金融科技发展背景下信息安全风险识别与防控机制研究

郭力维

中信财务有限公司，北京 100004

摘要：随着金融科技的蓬勃发展，大数据、人工智能、区块链等技术深度融入金融领域，在提升金融服务效率与创新能力的同时，也带来了前所未有的信息安全风险。本文聚焦金融科技发展背景，深入剖析信息安全风险的类型与特征，运用多种分析方法实现精准的风险识别，并构建全面系统的防控机制。研究表明，通过建立科学的风险识别体系与完善的防控机制，能够有效降低信息安全风险，保障金融科技稳健发展。

关键词：金融科技；信息安全风险；风险识别；防控机制

DOI：10.63887/jfem.2025.1.2.18

1 引言

1.1 研究背景

近年来，金融科技（FinTech）凭借大数据、云计算、人工智能、区块链等新兴技术，对传统金融模式进行了深度变革与创新。移动支付、网络借贷、智能投顾等金融科技应用不断涌现，极大地提升了金融服务的便捷性、普惠性和效率。以移动支付为例，2023 年我国移动支付交易规模已突破 500 万亿元 ，其便捷性让 “一部手机走天下” 成为现实。然而，在金融科技快速发展的背后，信息安全风险问题日益凸显。金融行业作为数据密集型行业，涉及大量客户个人信息、交易数据以及金融机构核心业务数据。一旦信息安全出现问题，不仅会损害客户利益，还可能引发系统性金融风险，危及金融稳定与安全。因此，在金融科技发展背景下，研究信息安全风险识别与防控机制具有重要的现实意义。

1.2 研究意义

理论上，本研究有助于丰富金融科技与信息安全领域的学术研究，完善信息安全风险识别与防控的相关理论体系。实践中，为金融机构提供科学的信息安全风险识别方法和有效的防控策略，帮助其降低信息安全风险，保障业务的稳定运行；为监管部门制定合理的监管政策提供参考，促进金融科技行业健康、有序发展，维护金融体系的稳定与安全。

2 金融科技发展背景下信息安全风险现状分析

2.1 金融科技的发展特点与趋势

金融科技呈现出技术融合性强、创新速度快、应用场景广泛等特点。大数据技术用于客户信用评估和风险预测，人工智能实现智能客服和自动化投资决策，区块链技术保障交易的安全与透明。未来，金融科技将朝着更加智能化、场景化、生态化的方向发展，与实体经济的融合也将更加深入。例如，在智慧金融领域，金融科技将实现对客户需求的精准把握和个性化服务，推动金融服务模式的全面升级。在智能投顾方面，通过人工智能算法分析客户的资产状况、风险偏好和市场趋势，为客户提供定制化的投资组合建议，目前国内智能投顾管理资产规模已达数千亿元，展现出巨大的发展潜力。

2.2 信息安全风险的主要表现形式

2.2.1 数据泄露风险

金融科技企业在数据收集、存储和处理过程中，由于技术漏洞、管理不善等原因，容易导致客户个人信息、交易数据等敏感信息泄露。例如，某些网络借贷平台因系统安全防护不足，遭到黑客攻击，大量用户的身份信息、银行卡信息等被窃取，给用户带来严重的经济损失和隐私泄露风险。2022 年，某知名网络借贷平台因数据库未加密且缺乏有效的访问控制，导致数百万用户的个人信息被非法获取，引发了广泛的社会关注，平台不仅面临用户的集体诉讼，还受到了监管部门的严厉处罚，声誉严重受损[1]。

2.2.2 网络攻击风险

金融科技系统面临着来自外部的多种网络攻击，如分布式拒绝服务（DDoS）攻击、恶意软件攻击、钓鱼攻击等。这些攻击可能导致系统瘫痪、数据丢失或被篡改，影响金融业务的正常开展。例如，黑客通过钓鱼邮件诱导用户点击恶意链接，获取用户的账户密码，进而盗取用户资金。2023 年，某地区多家银行遭遇 DDoS 攻击，导致网上银行和手机银行服务中断数小时，大量客户无法进行转账、查询等操作，给银行的正常运营和客户体验带来极大影响，银行不得不紧急投入大量资源进行系统修复和安全加固。

2.2.3 技术漏洞风险

新兴技术在金融领域的应用尚处于不断完善阶段，存在一定的技术漏洞。例如，区块链技术虽然具有去中心化、不可篡改等优势，但智能合约存在代码漏洞，可能被黑客利用进行非法操作；人工智能算法可能存在偏差和偏见，影响风险评估和决策的准确性。在一些区块链项目中，黑客利用智能合约中的逻辑漏洞，非法转移代币，导致投资者遭受重大损失。而人工智能在信用评估中，若训练数据存在偏差，可能会对特定群体产生不公平的评估结果，影响金融服务的公平性和可及性。

