Finance 金融, 2024, 14(4), 1518-1523
Published Online July 2024 in Hans. https://www.hanspub.org/journal/fin
https://doi.org/10.12677/fin.2024.144156

Hans汉斯

网络金融环境下电子支付的安全性分析与优化

余欣芮[1*]，陈梦琳[2]

[1]东北大学秦皇岛分校经济学院，河北 秦皇岛
[2]四川轻化工大学经济学院，四川 宜宾

收稿日期：2024年5月31日；录用日期：2024年6月19日；发布日期：2024年7月25日

摘 要

网络金融的兴起为电子支付带来了广阔的发展空间，但安全问题日益凸显。本文聚焦于电子支付的安全性，分析了其面临的主要挑战。通过案例剖析，揭示了安全问题的根源。同时，本文探讨了电子支付安全性的关键技术，并回顾了相关法规。最后，提出了针对性的优化策略，旨在平衡用户体验与安全性，为电子支付行业的健康发展提供参考。

关键词

网络金融，电子支付，安全性，技术，标准与法规，优化策略

Security Analysis and Optimization of Electronic Payment in the Network Finance Environment

Xinrui Yu[1*], Menglin Chen[2]

[1]School of Economics, Northeastern University at Qinhuangdao, Qinhuangdao Hebei
[2]School of Economics, Sichuan University of Science & Engineering, Yibin Sichuan

Received: May 31st, 2024; accepted: Jun. 19th, 2024; published: Jul. 25th, 2024

Abstract

The rise of online finance has brought vast development space for electronic payments, but security issues are increasingly prominent. This article focuses on the security of electronic payments and analyzes the main challenges they face. Through case analysis, the root cause of security is-

*通讯作者。

文章引用: 余欣芮, 陈梦琳. 网络金融环境下电子支付的安全性分析与优化[J]. 金融, 2024, 14(4): 1518-1523.
DOI: 10.12677/fin.2024.144156

sues was revealed. Meanwhile, this article explores the key technologies for electronic payment security and reviews relevant regulations. Finally, targeted optimization strategies were proposed to balance user experience and security, providing reference for the healthy development of the electronic payment industry.

Keywords

Network Finance, Electronic Payments, Security, Technology, Standards and Regulations, Optimization Strategies

1. 引言

随着网络信息技术的迅猛发展，电子支付已成为我们日常生活中不可或缺的一部分。然而，网络金融环境下电子支付的安全性问题也日益凸显，给消费者和企业带来了严重的风险。因此，本文旨在全面分析电子支付在网络金融环境中的安全性问题，并提出相应的优化策略，以期为保障电子支付的健康发展提供参考。

2. 基本概念

2.1. 网络金融

网络金融是一种随着互联网发展逐渐产生的新型金融服务方式，即可以通过网络随时随地进行各种金融操作。它以金融服务提供者的主机为核心，依托互联网作为传输媒介。通过软件平台，以用户终端作为操作界面，实现了金融服务的便捷与高效。比如，不用去线下金融机构就能直接实现在互联网上进行转账汇款，购买股票和基金等。

2.2. 电子支付

电子支付就是通过网络或其他电子方式来完成支付的行为。它涉及买家、卖家以及金融机构之间的信息传输[1]。通过信息网络，这些支付信息能够安全地传递到相应的处理机构，从而实现货币支付。电子支付的业务类型按电子支付指令发起方式分为销售点终端交易、电话支付、移动支付、网上支付和其他电子支付。

3. 电子支付安全性的风险分析

3.1. 电子支付的主要安全风险

3.1.1. 信息泄露风险

在电子支付过程中，常常需要用户提供姓名、银行卡号、身份证号等隐私信息。这些信息如果在传输和储存过程中未得到妥善保管，极易被黑客或不法分子窃取并进行倒卖去做非法的事情，极大影响用户的信用额度和正常生活。

3.1.2. 交易欺诈风险

交易欺诈风险的主要来源之一是虚假交易。诈骗分子可能在网上散布虚假的销售信息，来诱导用户

进行交易。这些交易往往是虚假的，没有实际的商品存在或是商品的质量远远低于描述的情况。用户一旦支付，就可能会面临资金损失收不回来的风险。其次，不法分子还会利用各种技术手段创建与真实网站没有差别的虚假网站来诱骗用户输入个人隐私信息，直接窃取资金。

