基于人工智能的医院网络安全漏洞自动化扫描与修复方法

梁衍旭

（郓城县潘渡镇卫生院，山东 菏泽 274700）

摘 要 人工智能在医疗领域的应用已经取得了显著的成果，然而随之而来的是医院网络安全问题的日益突出。医院作为关乎人民生命健康的重要单位，其网络安全问题不容忽视。网络安全漏洞的存在给医院的信息系统带来了巨大的风险，可能导致病人数据泄露、医疗设备被恶意操控等严重后果。因此，研究和实施一种基于人工智能的医院网络安全漏洞自动化扫描与修复方法成为当下迫切需要解决的问题。

关键词 人工智能；医院网络安全漏洞；自动化扫描修复

中图分类号：TP18 **文献标识码**：A **文章编号**：2097-3365(2024)03-0104-03

传统的网络安全扫描方法往往依赖于人工操作，效率低下且容易出错，而基于人工智能的扫描与修复方法则能够充分利用机器学习和自然语言处理等技术，自动化地发现和修复医院网络中存在的安全漏洞。通过分析大量的网络数据和漏洞信息，人工智能系统能够准确识别潜在的威胁，并提供相应的修复建议，这种方法不仅能够提高扫描效率，还能够减少人为操作带来的错误和遗漏，提高医院网络的整体安全性。应不断研究基于人工智能的医院网络安全漏洞自动化扫描与修复方法，为医院网络安全漏洞扫描与修复提供高效而准确的方法。

1 医院网络安全的重要性

1.1 保护患者隐私

医院网络存储了大量的患者敏感信息，包括个人身份信息、病历、诊断结果等，这些数据一旦被黑客攻击或泄露，将对患者的隐私和权益造成严重威胁。个人身份信息一旦落入不法分子手中，可能被用于进行诈骗、冒名顶替等违法犯罪行为。而患者的病历和诊断结果等敏感信息，一旦被泄露，不仅可能引起个人的尴尬和困扰，还可能被不法分子利用进行敲诈勒索，所以加强医院网络安全可以有效保护患者的隐私，维护患者的合法权益[1]。

1.2 稳定医院正常运行

医院网络承载着医疗设备、医疗信息系统和其他相关系统的运行，如果这些系统遭到黑客攻击，将严重影响医院的正常运行。例如，黑客可能篡改患者的病历数据，导致错误的诊断和治疗，甚至可能影响到手术和急救等关键环节。医疗设备的异常操作也可能对患者的健康造成严重威胁，所以保障医院网络安全对于保障患者的生命安全至关重要。

1.3 保障患者治疗安全

医院网络涉及医疗设备的联网和远程监控，一些高级医疗设备如心脏起搏器、呼吸机等可以通过网络进行远程监控和控制，这为医生提供了更好的治疗手段，但同时也带来了潜在的风险。如果黑客入侵这些设备的网络，有可能导致设备失控或被篡改，从而对患者造成危害，所以确保医院网络的安全性对于保障患者的治疗安全至关重要。

2 医院网络安全存在的问题

2.1 普遍存在安全漏洞

一方面，医院网络设备可能存在安全漏洞，如路由器、交换机、防火墙等，这些设备如果未及时更新补丁或配置不当，容易被黑客利用进行攻击或入侵，从而导致医院信息系统遭受破坏或数据泄露。另一方面，医院员工对网络安全的意识和培训不足，容易成为黑客攻击的目标，一些员工可能使用弱密码或未能定期更改密码，这使得黑客能够轻易猜测或破解密码，进而获取敏感信息[2]。

2.2 网络设备和软件更新滞后

医院网络设备和软件的更新和升级是确保网络安全的关键措施之一，然而由于医院常常注重医疗技术的更新和设备的购买，对网络设备和软件的更新升级却相对较少关注。这导致医院网络设备和软件长时间没有得到及时的安全补丁和更新，容易受到已知漏洞

的攻击，例如，近年来流行的勒索病毒攻击就是利用已知漏洞入侵网络系统，对医院信息系统造成严重破坏，甚至导致医院瘫痪。

2.3 网络安全管理机制不健全

医院网络安全管理机制不健全是一个普遍存在的问题，在医院网络中，缺乏明确的安全策略和指导，没有完善的安全管理流程和制度，医院网络管理员对于网络安全的重要性认识不足，缺乏对潜在威胁的及时识别和应对能力。同时医院内部的人员管理也存在问题，员工的安全意识普遍较低，对于网络安全风险的认知和防范措施欠缺。

2.4 缺乏灾备和恢复机制

医院网络缺乏灾备和恢复机制，一旦发生网络安全事件，医院往往无法迅速做出应对，导致严重的后果。医院网络数据的备份和恢复机制不完善，一旦遭受黑客攻击、病毒感染或硬件故障，可能导致重要数据的丢失和服务的中断。此外，医院在面对网络安全事件时缺乏应急预案和团队，无法快速有效地进行应急响应和恢复工作，给医院的运营和患者的安全带来严重影响。

