工程与管理科学
Engineering and Management Science
第 7 卷◆第 4 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

基于风险矩阵的 API 金融数据泄露风险管理系统设计与研究

章积伟
上海数禾信息科技有限公司　上海　201203

DOI：10.12238/ems.v7i4.12747

［摘　要］随着金融行业对 API 接口的广泛应用，金融数据泄露的风险日益严重。本文设计并研究了一种基于风险矩阵的 API 金融数据泄露风险管理系统。首先，通过构建风险评估模型，对 API 接口的潜在风险进行量化评估；然后，设计系统架构，提出风险控制和预警机制，确保金融数据的安全性。研究表明，基于风险矩阵的方法能有效识别并应对数据泄露风险，具有较强的实践意义和应用价值。

［关键词］API 接口；金融数据；泄露风险

引言：

随着科技进步和金融科技的发展，API 接口在金融行业中的应用逐渐普及，尤其在移动支付、在线银行、金融交易等领域，API 接口的普遍使用为提升业务效率提供了巨大支持。然而，随着 API 接口的开放，数据泄露和安全漏洞问题也日益凸显，成为金融机构面临的重要安全挑战。数据泄露不仅损害了用户的隐私，还可能导致重大经济损失。为了有效应对这一问题，风险矩阵作为一种科学的风险评估工具，在金融数据保护中展现出巨大的应用潜力。

1.金融数据泄露的严重性及对金融行业的影响

现代金融行业数据泄露问题已成为日益严重的风险问题。金融机构拥有大量个人敏感信息，账户数据，交易记录以及市场动态等重要信息，当这些信息遇到泄漏时，就会给个人客户带来损失、金融机构和整个金融体系都带来了不可估量的损失。数据泄露会直接造成客户隐私受到侵害，其身份信息也会被不法分子用于诈骗，盗刷等违法活动。金融机构声誉损害问题不容忽视，而一个严重的数据泄露事件会使顾客对金融机构丧失信任感，进而影响金融机构市场份额及品牌形象[1]。另外，金融数据泄露也会造成金融市场不稳定，特别是涉及到重大金融交易信息外泄时，会造成市场波动甚至金融危机。所以金融数据泄露风险不只是一个技术问题，而是一个关系金融行业长远发展与社会稳定的重大问题。

2.金融数据泄露风险分析

2.1 数据收集和传输环节的风险

在金融数据采集与传递过程中，最关键，也最容易被攻击。数字化时代来临，金融机构和客户及合作伙伴的交互方式有了很大改变，由传统纸质数据向电子数据过渡。这类数据一般都是在互联网或者内部网络上进行传递的，如果出现漏洞或者安全防护不到位，就很容易遇到数据窃取的情况。特别在数据收集部分，信息采集系统若加密保护不到位或者防火墙不完善，在传输数据时极易拦截。对金融机构而言，客户银行账户信息，交易密码和信用卡号这些敏感数据若未进行有效的加密，则很容易在传递时遭到黑客的盗取。另外，采用不安全 API 传输数据易造成数据泄露。比如没有加密 API 接口就会变成黑客入侵通道。

2.2 数据处理与存储环节的风险

从数据处理和存储环节来看，金融数据也存在严重泄露风险。金融机构一般都要处理和存储大量数据，其中常常含有客户身份信息，账户余额，交易历史以及其他敏感信息。数据处理与存储环节管理不到位，可能是数据泄露导火索。若数据存储系统不经过严格访问控制及加密保护，非授权人就有可能利用漏洞获取敏感数据。另外数据备份还是可能泄露的风险点。备份文件若得不到适当的管理或加密保护就有可能遭到非法访问和泄密。同时数据处理系统的不恰当设计会带来泄露风险。如数据分级保护措施不强，造成高风险数据与低风险数据储存于同一地点，加大泄露概率。