2.3 信息安全风险的影响

信息安全风险对金融科技行业产生了多方面的负面影响。从客户角度来看，信息泄露可能导致客户遭受经济损失、隐私侵犯，降低客户对金融机构的信任度；从金融机构角度来看，信息安全事件会损害机构的声誉，导致客户流失，增加运营成本，甚至面临法律诉讼和监管处罚；从整个金融体系来看，严重的信息安全风险可能引发系统性金融风险，威胁金融稳定和国家安全。例如，一次大规模的数据泄露事件可能导致客户对整个金融科技行业产生不信任，进而减少使用相关金融服务，影响行业的健康发展。而金融机构因信息安全问题导致的声誉损失，可能需要花费数年时间和大量资源才能修复。

3 金融科技信息安全风险识别方法

3.1 基于大数据分析的风险识别

利用大数据技术对金融科技系统产生的海量数据进行收集、整理和分析，通过建立风险识别模型，挖掘数据中的潜在风险特征。例如，分析客户交易数据中的异常交易模式，如频繁大额转账、非工作时间异常交易等，识别可能存在的欺诈风险；通过对系统日志数据的分析，检测网络攻击行为和系统异常操作。以某银行的大数据风险识别系统为例，该系统通过分析客户的交易时间、地点、金额、交易对象等多维度数据，建立了复杂的欺诈交易识别模型，能够实时监测交易数据，一旦发现异常交易模式，立即触发预警机制，及时阻止欺诈行为。自该系统上线以来，成功拦截了数千起潜在的欺诈交易，为银行和客户避免了大量经济损失[2]。

3.2 基于人工智能的风险识别

人工智能技术在信息安全风险识别中具有独特优势。机器学习算法可以通过对大量历

史数据的学习，自动识别风险模式和趋势。例如，利用深度学习算法对网络流量数据进行分析，识别恶意网络流量；自然语言处理技术可用于分析客户投诉、社交媒体数据等文本信息，发现潜在的安全风险和客户不满情绪。此外，人工智能还可以实现风险的实时监测和预警，提高风险识别的效率和准确性。某金融科技公司运用深度学习算法对网络流量进行实时分析，能够精准识别出各种新型网络攻击行为，包括零日漏洞攻击。同时，通过自然语言处理技术分析客户在社交媒体上的反馈，及时发现产品存在的安全隐患和用户的不满情绪，为公司改进产品和服务提供了重要依据[3]。

3.3 基于区块链的风险识别

区块链技术的分布式账本和加密特性，有助于实现信息安全风险的识别和追溯。在金融交易中，区块链可以记录每一笔交易的详细信息，包括交易时间、交易双方、交易金额等，通过对这些交易记录的分析和比对，能够及时发现异常交易行为。同时，区块链的不可篡改特性保证了数据的真实性和完整性，为风险识别提供可靠的数据基础。例如，在供应链金融中，利用区块链技术可以追踪资金流向和货物流转情况，识别潜在的欺诈风险。某供应链金融平台基于区块链技术构建了交易信息记录系统，每一笔融资交易的相关信息，如订单、发票、物流信息等都被记录在区块链上，一旦出现异常交易，如虚假订单融资，系统可以快速追溯交易源头，及时发现欺诈行为，保障了参与各方的资金安全[4]。

4 金融科技信息安全防控机制构建

4.1 技术防控机制

4.1.1 加强数据安全保护

采用先进的数据加密技术，对客户数据进行加密存储和传输，防止数据在存储和传输过程中被窃取或篡改。例如，使用对称加密算法和非对称加密算法相结合的方式，确保数据的安全性；建立数据访问控制机制，严格限制用户对数据的访问权限，根据用户的角色和职责分配不同的访问级别。某大型金融机构在数据存储方面，采用了 AES（高级加密标准）对称加密算法对客户敏感数据进行加密，并使用 RSA 非对称加密算法保护加密密钥。同时，通过基于角色的访问控制（RBAC）模型，对员工和合作伙伴的访问权限进行精细管理，只有经过授权的人员才能访问相应的数据，有效保障了数据的安全性。

