 DOI: https://doi.org/10.12349/iser.v6i1.4493

Research on data security protection technology based on strong isolation access control

Jinhu Huang

Fujian CITIC Network Security Information Technology Co., Ltd., Fuzhou, Fujian, 350000, China

Abstract

In order to deeply explore the data security protection technology based on strong isolation access control, effectively prevent unauthorized access and data leakage. This paper analyzes the concept and principle of strong isolation access control, summarizes the data security protection technology based on strong isolation access control, for the current data security protection technology challenges, puts forward a set of targeted solutions to deal with the challenges in the current data security protection. The results show that the proposed scheme has a significant effect in improving the data security protection capability. In the future, we should continue to pay attention to the development of this field, and constantly optimize the technology to provide more powerful technical support for data security protection.

Keywords

strong isolation access control; data security protection; application strategy

基于强隔离访问控制的数据安全保护技术研究

黄金虎

福建中信网安信息科技有限公司，中国 · 福建 福州 350000

摘　要

为深入探讨基于强隔离访问控制的数据安全保护技术，有效防止未经授权的访问和数据泄露。本文分析了强隔离访问控制的概念和原理，总结了基于强隔离访问控制的数据安全保护技术要点，针对当前基于强隔离访问控制的数据安全保护技术面临的挑战，提出了一套针对性的解决方案，以应对当前数据安全保护中面临的挑战。研究结果表明，所提出的方案在提高数据安全防护能力方面具有显著效果。未来，应继续关注该领域的发展，不断优化技术，为数据安全保护提供更强大的技术支持。

关键词

强隔离访问控制；数据安全保护；应用策略

1 引言

随着信息技术的飞速发展，数据已经成为企业、组织和个人重要的资产。然而，数据泄露、非法访问等安全问题也日益突出，给数据安全带来了巨大的挑战。特别是在云计算、物联网等新兴技术的推动下，数据存储和传输的复杂性不断增加，传统的访问控制方法已无法满足日益严格的数据安全需求。因此，研究基于强隔离访问控制的数据安全保护技术显得尤为重要。本文旨在探讨基于强隔离访问控制的数据安全保护技术，分析其重要性、现有研究现状以及面临的挑战，并提出相应的解决方案和未来发展方向。

【作者简介】黄金虎（1977–），男，中国福建南安人，硕士，工程师，从事数据安全，网络安全研究。

2 强隔离访问控制技术概述

2.1 强隔离访问控制的概念和原理

强隔离访问控制是一种严格的网络安全技术，旨在通过物理或逻辑手段，将网络中的不同安全域相互隔离，以防止恶意代码、攻击和未授权访问从一个域传播到另一个域[1]。其核心内涵在于实现不同安全域之间的信息流动最小化，确保系统的安全性和稳定性。强隔离访问控制根据系统的安全需求，将网络划分为不同的安全域，如内网、外网、DMZ区等。通过物理隔离（如防火墙、物理隔离卡等）或逻辑隔离（如访问控制列表、安全策略等）手段，实现不同安全域之间的隔离。为每个用户和应用程序分配最小权限，以减少潜在的攻击面。对安全域之间的访问进行实时监控和审计，及时发现并处理异常情况。

2.2 强隔离访问控制技术的分类

2.2.1 物理隔离

物理隔离是指通过物理手段实现不同安全域之间的隔

离，如防火墙、安全隔离网闸、物理隔离卡等。物理隔离可以有效地防止恶意代码、攻击和未授权访问从一个域传播到另一个域。物理隔离设备通常具有较高的可靠性和稳定性。物理隔离设备需要投入较大的资金和人力资源。

2.2.2 逻辑隔离

逻辑隔离是指通过软件手段实现不同安全域之间的隔离，如访问控制列表、安全策略、安全区域等。逻辑隔离可以根据实际需求进行灵活配置。逻辑隔离通常只需要投入较少的资金和人力资源。逻辑隔离容易受到恶意代码、攻击和未授权访问的影响。

2.2.3 混合隔离

混合隔离是指将物理隔离和逻辑隔离相结合，以实现更全面、更安全的安全域隔离。混合隔离结合了物理隔离和逻辑隔离的优点，提高了系统的安全性。混合隔离可以根据实际需求进行灵活配置。混合隔离需要同时投入物理隔离和逻辑隔离的资金和人力资源。

