基于数据加密技术的医院信息管理系统通信安全防御研究

王 俊，杜晨扬*

（北京大学肿瘤医院内蒙古医院（内蒙古医科大学附属肿瘤医院），内蒙古 呼和浩特 010000）

摘 要 医院信息管理系统（HIS）在提高医疗服务效率和质量方面发挥着重要作用。然而，HIS面临的安全威胁也日益严峻，尤其是数据泄露和通信安全问题。黑客攻击和内部泄密等安全事件频发，对患者隐私和医院运营造成了严重威胁。本研究探讨基于数据加密技术的医院信息管理系统通信安全防御策略。通过分析对称加密和非对称加密技术的应用，提出了一系列具体的防御措施，如数据传输加密、患者信息泄露防范、访问控制与身份认证等。这些措施的实施不仅提高了系统的安全性和稳定性，还有效保障了患者的隐私和数据的完整性，以期为医院信息管理系统的安全运行提供坚实的技术支持。

关键词 医院信息管理系统；数据加密技术；通信安全

中图分类号：TN918 **文献标志码**：A **文章编号**：2097-3365(2024)09-0025-03

医院信息管理系统(Hospital Information System，HIS)是医疗行业的重要组成部分，HIS通过数字化手段，将患者的诊疗信息、病历数据、检验报告等整合到一个统一的平台上，极大地提高了医疗服务的效率和准确性。随着医疗数据的日益增加和信息化程度的提升，HIS不仅能够实现数据的高效管理，还能够提供数据分析、决策支持等功能，为医疗人员提供了强大的辅助工具[1]。此外，HIS在优化医院资源分配、缩短患者等待时间、提高诊疗质量等方面也发挥了积极作用。因此，HIS在现代医疗系统中的地位和作用越来越重要。

1 医院信息管理系统与安全威胁

1.1 医院信息管理系统概述

随着医疗行业的数字化转型，医院信息管理系统（HIS）已经成为现代医院运作的核心组成部分。本研究的系统MedSecure HIS旨在提升医院的运营效率和医疗服务质量。MedSecure HIS包括患者管理、临床管理、检验与检查、药品管理、财务管理和系统管理等多个模块，通过这些模块的协同工作，实现了医院内部各个部门的信息共享与无缝连接[2]。

1.2 系统架构与功能模块

MedSecure HIS采用模块化架构，确保各个功能组件能够高效、稳定地运行，并能根据需要灵活扩展。系统架构主要分为前端应用层、中间业务层和后端数据层，各层之间通过安全、可靠的通信协议进行交互。（见图1）

前端应用层涵盖医生工作站、护士工作站、患者门户和管理人员工作站，提供诊疗、患者管理、个人信息查询和业务统计等功能。中间业务层包括患者管理、临床管理、检验与检查、药品管理、财务管理和系统管理等模块，支持医院日常运营的各项业务。后端数据层负责数据存储和管理，包括数据库服务器、备份服务器和日志服务器，确保数据的完整性、安全性和可追溯性。

1.3 面临的主要安全威胁

MedSecure HIS在提升医院效率和服务质量的同时，面临多重安全威胁。为保障系统安全性和患者隐私，研究围绕这些威胁展开，旨在通过数据加密、加强访问控制和日志审计、实施综合性防御措施、提升员工安全意识、定期安全评估和漏洞扫描以及确保数据传输加密等措施，有效防御这些威胁。

2 数据加密技术在系统中的应用

2.1 数据加密技术概述

数据加密技术主要分为对称加密和非对称加密两大类[3]，每种加密技术都有其独特的应用场景和优缺点。MedSecure HIS广泛应用数据加密技术，确保系统安全性和患者隐私。数据存储层面采用对称加密技术