3.1.3. 税收洗钱风险

电子支付的匿名性和便捷性为洗钱者提供了隐蔽的资金转移渠道。通过伪造交易等方式，利用电子支付平台的跨境支付功能，犯罪人员可以轻易地将钱送到世界上的任何地方且不留下任何记录。相关税务部门如想进行监管和追查，程序十分繁琐复杂，需要检查网上所有的数据并破译密码，这几乎是不可能的。

3.2. 电子支付安全风险产生原因

3.2.1. 软件系统存在漏洞

电子支付的实现在很大程度上要依赖于先进的网络技术和信息系统[2]。然而，目前我国网络环境复杂多变，软件系统中或多或少存在着一些安全隐患和漏洞。这会为黑客和恶意攻击者提供可乘之机，导致用户的隐私信息被盗取。软件系统的漏洞还可能导致支付流程的中断或异常，引发交易失败、支付延迟或资金划分错误等问题。

3.2.2. 市场监管不够完善

当前，法律法规在电子支付领域的规范与监管不够完善，这会使得消费的权益无法得到足够的保障，消费者的投诉和维权将会面临挑战，如维权成本高等，消费者因为虚假信息而损失的资金费用便也无法追回[3]。

3.2.3. 用户安全意识不高

当用户安全意识欠缺时，他们更容易受到网络诈骗的侵害。比如，在设置密码时，可能不够谨慎将密码设置的过于简单，这便降低了密码的安全性，大大增加了账号被盗用的风险；在电子支付过程出现异常或风险提示时，他们也可能不重视警告，从而陷入诈骗人员的陷阱[4]。

3.3. 电子支付安全性问题的案例和启示

3.3.1. 2018 年印度支付应用漏洞

2018 年，印度一款流行的移动支付应用 Juspay 由于代码中的一个漏洞，导致黑客能够绕过支付验证，直接从用户账户中盗取资金。这一事件导致数百万用户的财产安全受到威胁，且对该支付平台的信任度造成了长期的负面影响。

3.3.2. 2020 年美国美国薪资协会遭遇数据泄露

2020 年，黑客利用 APA 组织内容管理系统中的一个安全漏洞，成功地攻破了 APA 的网站和在线商店并部分部署了数据窃取器，通过窃取器，他们收集并窃取用户的敏感信息，包括登录信息以及个人支付卡信息。超过 1000 万用户的个人信息和信用卡详情被非法访问。这一事件导致大量的经济损失，并且引发了对支付系统安全性的广泛关注。

3.3.3. 启示与对策

① 加强代码安全和审计

软件和应用的安全漏洞往往是黑客攻击的主要入口。企业需要定期进行代码审计和安全测试，确保没有安全漏洞被遗漏。此外，开发过程中引入安全开发生命周期管理(SDLC)可以从根本上减少安全风险。

② 数据加密和安全存储

对于存储和传输的数据，必须使用强加密标准来保护用户的敏感信息。此外，应限制对敏感数据的访问，确保只有授权人员才能访问重要数据。

③ 用户身份验证和多因素认证

增强用户身份验证机制，如引入多因素认证(MFA)，可以大幅提高账户安全性。即使攻击者获得了用户的密码，也因为缺乏其他认证因素而难以实际访问账户。

④ 及时更新和修补

软件和系统的漏洞往往是不可避免的，但及时的更新和修补可以最大限度地减少这些漏洞被利用的机会。企业应确保所有系统和应用都运行最新版本的软件，并且安装了所有安全补丁。

⑤ 教育和培训

用户的安全意识同样重要。通过定期的安全培训和教育，可以使用户意识到潜在的风险，并教会他们如何保护自己的账户不受攻击。

4. 电子支付安全性的技术分析

4.1. 关键技术分析

4.1.1. 私有密钥加密技术

其原理是信息发送方会运用特定的密钥对数据进行加密处理。只有掌握这一相同密钥的信息接收方，才能够对该加密数据进行解密。这种方法在专用网络中的使用效果好，且速度快、投入成本低。银行内部专用网络和军事指挥网络一般都采用这种加密方法。其缺点是在与多人通信时，需要使用很多密钥，给每人都配置一把密钥十分繁琐。