3 基于强隔离访问控制的数据安全保护技术

3.1 数据加密技术在强隔离访问控制中的应用

3.1.1 加密算法的选择与应用

在强隔离访问控制中，数据加密技术是实现数据安全保护的关键手段之一。加密算法的选择与应用主要包括以下几个方面：（1）对称加密算法：对称加密算法具有加解密速度快、密钥管理简单等特点，适用于数据传输和存储过程中的加密。常用的对称加密算法有 DES、AES、3DES 等。（2）非对称加密算法：非对称加密算法具有加解密速度慢、密钥管理复杂等特点，适用于密钥交换和数字签名等场景。常用的非对称加密算法有 RSA、ECC 等。（3）哈希算法：哈希算法在数据加密中主要用于生成数据摘要，确保数据完整性。常用的哈希算法有 MD5、SHA-1、SHA-256 等。在实际应用中，根据数据安全需求选择合适的加密算法，并结合多种加密技术，提高数据安全性。

3.1.2 密钥管理与分发

密钥管理是数据加密技术中的核心环节，直接关系到数据安全。采用安全的随机数生成器生成密钥，确保密钥的唯一性和随机性。将密钥存储在安全的环境中，如硬件安全模块（HSM）或密钥管理系统，防止密钥泄露。采用安全的方式进行密钥分发，如使用公钥基础设施（PKI）或数字证书等。定期更换密钥，降低密钥泄露风险。当密钥被泄露或过期时，及时撤销密钥，确保数据安全。

3.2 身份认证与授权技术在强隔离环境中的实现

3.2.1 多种身份认证方式的结合

在强隔离环境中，为了提高安全性，通常会采用多种身份认证方式相结合的策略。双因素认证（2FA）通过结合两种或两种以上不同类型的认证方式，如密码和动态令牌、密码和生物识别信息等，以增强认证的安全性。多因素认证（MFA）与双因素认证类似，但可以包含更多种类的认证方式，如密码、短信验证码、电子邮件验证码、智能卡、指纹识别等 [2]。在强隔离环境中，使用身份认证代理可以降低认证过程中的风险。身份认证代理负责处理认证请求，并将认证结果传递给用户。集成认证将强隔离环境中的认证系统与其他系统（如企业内部系统、云服务等）进行集成，实现单点登录（SSO）。

3.2.2 基于角色的访问控制（RBAC）与强隔离的融合

基于角色的访问控制（RBAC）是一种常用的访问控制方法，通过将用户分为不同的角色，并针对每个角色设置相应的权限，从而实现对用户访问资源的控制。在强隔离环境中，访问控制列表（ACL）用于定义哪些用户或角色可以访问哪些资源。在强隔离环境中，可以将 ACL 与 RBAC 结合，实现细粒度的访问控制。安全域是一种将资源划分为不同安全级别的机制。在强隔离环境中，可以结合安全域和 RBAC，实现跨域访问控制。通过定义访问控制策略，可以进一步细化 RBAC 的权限控制。在强隔离环境中，结合访问控制策略可以实现对不同角色在特定场景下的访问限制。访问控制引擎负责根据 RBAC 和访问控制策略，对用户访问请求进行实时判断和处理。在强隔离环境中，访问控制引擎可以与其他安全组件（如防火墙、入侵检测系统等）协同工作，提高整体安全性。

3.3 安全审计与监控技术在强隔离系统中的部署

3.3.1 审计日志的记录与分析

在强隔离系统中，审计日志的记录应包括以下内容：1）用户操作记录：记录用户登录、访问、修改、删除等操作的时间、操作对象、操作结果等；2）系统事件记录：记录系统启动、停止、异常等事件的时间、原因、影响等；3）安全事件记录：记录入侵检测、恶意代码检测、异常访问等安全事件的时间、类型、影响等。通过对审计日志的实时分析，发现并识别异常行为，如频繁登录失败、异常访问等，以便及时采取措施；分析安全事件的发生原因、影响范围、处理过程等，为安全事件的预防、应急响应提供依据；根据相关法律法规和标准，对审计日志进行合规性检查，确保系统安全合规运行。

3.3.2 实时监控与预警机制

实时监控系统资源使用情况，如 CPU、内存、磁盘空间等，确保系统资源合理分配，避免资源耗尽；实时监控网络流量，发现异常流量，防止网络攻击；实时监控用户行为，发现异常操作，如频繁登录失败、非法访问等 [3]。根据系统实际情况，设置各类监控指标的阈值，当监控指标超过阈值时，触发预警；当系统发生异常或安全事件时，及时向相关人员发送预警通知，以便迅速采取应对措施；根据预警信息，启动应急预案，进行应急响应，确保系统安全稳定运行。