3.基于风险矩阵的API金融数据泄露风险管理系统设计的难题

3.1 如何准确识别与分类 API 数据泄露风险

API 接口是金融机构和外部系统进行互动的一种重要手段，它的安全与否直接关系着金融数据泄露的风险。如何精准识别 API 数据泄露风险已成为当前金融行业急需解决的难题。API 复杂多样，风险识别难度加大。在现代金融系统当中，API 接口量大面广，所涉及到的业务类型也非常多，覆盖支付，账户查询以及数据传输等诸多领域[2]。不同 API 接口会有不同种类的安全隐患。比如有些 API 接口会由于访问验证机制的缺失而易为恶意攻击者所使用。确定 API 数据泄露风险，还要对 API 访问权限，数据处理流程等进行精确的评估。有的 API 接口设计时没有考虑到数据加密或者权限限制等问题，造成数据传输时遇到泄露的情况。

3.2 高风险与低风险事务的区分与优先级管理

在管理金融数据泄露的风险时，区别高风险和低风险的事务，并合理分配优先级，是确保数据安全的关键策略。由于金融系统复杂多变，各类事务所涉及风险等级不一。高风险事务往往涉及大量资金转移，敏感数据处理或者重要账户运行，数据泄露后会造成严重财务损失与声誉危机。对于低风险的事务，它们通常被视为常规操作，例如查询账户、检查余额等，这些操作对数据泄露的风险相对较低。为有效地管理数据泄露的风险，金融机构有必要将事务划分为不同类别，按照它们在金融系统中的作用大小来配置资源。高风险事务需优先考虑防护措施，如通过增强 API 接口身份验证，加密技术及访问控制来保障数据安全。尽管低风险事务对安全资源要求不高，但是仍有必要进行基本安全控制来预防潜在袭击。

3.3 跨系统、跨部门协同的风险管理难度

金融机构一般都是由若干个系统、部门构成，各个部门、各个系统间数据交互非常多。如何实现跨系统，跨部门协同下 API 金融数据泄露风险有效治理已成为一大难题。不同系统间的安全标准与协议会有所不同，造成数据交换时一些安全漏洞被忽略。各个部门在数据安全认知与管理水平上存在差异，这可能会导致资源与战略不和谐，从而影响总体风险防控成效。为解决这一难题，金融机构有必要加强跨部门间的交流和合作，统一标准进行数据安全管理，以保证各系统数据交换过程中能够按照严格安全协议进行[3]。另外，还要经常性地开展跨部门安全演练活动，以增强各个部门职工风险意识及应对能力。

4.基于风险矩阵的API金融数据泄露风险管理系统设计的策略

4.1 风险点识别与评估策略

构建以风险矩阵为基础的 API 金融数据泄露风险管理系统的首要工作就是对可能存在的风险点进行精确地识别与评价。通过风险矩阵的建立，金融机构能够直观的对不同种类的风险按照发生概率及影响程度加以划分，从而对决策起到辅助作用。金融机构应彻底扫描所有 API 接口风险，确定可

能存在安全漏洞及风险点。每一个 API 使用场景都需详细地分析并对所暴露于外界的风险等级做出评估[4]。对风险较大 API 接口应重点监测并采取防护措施，以保证其实际运行安全。另外，还应依据风险矩阵评价结果对风险防控策略进行动态调整，以保证数据泄露风险始终处于可控制范围。

4.2 高风险事务的优先防护策略

在风险矩阵基础上金融机构应采用差异化防护策略优先防护高风险事务。高风险事务一般会涉及资金转移，敏感信息传递或者关键账户运行等问题，如果出现泄漏，会给金融机构安全，客户资金和信誉等方面带来严重的影响。所以金融机构应该将资源放在优先地位来加强保护这些高风险事务 API 接口。具体措施有利用多因素认证技术，加密传输协议，实时监控以及日志审计来保证高风险事务实施时受到严格监督与防护。如图 1 所示：

图 1　数据泄露防护图

4.3 跨部门协作的风险管理策略

为有效治理 API 金融数据泄露的风险，跨部门协作显得尤为重要。金融机构各部门通常在收集，处理，储存及传输数据等方面发挥着不同作用，预防数据泄露需依靠部门间紧密协作。金融机构要建立跨部门协作机制，确定部门数据安全工作责任和任务。定期举行跨部门安全审查会，探讨可能存在的风险及防护措施，保证各部门能按照各自功能做好风险防控工作。另外，通过构建统一风险管理平台来实现部门间信息共享与联动，增强了全机构应对 API 数据泄漏风险的能力。