*本文通讯作者，E-mail：dcy8412576@163.com。

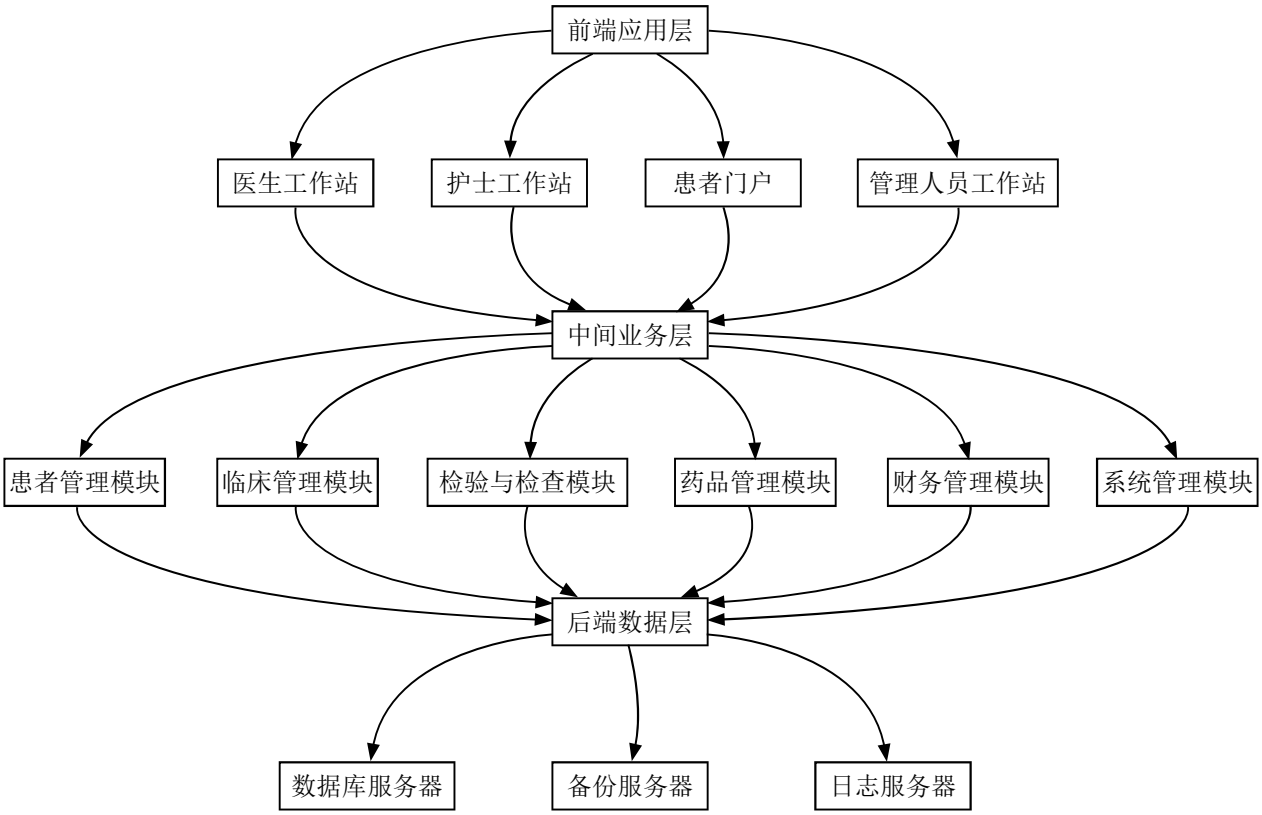

图1 系统架构图

加密敏感数据和备份文件。数据传输层面使用SSL/TLS协议保障安全。系统还通过非对称加密实现强身份认证和访问控制，并使用数字签名技术确保数据完整性和真实性。

2.2 对称加密与非对称加密

常用的对称加密算法包括AES（Advanced Encryption Standard）[4]。为了比较不同对称加密算法的性能，研究对AES、DES和3DES进行了加密速度测试。表1展示了每种算法在处理1MB数据时的加密时间（单位：毫秒）。

从表1和图2中可以看出，AES算法在加密速度上明显优于DES和3DES，因此在MedSecure HIS中，研究主要采用AES算法对患者数据进行加密存储和传输。

表1 加密算法性能对比表

加密算法	加密时间（ms）
AES	5
DES	20
3DES	60

非对称加密由于其安全性高，特点是使用公钥进行加密，私钥进行解密，解决了对称加密中密钥分发和管理的问题。非对称加密的安全性与其密钥长度密切相关。

3 通信安全与信息防泄露防御策略

3.1 安全需求分析

MedSecure HIS是一个复杂的医院信息管理系统，其安全需求主要体现在保护患者隐私、防止数据泄露和确保系统稳定运行等方面。其包括保障数据在存储和传输过程中的机密性、完整性和可用性；防范内部和外部的非法访问和攻击；确保系统在遭受攻击或出现故障时能够快速恢复，并保持连续性和可靠性。为了实现这些目标，系统必须采用多层次、多方面的安全防御措施，涵盖数据加密、访问控制、身份认证、系统监控和漏洞修复等领域。

3.2 数据传输加密

为了防止数据在传输过程中被截获、篡改或者泄露，系统采用SSL/TLS协议对所有网络通信进行加密。SSL/TLS协议通过非对称加密技术进行密钥交换，随后使用对称加密技术对数据进行加密传输，确保数据在客户端和服务器之间的传输过程中保持高度的机密性和完整性。这种双重加密机制不仅提升了数据传输的安全

