# 人工智能医疗器械软件网络安全技术研究

宁春华[1] 马方达[2] 王增利[3]
1. 济南百博生物技术股份有限公司 山东 济南 250000；
2. 青岛顺时医疗科技有限公司 山东 青岛 266000；
3. 山东恒麟智能科技有限公司 山东 济南 250000

**摘 要** 随着人工智能技术在医疗器械领域的广泛应用，医疗器械软件的网络安全问题日益凸显。为了促进医疗器械网络安全的合规化建设，保障患者生命安全，本文将从人工智能医疗器械软件概述出发，阐述当前人工智能医疗器械软件面临的网络安全挑战。基于此，提出了一系列针对性的网络安全技术，如加密技术、入侵检测与防御技术等。通过综合运用这些网络安全技术，能够有效提升人工智能医疗器械软件的网络安全性，为提升该领域的网络安全水平提供理论支撑和技术参考。

**关键词** 人工智能；医疗器械软件；网络安全

**Research on Cybersecurity Technology for AI Medical Device Software**

Ning Chun-hua[1], Ma Fang-da[2], Wang Zeng-li[3]
1. Jinan Biobase Biotech Co., Ltd., Jinan 250000, Shandong Province, China;
2. Qingdao Shunshi Medical Technology Co., Ltd., Qingdao 266000, Shandong Province, China;
3. Shandong Henglin Intelligent Technology Co., Ltd., Jinan 250000, Shandong Province, China

**Abstract** With the widespread application of artificial intelligence technology in the medical device field, cybersecurity issues related to medical device software have become increasingly prominent. To promote the compliant construction of cybersecurity for medical devices and ensure patient safety, this paper starts with an overview of AI medical device software and elaborates on the current cybersecurity challenges faced by such software. Based on this analysis, a series of targeted cybersecurity technologies are proposed, including encryption technology, intrusion detection and prevention technology, among others. Through the comprehensive application of these cybersecurity technologies, the network security of AI medical device software can be effectively enhanced, providing theoretical support and technical reference for improving the level of cybersecurity in this field.

**Key words** Artificial Intelligence; Medical Device Software; Cybersecurity

在当今数字化与智能化浪潮席卷的时代，人工智能已成为推动各个领域革新的核心力量，医疗器械领域自然也不例外。人工智能医疗器械软件的涌现，极大地提升了医疗诊断的效率与精准度，为患者带来了更为优质的医疗服务体验[1]。然而，由于该软件涉及大量敏感的患者数据和关键的医疗决策信息，网络安全问题也随之成为不可忽视的重大隐患。一旦人工智能医疗器械软件遭受网络攻击，不仅会造成患者个人信息的泄露，更可能干扰医疗设备的正常运行，导致诊断结果出现偏差，严重威胁患者的生命健康。因此，开展人工智能医疗器械软件网络安全技术研究具有至关重要的现实意义。

## 1 人工智能医疗器械软件概述

人工智能医疗器械软件是一种融合了人工智能技术与医疗专业知识的创新型软件产品。它依托先进的算法和海量的医疗数据，能够模拟人类的智能思维和决策过程，为医疗领域提供精准、高效的辅助支持。该软件主要由数据层、算法层和应用层构成，如图1所示。

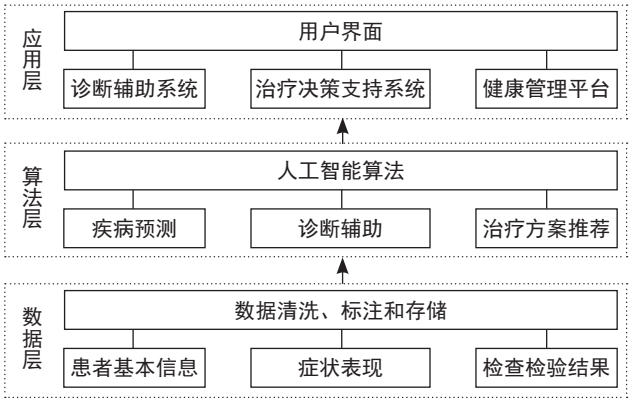



图1 人工智能医疗器械软件

数据层是人工智能医疗器械软件的基石，汇聚了来自医院信息系统、电子病历、医学影像等多渠道的海量医疗数据。这些数据涵盖了患者的基本信息、症状表现、检查检验结果等各个方面，为后续的分析和决策提供了丰富的素材。同时，数据层还负责对数据进行清洗、标注和存储，以确保数据的质量和可用性[2]。