3 基于人工智能的医院网络安全漏洞扫描方法

3.1 数据收集与分析

数据收集是基于人工智能的漏洞扫描的关键步骤之一，在这一阶段，需要收集医院网络中的各类数据，包括网络拓扑结构、设备配置、日志信息等。通过使用网络扫描工具和安全设备，可以主动收集目标网络的信息。此外，还可以利用被动式监控和数据包分析技术，实时获取网络流量和数据包信息，通过大量的数据收集，可以为后续的漏洞分析提供充分的依据。数据分析是基于人工智能的漏洞扫描方法中至关重要的一步，通过使用机器学习和数据挖掘技术，可以对收集到的数据进行深度分析和处理[3]。可以建立漏洞数据库，将已知的漏洞信息进行整理和归类，以便与扫描结果进行对比和匹配，或者可以利用数据分析算法，对收集到的网络数据进行模式识别和异常检测，及时发现网络中存在的潜在漏洞，还可以通过挖掘网络日志和事件信息，可以追踪和还原网络攻击过程，为后续的漏洞修复提供有效的参考。在数据收集和分析环节中，需要注意确保数据的完整性和准确性，避免因为错误或遗漏导致的误判，应保护数据的安全性，采取加密和访问控制等措施，防止数据泄露和非法访问。还要及时更新漏洞数据库和分析算法，跟进最新的漏洞信息和攻击手法，提高漏洞扫描的准确度和效率。

3.2 漏洞检测与识别

漏洞检测是基于人工智能的漏洞扫描方法的关键步骤之一，在这一阶段，系统需要通过网络扫描工具对医院网络进行全面扫描，收集各类设备和应用程序的信息，通过分析网络流量、检测网络中的异常行为和漏洞特征，系统能够准确识别出潜在的漏洞问题，同时系统还可以利用机器学习算法对历史数据进行分析，建立漏洞模型，提高漏洞检测的准确性和效率。漏洞识别是基于人工智能的漏洞扫描方法的另一个关键环节，在这一阶段，系统需要将扫描得到的漏洞信息与已知的漏洞数据库进行比对，以确定漏洞的类型、危害程度和修复建议。通过利用人工智能技术，系统能够自动识别和分类漏洞，提供准确的漏洞分析和解决方案。同时系统还可以利用自然语言处理技术，将漏洞信息转化为易于理解和操作的形式，方便医院管理者和技术人员进行进一步的漏洞修复工作。在漏洞检测与识别的过程中，数据的质量和安全性至关重要，要确保数据的准确性和完整性，避免因数据误差或不完整导致的误判。要保护数据的安全性，采取加密和访问控制等措施，防止数据泄露和非法访问，还要及时更新漏洞数据库和分析算法，跟进最新的漏洞信息和攻击手法，提高漏洞检测与识别的准确度和效率。

3.3 漏洞评估与分类

漏洞评估是基于人工智能的漏洞扫描方法的核心环节之一，在这一阶段，系统将对医院网络中的漏洞进行全面评估，以确定漏洞的危害程度和潜在风险。通过人工智能技术的应用，系统可以自动化地分析和评估各种已知漏洞，包括操作系统漏洞、应用程序漏洞、网络设备漏洞等，同时系统还可以利用机器学习算法，通过学习历史漏洞数据和实时网络流量，提高漏洞评估的准确性和效率[4]。漏洞分类也是基于人工智能的漏洞扫描方法中不可或缺的环节，在漏洞评估之后，系统将根据漏洞的特征和危害程度，将漏洞进行分类。常见的漏洞分类包括远程代码执行漏洞、拒绝服务漏洞、跨站脚本漏洞等，通过将漏洞进行分类，系统可以更好地理解漏洞的本质和影响范围，并为后续的修复工作提供指导。

3.4 漏洞定位与修复建议生成

在漏洞定位中，系统会对医院网络进行全面的扫描，收集网络中的各种安全漏洞，通过人工智能技术的应用，系统可以自动分析漏洞的类型、来源和可能造成的危害程度。同时系统还可以根据已有的安全漏洞库和相关的安全知识进行对比和参考，以进一步确认漏洞的准确性和重要性。在漏洞定位的基础上，基于人工智能的医院网络安全漏洞扫描方法还能生成修复建议，通过对扫描结果的分析，系统可以自动生成

相应的修复建议，帮助医院网络管理员更好地修复漏洞。修复建议的生成是基于人工智能算法对漏洞的分析和评估，系统会根据漏洞的类型和危害程度，提供相应的解决方案和修复措施，这些修复建议可以帮助医院网络管理员迅速找到并解决网络安全漏洞，提高系统的安全性。

