文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

# 银行数据安全防护关键技术研究

冯庆磊
深圳前海微众银行股份有限公司
DOI:10.12238/acair.v3i1.11890

[摘　要] 随着信息技术的飞速发展,银行数据安全防护成为金融行业关注的焦点。本文针对银行数据安全防护关键技术进行综述,从数据加密技术、安全协议与技术、数据丢失防护、高级加密技术、AI在网络安全中的应用、网络安全运营与防护体系、数据安全法规与标准、大数据技术在信息安全中的应用以及数据安全管理与风险控制等方面展开论述,为我国银行数据安全防护提供理论支持和实践参考。
[关键词] 银行数据安全；加密技术；安全协议
**中图分类号**：TP309.7　**文献标识码**：A

## Research on Key Technologies for Security of Bank Data

Qinglei Feng
Shenzhen Qianhai WeBank Co., Ltd

[Abstract] With the rapid development of information technology, bank data security protection has become a focus of attention in the financial industry. This article provides an overview of key technologies for bank data security protection, including data encryption technology, security protocols and technologies, data loss prevention, advanced encryption technology, the application of AI in network security, network security operation and protection system, data security regulations and standards, the application of big data technology in information security, and data security management and risk control. It provides theoretical support and practical reference for China's bank data security protection.
[Key words] bank data security; Encryption technology; Security protocol

## 引言

在金融行业,银行数据安全至关重要。近年来我国银行业在数据安全防护方面取得了显著成果,但仍面临诸多挑战。为了更好地保障银行数据安全,本文对相关关键技术进行综述,以期为我国银行数据安全防护提供借鉴和参考。

## 1 数据加密技术

### 1.1加密算法的应用

在银行领域,加密算法的应用至关重要。对称加密算法,如AES(高级加密标准),由于其加密和解密使用相同密钥,因此在处理大量数据时效率较高。然而,对称加密的挑战在于密钥的安全分发和存储。为了解决这个问题,银行通常会采用非对称加密算法,如RSA,它使用一对密钥(公钥和私钥)进行加密和解密,公钥可以公开分发,而私钥则必须保密。非对称加密在数据传输过程中提供了更高的安全性,但处理速度相对较慢。混合加密算法结合了对称和非对称加密的优点,例如在数据传输开始时,使用非对称加密来安全地交换对称加密的密钥,然后使用对称加密来传输实际数据,这样既保证了安全性,又提高了效率。在银行系统中,这种混合加密策略被广泛应用于网上银行、移动支付等场景,确保了交易数据的安全。

### 1.2数据脱敏技术

数据脱敏技术在银行数据安全中扮演着重要角色。它通过多种方式对敏感数据进行处理,以防止未授权访问。数据掩码会在用户界面显示时隐藏部分数据,如信用卡号码的后四位;数据替换则用虚构的数据替换真实数据,用于测试和开发环境;而数据加密则是在存储或传输过程中对数据进行加密处理。银行在实施数据脱敏时,需要考虑数据的用途和上下文。例如对于需要在内部共享但又不涉及对外公开的数据,可以采用静态数据脱敏,这种脱敏是永久性的。而对于需要实时脱敏的场景,如客户服务代表访问客户信息时,动态数据脱敏技术可以在数据展示前瞬间进行脱敏处理,确保敏感信息不被泄露。

## 2 安全协议与技术

### 2.1 HTTPS和SSL/TLS的安全协议

HTTPS,即安全超文本传输协议,是一种在传统HTTP协议基础上加入了SSL/TLS加密层的网络传输协议,保障数据在客户端和服务器间的安全传输。SSL(安全套接层)及其后续的TLS(传输层安全)协议,为互联网上的加密通信提供了安全保障。通过使

用SSL/TLS协议,HTTPS实现了多重安全功能:首先它对数据进行加密,确保只有目的服务器能够解密并读取数据,有效防止了数据在传输过程中被窃听；其次利用消息摘要算法,HTTPS验证了数据的完整性,保障数据在传输过程中未被篡改;最后通过数字证书,HTTPS能够验证服务器的身份,避免用户误访问伪装的恶意网站。在银行系统中,HTTPS协议被广泛应用于网上银行、移动银行等在线服务,确保用户在交易过程中,诸如登录凭证、交易详情等敏感信息得到有效保护。面对不断升级的网络安全威胁,银行也在持续更新和升级SSL/TLS协议版本,以增强防御能力,应对中间人攻击等安全风险。