4.1.2. 公开密钥加密技术

其原理是共用两个在数学上相关的密钥，信息接收方将其中一个作为私人密钥加密并保存好，信息发送方用另一个公开密钥将信息加密，这些信息便只能被接收方收到。用户只需要保护好私人密钥，就不用担心泄露。该方法可以在网络支付结算中起到“认证支付行为”和“防抵赖”的作用。这种方法相对私有加密技术速度就慢得多。

4.1.3. 数字信封技术

该方法是以上两种技术的结合。通过公开密钥加密含有私有密钥的数字信封，并使用私有密钥加密原本的密文[5]。在该方法中，私有密钥是由发送方每次随机生成的，并且会通过公开密钥进行加密，从而显著提升了信息的安全性。对于像银行卡号、支付密码这类重要且简短的信息，利用数字信封技术来进行传送可以确保这些信息在传输过程中不会被泄露或篡改。

4.1.4. 数字摘要技术

其原理类似于给信息加上“数字指纹，即通过使用一定算法对传送的数据生成一个特定值，并将此值一起传送给接收者，接收者在收到后可以通过新值与特定值的对比来检验数据在传送过程中是否被改动[5]。其特点是能处理任意信息，并对其生成特定对应的数据摘要，如果信息被修改，前后生成的特定摘要必定不同，因此可以确定数据有无修改或变化。

4.1.5. 数字签名技术

数字签名就是指在发送者在发送消息时附上自己才能产生而别人无法伪造的签名或印章以表示消息是真实出自发送者[5]。使用该方法可以解决网络支付中“发送者或接收者否认”、“第三方冒充”、“接

收方伪造”等问题，保证了信息传输过程中的完整性和消息发送者身份的不可抵赖性。

4.1.6. 双重签名技术

该技术巧妙地在客户、商户和银行之间搭建起一个安全的桥梁。通过将发送给不同接收者的两条消息进行串联，它不仅实现了信息的有效传递，还很好地保护了消费者的隐私。

4.1.7. SSL 安全协议

SSL 是一种协议，它负责对计算机之间的整个通信会话进行加密处理。它主要提供以下三方面的服务：首先，SSL 认证用户和服务器的身份，确保双方能够确认数据将准确无误地发送到目标客户机和服务器上；其次，SSL 对数据进行加密，以保护在传输过程中被传送的敏感信息，防止其被未经授权的第三方窃取或窥视；最后，SSL 还维护数据完整，通过一系列机制确保数据在传送过程中不被改变。

4.2. 电子支付的新兴技术展望

4.2.1. 区块链技术

区块链提供了一种去中心化的支付方式，可以增加交易的透明度和不可篡改性[6]。例如，比特币等加密货币就是基于区块链技术，它们通过公开的账本记录所有交易，增强了交易的安全性。

4.2.2. 人工智能与机器学习

AI 和机器学习被用于监测和分析交易模式，以识别和防止欺诈行为。通过实时分析大量的交易数据，这些技术可以快速识别出异常行为，从而阻止潜在的欺诈交易。

4.2.3. 生物识别技术

指纹识别、面部识别和虹膜识别等生物识别技术被越来越多地用于电子支付，以增强用户身份验证的安全性。这些技术能够确保支付行为由真实的用户本人执行，大大降低了身份盗用的风险。

5. 电子支付安全性的优化策略

5.1. 软件技术层面的优化

当前，电子支付主要依赖于数字证书与加密技术来保障安全。专业人员应当不断发掘更高效、更安全的加密方法，增加支付过程中的身份验证环节，有效防止账号信息被盗取。同时，国家应加大对网络技术的资金投入，不断引进先进的设备与技术，加强人才培养，为电子支付安全提供坚实的技术支撑[7]。