4 基于人工智能的医院网络安全漏洞修复方法

4.1 修复建议的优先级排序

基于人工智能的医院网络安全漏洞修复方法通过对医院网络系统中潜在漏洞进行全面扫描和分析，识别出存在的安全漏洞，要根据漏洞的严重程度、影响范围和潜在风险等因素，制定修复建议，并按照优先级排序，以确保修复工作的高效性和有效性。在确定修复建议的优先级时，应考虑根据漏洞对医院网络系统的影响程度，将其划分为高、中、低三个级别，高级别漏洞可能导致系统瘫痪或敏感数据泄露，应优先修复；中级别漏洞可能引发数据损坏或恶意软件感染，也需要及时修复；低级别漏洞对系统影响较小，可以稍后处理[5]。根据漏洞可能对医院网络系统的各个模块和功能造成的影响，将其划分为广泛、局部、个别三个级别，广泛影响的漏洞需要优先修复，以保障整个系统的安全性；局部影响的漏洞可以稍后处理；个别影响的漏洞可以放在修复优先级的后面。根据漏洞被黑客利用的可能性和造成的潜在危害，将其划分为高、中、低三个级别，高风险漏洞可能导致重大的数据泄露和系统瘫痪，需要尽快修复；中风险漏洞可能导致部分数据泄露和系统异常，也需要及时修复；低风险漏洞对系统的影响较小，可以稍后处理。

4.2 自动化修复与补丁管理

基于人工智能的安全漏洞扫描技术可以高效地检测医院网络系统中的漏洞，这些技术能够自动扫描整个网络，识别出存在的漏洞，并生成相应的修复方案，通过使用人工智能技术，医院网络管理员可以大大减少手动检测漏洞所需的时间和精力，提高修复效率。自动化修复是基于人工智能的医院网络安全漏洞修复方法的核心，一旦漏洞被检测出来，系统可以自动进行修复操作，无需人工干预，这种自动化修复能够快速有效地消除漏洞，降低黑客攻击的风险，并保护医院网络系统的安全。补丁管理也是基于人工智能的医院网络安全漏洞修复方法中不可或缺的一部分，补丁是修复漏洞的关键措施之一，但大规模的医院网络系统中，漏洞数量繁多，补丁管理变得非常复杂。利用人工智能技术，可以自动跟踪漏洞修复进展，及时更新补丁，并对系统进行监控和管理，通过智能化的补丁管理，医院网络管理员可以更好地掌握漏洞修复情况，及时采取措施，提升网络系统的安全性。

4.3 修复效果评估与反馈机制

在修复效果评估方面，可以采用多种指标和评估方式，可以通过对修复后的系统进行全面的功能和性能测试，以评估系统的稳定性和可用性[6]。或者通过模拟各种攻击和漏洞利用情景，对修复后的系统进行渗透测试，以评估系统的安全性和抗攻击能力。还可以根据测试结果和评估指标，生成评估报告，对修复效果进行综合评估。评估报告中除了对修复效果进行定量评估外，还需要对修复过程中的问题和不足进行反馈，基于人工智能的医院网络安全漏洞修复方法会自动收集修复过程中的数据和日志，并进行分析和挖掘，通过对这些数据和日志的分析，可以发现修复过程中的潜在问题和不足之处，以及可能存在的新的安全漏洞，修复团队可以根据这些反馈信息及时进行优化和改进，以进一步提高修复效果和系统的安全性。

5 结语

基于人工智能的医院网络安全漏洞自动化扫描与修复方法，为医院网络安全提供了一种高效、准确的解决方案。通过利用人工智能算法的强大计算能力和智能化分析能力，该方法能够全面扫描医院网络中的安全漏洞，并自动修复这些漏洞，有效提升了医院网络的安全性和稳定性。这一方法的应用不仅可以减少医院网络遭受恶意攻击和数据泄露的风险，还能够保护医院的核心业务运行和患者信息的安全。未来随着人工智能技术的不断发展和完善，基于人工智能的医院网络安全漏洞自动化扫描与修复方法有望成为医院网络安全的标准解决方案。

参考文献：

[1] 何丽君，周晓娓.基于人工智能下医院耳鼻咽喉科网络安全信息化的建设[J].中国医学文摘（耳鼻咽喉科学），2021,36(04):210-212.
[2] 巫新玲，李文侠.人工智能下医院网络安全信息化的建设路径探索[J].大众标准化，2021(11):182-184.
[3] 卢熙.医院网络安全入侵防御系统研究与设计[J].网络安全技术与应用，2021(02):124-126.
[4] 赵桂兵.基于人工智能下医院网络安全信息化的建设[J].信息技术与信息化，2020(02):205-207.
[5] 林龙滔，马盛丹.医院信息化网络安全与防御措施研究[J].电脑编程技巧与维护，2019(12):171-172.
[6] 郑序颖.医学装备智能化带来数据管理新命题，多维度医院信息安全建设至关重要[J].科技新时代，2018(04):30-31.