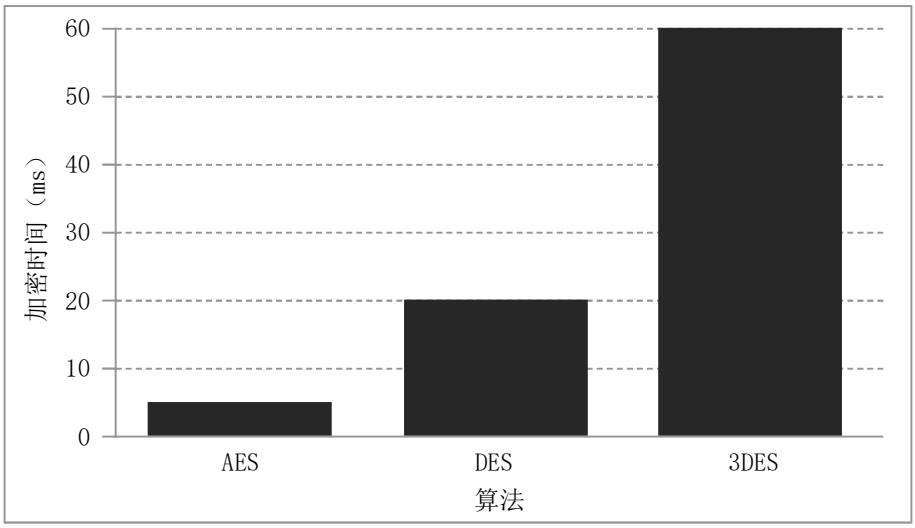

图 2 对称加密算法性能比较

性，还提高了系统的整体通信效率。

3.3 患者信息泄露的防范

患者信息的泄露不仅会对患者的隐私造成严重侵害，还可能带来法律和经济上的风险。为防止患者信息泄露，MedSecure HIS 采取了一系列防护措施，包括对患者数据进行加密存储、严格控制数据的访问权限、定期进行安全审计和监控。同时，系统还采用数据脱敏技术，在展示或使用敏感数据时，对部分数据进行遮盖或替换处理，确保即使数据被泄露，也不会暴露患者的真实身份和隐私信息。

3.4 人员信息防范策略

MedSecure HIS 通过建立完善的人员信息防范策略，来减少内部威胁。具体措施包括对员工进行定期的安全培训，增强其安全意识和防范能力；实施严格的访问控制，根据岗位职责分配权限，确保员工只能访问与其工作相关的数据和功能；对敏感操作进行多因素认证，防止非法使用他人账号进行恶意操作。此外，系统还记录并监控所有的操作日志，及时发现和处理异常行为。

3.5 访问控制与身份认证

强大的访问控制与身份认证机制是保障系统安全的重要基础。MedSecure HIS 通过多层次的访问控制策略，确保只有经过授权的用户才能访问相应的数据和功能模块。系统采用基于角色的访问控制（RBAC），根据用户的角色和职责分配权限，避免权限过度集中[5]。

为了进一步强化访问控制与身份认证机制，MedSecure HIS 系统还引入了多因素认证（MFA）技术，通过结合密码、动态令牌和生物识别等多种认证方式，提升了身份验证的安全性。此外，系统对所有用户的登录和操作行为进行实时监控和记录，建立了异常行为检测模型，能够迅速识别并响应潜在的安全威胁。这种综合的防御策略，不仅提高了系统的安全性，还确保了患者数据的高度保密性和完整性。通过这种方式，系统有效防范了内部和外部的各种安全攻击。

4 结束语

通过对 MedSecure HIS 的深入研究，本文明确了医院信息管理系统在数据加密和安全防御方面的关键要素，探讨了对称与非对称加密技术在各环节的应用，以及多层次安全防御措施的实施。这些技术和策略的综合运用提高了系统的安全性和可靠性，有效保护了患者隐私和医院核心数据，推动了医院信息化管理水平的提升。

参考文献：

[1] 龙雨希,林怀德,刘梦楚,等.基于微信平台的信息管理系统在眼遗传病临床基因检测中的应用[J].眼科学报,2024,39(01):1-10.

[2] 张泽宇,郭宜家,刘宇航,等.电子病历管理系统及其加密技术的设计与实现[J].无线互联科技,2018,15(15):49-52.

[3] 刘孝鼎.医院网络安全防御管理系统透析[J].网络空间安全,2024,15(02):78-81.

[4] 王医成,贺康,唐博,等.基于微服务架构的生物样本库信息管理系统的建设与应用[J].中国医疗设备,2023,38(11):105-110.

[5] 李悦.基于PKI技术的医院电子档案安全管理系统研究[J].科学与信息化,2023(21):178-180.