5.2. 法律监管层面的优化

在 PCI DSS 国际标准保障下，电子支付环境得到防护，此标准要求所有处理、存储或传输信用卡信息的实体都必须遵守一系列严格的安全措施，以此帮助组织保护支付卡数据的安全。此外，为切实提高电子支付的安全性，各国还针对电子支付颁布了相关法规，例如中国的《网络安全法》《电子支付法》和美国的《加州消费者隐私法案(CCPA)》等[8]，这些法规通常要求企业在处理支付和个人数据时，必须采取合理的安全措施，以防数据泄露和其他安全威胁。但是，目前电子支付市场的监管仍不完善，还存在许多不规范的行为[9]，国家应制定并执行相关法律法规，明确电子支付各方的责任与义务，同时建立快速响应的投诉和纠纷解决机制，为消费者提供便捷的维权渠道，及时解决电子支付过程中出现的问题。其次，金融监督部门要加强对电子支付平台的监督和检查力度，并定期进行检查，确定一切合法合规，从而保障用户资金安全。

5.3. 用户教育层面的优化

首先，相关部门需通过媒体、社交平台等多个渠道传播广泛普及电子支付相关安全知识，提升用户的安全意识[10]。其次，制作针对不同用户群体的安全教育材料，通过直观生动的方式向他们展示电子支付安全的防范措施。同时，在各种支付平台加强用户风险的提示，帮助用户及时识别潜在风险并及时止损。

5.4. 国际合作层面的优化

随着跨境电子支付交易的日益增多，跨境电子支付犯罪也呈上升趋势，加强国际合作对于维护国际电子支付市场的安全和稳定具有重要意义。各国可以通过建立更加紧密的沟通机制，实现信息共享和情报交流，从而共同分析犯罪趋势，制定更为有效的防范措施，共同应对跨境电子支付领域面临的挑战，推动全球电子支付市场的健康、稳定发展。

5.5. 用户体验与安全性平衡

5.5.1. 简化的用户验证流程

虽然多因素认证提高了安全性，但也可能使支付过程变得繁琐。因此，设计者需要探索如何简化认证流程而不牺牲安全性，例如，通过使用生物识别技术代替传统的密码系统。

5.5.2. 透明的用户界面设计

确保用户能够容易理解和操作支付界面，包括清晰显示的支付信息、费用和安全提示。这不仅可以提升用户体验，还可以帮助用户做出更安全的支付决策。

5.5.3. 个性化的安全设置

允许用户根据自己的需求调整安全设置，例如设置交易限额或选择更严格的登录验证方法[11]。这种个性化可以让用户在享受便捷的同时，也能根据自己的安全需求进行调整。

6. 结论与展望

本文深入研究了电子支付的风险和产生原因，结合现有技术，从“软件技术”、“法律监督”、“用户教育”、“国际合作”等四个层面提出技术与管理并重的优化策略，同时深入考虑用户体验感的提升与使用安全性提升的平衡问题。电子支付安全性优化对于保障用户权益、促进金融行业健康发展具有重要意义，相关人员和部门都应该重视并共同合力推动优化。

参考文献

[1] 王国存. 电子支付主体刍议[J]. 电脑知识与技术, 2010, 6(33): 9436.
[2] 王琳. 电子支付存在的安全问题及解决对策[J]. 中小企业管理与科技(下旬刊), 2018(9): 176-177.
[3] 陈吟. 电子支付安全问题及其解决策略[J]. 现代经济信息, 2018(30): 298.
[4] 谢宏武, 许一凡. 浅析在电子商务环境下用户体验对商品销售的影响及对策[J]. 商场现代化, 2017(18): 19-20.
[5] 曹世源. 电子支付安全技术及其应用的研究[J]. 数字技术与应用, 2019, 37(1): 215-216.
[6] 董学倩, 董西梅. 区块链技术与我国电子支付体系的研究[J]. 商讯, 2020(12): 150, 152.
[7] 张红艳. 电子支付的安全及发展研究[J]. 现代营销(信息版), 2020(1): 223.
[8] 于昕彤. 《电子商务法》视域下的电子支付安全问题研究[D]: [硕士学位论文]. 锦州: 渤海大学, 2022.
[9] 张敏, 闫育芸, 姚雨秋. 浅析电子支付的安全问题及防护措施[J]. 网络安全技术与应用, 2022(12): 123-124.
[10] 肖丁铭, 魏周思宇. 电子商务网络安全支付问题解析[J]. 智库时代, 2020(7): 39-40.
[11] 章诗琦. 电子支付网站用户帮助平台的用户体验研究与设计[D]: [硕士学位论文]. 上海: 上海交通大学, 2013.