2.2磁盘加密技术

磁盘加密技术是银行保护存储数据安全的关键手段,它通过对磁盘上的数据进行加密处理,确保在磁盘丢失、被盗或不当处置的情况下,数据仍不会被未授权的第三方读取。该技术主要包括全盘加密(Full Disk Encryption,FDE),它对整个磁盘包括操作系统、应用程序及所有数据进行加密,用户在启动计算机时需输入密码或使用加密令牌来解密磁盘以访问数据；文件级加密(File-Level Encryption,FLE),这种技术只对特定文件或文件夹进行加密,虽然更灵活,但管理上也更为复杂；以及卷级加密(Volume-Level Encryption),它允许用户对磁盘上的某个卷进行加密,通常用于保护特定数据集。在实施磁盘加密时,银行通常会采用硬件加密模块(HSM)来提升加密和解密操作的性能和安全性,并制定严格的加密策略和管理流程,确保加密密钥的安全存储和合理使用。磁盘加密技术的应用不仅有助于防止数据泄露,也是银行遵守数据保护法规的重要措施。

## 3 数据丢失防护(DLP)

数据丢失防护(DLP)是银行数据安全策略中的重要组成部分,其目标是监控并防止敏感信息的未授权访问、传输、泄露或丢失。在银行业务操作中,敏感数据无处不在,包括客户个人信息、财务记录、交易数据等,因此DLP的实施显得尤为重要。

3.1 DLP技术的核心在于识别和分类敏感数据

银行需采用先进的识别技术,如关键字搜索、数据指纹识别和机器学习算法,以准确识别不同格式的敏感信息。一旦数据被识别,DLP解决方案会根据预设的策略对其进行分类和保护。这些策略可能包括对特定类型的数据实施加密、访问控制或标记,以确保只有授权用户才能访问。

3.2 DLP技术还涉及到实时监控和阻断机制

通过监控网络流量和终端设备的使用情况,DLP系统能够实时检测到敏感数据的异常流动。一旦检测到潜在的数据泄露行为,系统可以立即采取措施,如警告用户、阻断传输或自动加密数据,从而防止数据外泄。

## 4 高级加密技术

4.1区块链技术的采用

区块链技术以其去中心化和不可篡改的特性,为银行数据安全提供了新的解决方案。在银行系统中,区块链技术的应用主要体现在以下几个方面：

4.1.1数据存储的可用性得到提升。

传统的中心化数据库容易受到单点攻击,而区块链的分布式账本结构使得数据存储在多个节点上,每个节点都保存着完整的数据副本,这大大增加了数据丢失的难度,提高了数据可用性。

4.1.2数据传输的透明性和可追溯性增强

区块链上的每一笔交易都是透明的,所有参与者都可以验证交易的真实性,但不会泄露任何个人信息。这种特性有助于银行在保证数据隐私的同时,提高交易的可审计性。

4.2高级加密算法的应用

随着计算能力的提升,传统的加密算法面临着被破解的风险。银行开始探索和应用高级加密算法,以增强数据安全防护能力。量子加密是一种利用量子力学原理的加密技术,它利用量子态的不可复制性和测量的不确定性,确保密钥传输的安全性。尽管量子加密目前还处于研究阶段,但其潜力巨大,未来有望在银行数据安全领域发挥重要作用。格密码是基于数学难题的加密算法,它被认为是抵抗量子计算攻击的有力候选者。格密码的复杂性和理论上的安全性,使其成为银行保护敏感数据的新选择。银行在采用这些高级加密技术时,需要考虑算法的复杂性、计算资源的需求以及与其他系统的兼容性。通过合理部署,这些高级加密算法能够为银行提供更强的数据安全保障,有效抵御未来可能出现的各种安全威胁。

## 5 AI在网络安全中的应用

5.1 AI基础的网络安全管理

AI系统能够不间断地监控网络活动,通过机器学习算法,AI可以学习正常的网络行为模式,从而快速识别出异常行为。一旦检测到潜在的威胁,AI可以自动触发响应机制,如隔离恶意流量或通知安全人员,实现实时防护。传统的入侵检测系统往往依赖于预定义的规则,而AI增强的IDS可以通过分析大量的历史数据来识别复杂的攻击模式。这种基于行为的检测方法能够有效识别未知威胁和零日攻击。AI能够分析用户行为,识别出与用户常规行为不符的异常模式。这对于检测内部威胁和账户接管等安全事件尤为重要。AI可以处理和分析大量的安全日志,快速识别潜在的安全事件,减少人为分析的工作量,提高事件响应速度。

5.2 AI对抗人工智能的安全策略

随着攻击者越来越多地使用AI技术,银行必须采取相应的对策来对抗这些威胁。对抗样本是经过特殊设计的输入数据,旨在欺骗AI模型做出错误的判断。银行可以通过生成对抗样本来测试和强化自己的AI安全系统,提高其对抗恶意攻击的能力。通过对抗性训练,即使用对抗样本对AI模型进行再训练,可以增强模型的鲁棒性。这种方法使得模型能够在面对未知攻击时保持较高的准确率。AI系统能够根据攻击模式的变化自动调整防御策略。这种自适应机制使得银行的安全防护系统能够持续进化,以应对不断变化的威胁环境。利用AI分析大量的安全数据,银行可以更准确地识别和预测新兴威胁,从而提前采取防御措施。