4.1.2 提升网络安全防护能力

部署防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等网络安全设备，实时监测和防范网络攻击。定期对网络安全设备进行升级和维护，确保其性能和防护效果。同时，加强网络安全漏洞扫描和修复工作，及时发现和修补系统中的安全漏洞。某金融科技公司构建了多层次的网络安全防护体系，在网络边界部署了高性能防火墙，对进出网络的流量进行严格过滤；内部网络中部署了 IDS 和 IPS 系统，实时监测网络攻击行为，并自动进行阻断。此外，公司还建立了漏洞扫描和修复机制，每周对系统进行一次全面的漏洞扫描，发现漏洞后及时安排技术人员进行修复，有效提升了网络安全防护能力。

4.1.3 完善技术架构安全

在金融科技系统的设计和开发过程中，遵循安全设计原则，采用安全可靠的技术架构。例如，采用微服务架构，将系统功能进行模块化拆分，降低系统的耦合度，提高系统的安全性和可维护性；引入容器技术，实现应用的隔离和快速部署，增强系统的安全性和灵活性。某银行在开发新一代核心业务系统时，采用了微服务架构，将业务功能拆分为多个独立的微服务，每个微服务都有独立的运行环境和安全防护措施。同时，利用容器技术对微服务进行封装和部署，实现了快速迭代和弹性扩展。这

种技术架构不仅提高了系统的安全性，还提升了系统的开发和运维效率[5]。

4.2 管理防控机制

4.2.1 建立健全信息安全管理制度

金融机构应制定完善的信息安全管理制度，包括数据管理制度、网络安全管理制度、人员安全管理制度等。明确各部门和岗位在信息安全管理中的职责和权限，规范信息安全管理流程，确保信息安全管理工作有章可循。例如，建立数据备份与恢复制度，定期对重要数据进行备份，确保在数据丢失或损坏时能够及时恢复。某证券公司制定了详细的信息安全管理制度，涵盖了数据管理、网络安全、人员培训等多个方面，确保数据的安全性和可用性。

4.2.2 加强人员信息安全培训

提高员工的信息安全意识和技能是防控信息安全风险的重要环节。金融机构应定期组织员工进行信息安全培训，培训内容包括信息安全法律法规、安全操作规范、风险防范知识等。通过培训，使员工了解信息安全的重要性，掌握信息安全防护技能，避免因人为因素导致信息安全事故的发生。某保险公司每年都会组织多次信息安全培训活动，邀请行业专家和内部技术人员为员工授课，培训内容涵盖了信息安全法规、网络安全知识、数据保护措施等方面。同时，公司还开展了信息安全意识竞赛、模拟钓鱼攻击演练等活动，通过实际操作和案例分析，提高员工的信息安全意识和应对风险的能力。

4.2.3 强化第三方合作管理

在与第三方机构合作前，对其信息安全管理能力进行全面评估，选择具有良好信誉和较高信息安全管理水平的合作伙伴。在合作过程中，签订详细的信息安全协议，明确双方在信息安全方面的权利和义务，加强对第三方机构的监督和管理，定期对其信息安全管理情况进行检查和评估，确保第三方机构的信息安全管理符合要求。某支付机构在选择第三方云计算服务提供商时，对其进行了严格的信息安全评估，包括数据中心的物理安全、网络安全防护能力、数据备份与恢复机制等方面。在合作过程中，双方签订了详细的信息安全协议，明确了数据保护责任和违约赔偿条款。支付机构还定期对云计算服务提供商进行信息安全审计，确保其服务符合安全要求，保障了客户数据的安全。

结论

在金融科技快速发展的背景下，信息安全风险已成为制约金融科技行业健康发展的重要因素。通过对金融科技信息安全风险的现状分析，采用大数据分析、人工智能、区块链等先进技术实现精准的风险识别，并从技术、管理和监管等多个层面构建全面系统的防控机制，能够有效降低信息安全风险，保障金融科技的稳健发展。

参考文献

[1]邓湘勤.信息安全风险评估与防范策略研究[J].数字通信世界,2024(2):29-31

[2]王盈丰,王燕嘉.人工智能在金融风险预警模型中的应用与优化策略[J].现代营销(下),2025(4):25-27

[3]黄福伟.区块链技术在网络安全中的作用分析——评《区块链安全技术指南》[J].中国安全科学学报,2020,30(11):192-192

[4]孟添,陆岷峰.科技金融生态体系建设的政策支持研究[J].信阳师范大学学报(哲学社会科学版),2025,45(2):30-38

[5]刘木旋.数字经济背景下科技金融对经济高质量发展的提升效应研究[J].营销界,2024,(24):74-76.