4 基于强隔离访问控制的数据安全保护技术面临的挑战

4.1 技术层面的挑战

4.1.1 性能瓶颈

强隔离访问控制通常需要加密敏感数据，这会导致额外的计算开销，从而降低系统处理速度。在强隔离环境下，访问控制策略需要根据用户权限和资源访问需求动态调整，这可能会引入延迟，影响用户体验。当系统需要与其他系统或设备进行数据交互时，强隔离访问控制技术可能成为性能瓶颈，导致数据传输速度下降。

4.1.2 兼容性问题

强隔离访问控制技术可能无法与现有系统无缝集成，导致兼容性问题，影响整体数据安全。强隔离访问控制技术可能对硬件设备或软件平台有特定要求，若现有设备或平台无法满足这些要求，将导致兼容性问题。强隔离访问控制技术可能对数据格式有特定要求，若现有数据格式与这些要求不符，将导致数据格式兼容性问题。

4.1.3 新技术冲击

随着信息技术的不断发展，云计算和大数据技术的广泛应用，使得数据存储和计算变得更加分散，给强隔离访问控制技术的实施带来挑战。人工智能和物联网技术的快速发展，使得数据安全面临更多潜在威胁，对强隔离访问控制技术提出了更高的要求。加密技术的不断更新换代，要求强隔离访问控制技术及时跟进，以适应新的安全需求。

4.2 应对挑战的策略

4.2.1 优化性能

在确保数据安全的前提下，通过优化数据传输协议、压缩技术等手段，降低数据传输过程中的延迟和带宽消耗。选择适合的加密算法，在保证数据安全的同时，降低加密和解密所需的计算资源 [4]。在数据处理过程中，利用并行计算技术提高处理速度，降低延迟。合理设计存储结构，提高数据访问速度，降低存储成本。

4.2.2 提升兼容性

开发基于强隔离访问控制的数据安全保护技术时，确保其能够在多种操作系统和硬件平台上正常运行。遵循国际数据安全标准，如 ISO/IEC 27001、ISO/IEC 27002 等，提高技术的通用性和兼容性。设计灵活的接口，方便与其他安全产品和系统进行集成。采用跨平台开发技术，如 Java、C++ 等，提高技术的兼容性。为用户提供全面的技术培训和支持，帮助用户更好地理解和使用基于强隔离访问控制的数据安全保护技术。

4.2.3 积极应对新技术

随着物联网设备的普及，加强设备身份认证和访问控制，确保数据安全。采用区块链技术，实现设备间安全通信。利用云计算平台，实现资源弹性伸缩，提高数据处理能力。采用容器化技术，实现应用快速部署和扩展。结合 AI 技术，实现智能访问控制，提高访问控制效果 [5]。例如，通过机器学习算法，对用户行为进行分析，识别异常行为，提前预警。利用区块链技术，实现数据安全存储和访问控制。通过分布式账本，保证数据不可篡改、可追溯。不断跟进和研究新的安全协议，如 TLS 1.3、QUIC 等，提高数据传输的安全性。

5 结论

基于强隔离访问控制的数据安全保护技术在保障数据安全、防止非法访问和数据泄露等方面具有重要意义，是构建安全可靠的信息系统的基础。随着信息系统的复杂性和数据量的增加，强隔离访问控制技术面临着如下挑战：如何平衡安全性与可用性、如何实现大规模分布式环境下的访问控制、如何应对新型攻击手段等。针对上述挑战，本文提出研究更加灵活、可扩展的访问控制模型，以提高系统的适应性和可扩展性。优化访问控制策略，使其更适应不同场景下的安全需求。结合人工智能、大数据等技术，实现智能化的访问控制；基于强隔离访问控制的数据安全保护技术是信息安全领域的重要研究方向，未来需进一步深化理论研究和技术创新，以应对不断变化的网络安全威胁。

参考文献

[1] 林维涛.多信道安全隔离和传输安全防护系统模型设计及其评估[D].电子科技大学,2023.

[2] 蒋鸿城,赵磊,蒋锦霞,等.基于消息中间件的电力内外网数据安全高效传输技术[C]//中国电机工程学会电力通信专业委员会.中国电机工程学会电力通信专业委员会第十三届学术会议论文集.国网浙江省电力有限公司信息通信分公司;,2022:4.

[3] 胡光俊,李海威,王锐.基于多层次行为安全的关键信息基础设施安全防护技术研究[J].警察技术,2021,(01):8-11.

[4] 王勇,辛存生,阎志军.基于强隔离的高性能内外网网关的研究与实现[J].新型工业化,2020,10(08):19-20+23.

[5] 余劲.基于CPU硬件特性的软件安全高效隔离技术研究[D].南京大学,2020.