## 6 网络安全运营与防护体系

6.1“一平台、四防线”纵深防护体系

“一平台、四防线”的网络安全防护体系,是一种多层次、立体化的防护策略,旨在为银行构建一个坚固的安全防护网。该体系的基础是基础设施防线,涉及服务器、存储、网络设备等硬件的安全,通过物理安全控制、硬件加密和冗余设计来确保基础设施的稳定性和安全性。接着是网络边界防线,它负责监控和控制进出银行网络的数据流,包括防火墙、入侵检测系统和入侵防御系统等,这些措施共同作用,以防止外部攻击和内部数据泄露。第三个层次是应用系统防线,它专注于银行提供的各种在线服务的安全,要求对应用程序进行定期的安全测试和代码审计,并实施严格的访问控制和身份验证机制。最终数据安全防线作为保护银行核心资产的最后一道防线,涵盖了数据加密、数据脱敏、访问控制和数据备份等策略,以保障数据的机密性、完整性和可用性。这一体系的建立,为银行提供了全方位的网络安全防护。

6.2常态化网络安全运营探索与实践

银行网络安全运营的常态化是确保信息安全的关键,它不应仅限于偶发性的应急响应,而应成为日常工作的固有部分。为此,首先需要建立和完善网络安全管理制度,确保安全策略、操作规程和应急预案得到有效执行,以此为基础,开展持续的监控和检测活动,利用安全信息和事件管理(SIEM)系统实时收集和分析网络流量数据,以便及时发现异常行为和潜在威胁。同时,定期对银行员工进行网络安全培训和意识提升,让他们了解最新的安全威胁和防护措施,从而减少人为错误导致的安全事件。此外,定期的安全评估和合规审计也是不可或缺的,它们用于验证防护体系的有效性,并根据评估结果调整和优化安全策略,以保持网络安全防护的持续性和先进性。

## 7 大数据技术在信息安全中的应用

7.1基于大数据的安全指挥中心构建

在信息安全领域,大数据技术的应用正日益成为提升银行安全防护能力的重要手段。安全指挥中心通过收集和整合银行内外部的海量数据,包括交易记录、用户行为、系统日志、网络流量等,运用数据挖掘和机器学习算法,对这些数据进行深度分析,从而揭示潜在的安全威胁和异常模式。大数据技术能够帮助安全指挥中心建立起一个全面的信息安全视图,通过实时数据流的分析,中心能够迅速识别出DDoS攻击、恶意软件传播、钓鱼网站等网络安全事件。通过对历史安全事件的深入学习,大数据分析能够预测未来可能发生的安全威胁,从而实现主动防御。此外,安全指挥中心还能够根据分析结果,自动调整安全策略,如更新防火墙规则、增强访问控制等,以应对不断变化的安全挑战。

7.2大数据时代银行信息安全保护研究

在大数据背景下,银行信息安全保护面临的数据量更大、数据类型更多样、攻击手段更复杂。因此研究工作不仅要关注如何利用大数据技术提升安全防护能力,还要考虑如何在大数据环境下确保数据隐私和合规性。这包括但不限于数据脱敏、加密存储、访问权限控制等技术的应用,以及建立一套完善的数据治理体系。

## 8 结束语

本文综合梳理了银行数据安全防护的关键技术,全面审视了我国银行业在数据安全领域的实践与挑战。随着信息技术的快速发展,银行数据安全防护将遭遇更为复杂多变的安全威胁。因此我国银行业必须坚持不懈地深化研究,不断提升数据安全防护的技术水平和管理能力,构建更加坚固的安全防线。只有这样才能确保金融业务的稳定运行,保护客户资产安全,促进金融行业的健康可持续发展。展望未来,银行数据安全防护任重而道远,需要业界同仁共同努力,不断创新前行。

## [参考文献]

[1]严文彬,肖鸣.广发银行常态化网络安全运营探索与实践[J].金融科技时代,2024(10):21-24.

[2]奚杰,王雨琪.GB/T 37931-2019在商业银行安全防控场景研发阶段的应用实践[J].信息技术与标准化,2024(z1):77-82.

[3]陈菲琪,吴昊,王巍,中小商业银行数据安全体系建设探索与实践[J].数字通信世界,2023(5):153-155.

[4]胡振鹏.商业银行金融数据安全研究和实践[J].计算机时代,2022(6):14-18.

## 作者简介：

冯庆磊(1981--),男,汉族,山东省潍坊市人,硕士研究生,研究方向：信息安全领域。