏感数据的访问权限，通过践行最小必要权限原则，银行能确保每位用户仅能触及执行任务所必需的最低限度的数据集，显著降低数据泄露的风险，增强数据安全保障。其次，银行需综合运用身份验证、访问权限控制及审计监控等手段，以进一步强化数据访问控制的效能。借助身份验证技术，银行可以精确辨识用户身份，有效阻挡非法用户的入侵企图。同时，实施访问权限控制技术的，能够实现对用户访问权限的精细化管理，确保用户活动严格限定在授权范围内。

4.4 建立健全数据备份与恢复机制

数据备份与恢复策略是确保数据安全不可或缺的关键措施，尤其在银行大数据隐私保护及信息安全管理体系中，其构建与完善显得尤为关键。银行必须构建健全的数据备份与恢复机制，以保障在数据遭遇丢失或损毁时能够迅速且有效地恢复。在数据备份策略的制定上，银行应采纳多元化的备份手段，综合运用全量备份、增量备份及差异备份等模式能确保备份数据的全面覆盖与精确性 [5]。同时银行还需定期对备份数据进行校验与测试，以保障备份数据的可用性与完整性，从而实现对数据备份过程的全面掌控，确保备份机制的高效与可靠。另外，银行还需建立一套数据恢复响应机制，一旦发生数据丢失或损毁事件，银行能够即刻启动恢复流程，确保数据服务的迅速恢复。

4.5 加强员工培训和意识提升

员工是银行大数据隐私保护与信息安全治理的重要一环，为提升员工的信息安全意识和技能水平，银行需定期组织员工进行信息安全和数据治理方面的培训。培训内容应包括法律法规、内部规章制度以及技术防范手段等。通过法律法规的培训，员工可以了解信息安全的重要性和风险点，增强信息安全意识，而内部规章制度的培训，可以帮助员工掌握信息安全的基本要求和操作流程，规范信息安全行为。同时，银行还需建立科学合理的激励机制，鼓励员工积极参与信息安全和数据治理工作，对在信息安全和数据治理方面表现突出的员工给予表彰和奖励，激发员工的积极性和创造力。加强员工之间的沟通与协作同样具有重要意义，共同构建信息安全和数据治理的良好氛围，可以形成信息安全和数据治理的合力，共同守护银行的数据安全。

5 结语

随着大数据技术的不断进步和银行业务的快速发展，数据隐私保护和信息安全治理面临着越来越多的挑战。通过加强技术研发和创新、完善数据治理体系、加强信息安全防护、提升员工安全意识和技能以及加强合作与共享等策略，银行可以有效地应对挑战，确保大数据的安全和合规使用，为银行运营发展的稳定性保驾护航。

参考文献

[1] 刘雨佳. 大数据背景下金融隐私权保护的困境与对策[J]. 西部学刊,2023(6):116-119.

[2] 张卓. 基于联邦学习的数据隐私权保护研究——以微众银行、平安科技等为例的分析[J]. 国外社会科学前沿,2024(5):86-99.

[3] 周建平,郑培钿,王云河,等. 浅析隐私保护计算技术对数据交易流通模式的影响[J]. 信息通信技术与政策,2022(5):25-33.

[4] 杨颖. 基于审计视角的商业银行金融数据治理和个人信息保护[J]. 现代营销,2022(6):12-14.

[5] 邵文莎,于倩. 区块链在学分银行数据安全治理中的应用研究[J]. 中国教育信息化,2023,29(9):82-90.