5. 案例分析：基于风险矩阵的API金融数据泄露风险管理系统设计

5.1 管理策略的实施与效果分析

通过对一个金融机构实际案例进行研究，分析基于风险矩阵 API 的金融数据泄露风险管理系统在该系统中的实现结果。本案例通过构造风险矩阵对金融机构 API 接口风险按高度，中度和低度分级并采取相应防护措施[5]。通过对 API 进行定期安全扫描及漏洞修复等措施成功阻止了多次可能发生的数据泄露。另外，金融机构对关键 API 接口加入多因素认证以进一步提升系统安全。通过实施风险管理策略，机构显著减少 API 数据泄露次数，增强用户对自身安全可靠性的信任。

5.2 面临的挑战与解决方案

在执行基于风险矩阵的 API 金融数据泄露风险管理系统时，金融机构遭遇了众多的挑战。其中最重要的就是跨部门协作困难。由于各部门对数据安全认识上的差异造成了信息共享与合作过程的阻碍。另外，金融机构系统规模大、结构复杂、API 接口多，造成风险评估与管理工作繁重。为解决上述问题，各金融机构通过加强跨部门交流和培训、建立数据安全管理统一标准等措施，并在此基础上引进自动化工具，以提升风险识别与保护工作效率。通过上述解决措施，金融机构在执行中有效地攻克了难点，保证 API 金融数据泄露风险管理系统能够平稳地运行。

6. API金融数据泄露风险管理系统的实施过程与最佳实践

6.1 系统实施的安全措施

实现 API 金融数据泄露风险管理系统时安全措施的制定和实施非常关键。金融机构采取了多层次安全措施以保证数据安全，其中包括数据加密，防火墙设定，入侵检测系统以及多因素认证。尤其在 API 界面设计与部署阶段，对所有 API 接口均需经过严格的安全审计以保证每一个接口均满足最严格安全标准[6]。另外金融机构也强化 API 流量监控、实时发现异常行为和自动化反应机制应对。通过采取上述安全措施，金融机构可以有效防止 API 数据泄露风险。

6.2 实施中的最佳实践与经验总结

各金融机构在执行过程中总结的一些最佳做法与经验值得同行们学习。风险管理系统建设阶段金融机构要全面了解 API 接口安全要求，并对风险做出细致评估与计划。跨部门间的合作和交流是保证系统成功执行的重点。通过制定统一安全管理标准、定期开展安全培训等措施，金融机构可切实提高全员安全意识，保证系统顺利实施。另外，金融机构发现定期开展系统审计、安全演练等活动有利于提前识别可能存在的安全漏洞、及时抢修漏洞。这些最佳做法与经验对金融机构执行 API 数据泄露风险管理系统具有重要借鉴意义。

结束语：

本文基于风险矩阵方法，设计了一套 API 金融数据泄露风险管理系统，并提出了具体的风险评估、控制及预警机制。通过系统的实施，金融机构能够更高效地识别和应对潜在风险，从而减少数据泄露的可能性并保障用户隐私。然而，随着技术的发展，新型风险的出现要求我们不断完善风险管理体系。未来的研究可以进一步深化风险评估模型，提高系统的智能化与自适应能力，以应对不断变化的网络安全挑战。

[参考文献]

[1]陈秀萍，李振.防患于未然：基于风险矩阵的 API 金融数据泄露风险管理[J].金融市场研究，2024，(07)：128-138.

[2]杜纪福.供应链金融模式下中小企业信用风险评价研究——以有色金属行业为例[J].中国金属通报，2024，(08)：155-158.

[3]王健.电力行业核心企业供应链金融风险识别及评估[J].时代金融，2022，(05)：29-31.

[4]陈灿.巴基斯坦伊斯兰金融发展、风险评估及启示[J].南亚研究季刊，1-18.

[5]蔡佳蔚.建筑行业供应链金融风险评估指标体系构建研究[J].财经界，2023，(24)：24-26.

[6]周雷，邱勋，朱奕，毛晓飞.基于大数据的供应链金融信用风险评估实证研究——以整车制造行业为例[J].金融发展研究，2022，(05)：64-70.

作者简介：章积伟（1983-6），男，汉，上海市，硕士研究生，无职称，研究方向：金融软件开发。