算法层是人工智能医疗器械软件的核心。它运用深度学习、机器学习等先进的人工智能算法，对数据层提供的数据进行挖掘和分析。通过建立各种模型，算法层能够发现数据中的潜在规律和模式，从而实现疾病的预测、辅助诊断和治疗方案推荐等功能。例如，在医学影像诊断中，算法层可以通过对大量的影像数据进行学习，识别出病变的特征和类型，为医生提供准确的诊断建议。

应用层是人工智能医疗器械软件面向用户的窗口。它将算法层的分析结果以直观、易懂的方式呈现给医生和患者。应用层可以包括诊断辅助系统、治疗决策支持系统、健康管理平台等多种形式。这些应用系统能够帮助医生提高诊断效率和准确性，为患者提供个性化的医疗服务。

## 2 人工智能医疗器械软件面临的网络安全挑战

### 2.1 数据泄露

人工智能医疗器械软件在运行过程中，会收集、存储和处理大量敏感的患者医疗数据，这些数据包含了患者的个人身份信息、健康状况、疾病史等高度隐私内容，因而数据泄露风险成为其面临的重大网络安全挑战。

在数据收集环节，由于软件可能需要与多种医疗设备、系统进行交互，接口的复杂性增加了数据泄露的潜在风险。一些不规范的设备可能存在安全漏洞，黑客可以利用这些漏洞拦截数据传输，获取患者的敏感信息。而且，在数据收集过程中，如果缺乏严格的身份验证和授权机制，不法分子可能伪装成合法用户，骗取系统的信任从而获取数据[3]。

在数据存储方面，大量的医疗数据通常会集中存储在服务器中。若服务器的安全防护措施不到位，如未进行加密处理，缺乏定期的数据备份和恢复机制等，一旦遭受网络攻击，如黑客入侵，恶意软件感染等，存储的数据就可能被窃取或篡改。

数据处理阶段，人工智能医疗器械软件对数据进行分析、建模和算法运算时，若软件本身的代码存在漏洞，黑客便可能利用这些漏洞植入恶意代码，干扰数据处理过程，导致分析结果出错，进而影响医生的诊断和治疗决策。而且，部分人工智能算法的复杂性使得难以对其进行全面的安全审查，这也为潜在的安全威胁提供了可乘之机。

### 2.2 网络攻击

人工智能医疗器械软件因依赖网络进行数据传输，极易遭受DDoS攻击、中间人攻击等网络安全威胁。

分布式拒绝服务攻击通过大量虚假请求淹没软件的服务器，导致服务器无法正常响应合法用户的请求。对于人工智能医疗器械软件而言，这种攻击可能导致软件系统崩溃，无法及时处理患者数据和提供诊断结果，严重影响医疗服务的连续性和有效性，甚至在紧急情况下可能危及患者生命。

中间人攻击是指攻击者在数据传输过程中拦截并篡改数据，使发送方和接收方之间的通信受到干扰。在人工智能医疗器械软件的网络环境中，攻击者可以通过中间人攻击窃取患者的敏感数据，或者篡改传输中的医疗数据，导致医生接收到错误的信息，做出错误的诊断和治疗决策。例如，攻击者可能会将患者的检查结果进行修改，使得原本正常的指标显示为异常，从而误导医生进行不必要的治疗；或者将严重的病情信息淡化，延误患者的治疗时机。

此外，医疗物联网的普及虽提升了数据共享效率，但也扩大了攻击面。单一设备的安全漏洞可能被利用，进而扩散至整个网络，威胁系统的整体安全运行。

### 2.3 算法安全隐患

在人工智能医疗器械软件中，人工智能算法通常基于大量的训练数据来学习和优化模型。若训练数据存在偏差、不完整或者被污染，那么训练出来的算法模型就可能存在缺陷。例如，在某些医疗影像识别算法的训练过程中，如果训练数据集中某种疾病的样本数量过少，可能导致算法在实际应用中对该疾病的识别准确率降低，从而影响诊断的准确性。

同时，部分人工智能算法具有黑盒特性，使得决策过程难以解释和理解。医生在使用这类软件进行诊断时，往往只能得到最终的结果，而无法知晓算法是如何得出该结论的。这使得医生难以判断结果的可靠性，也无法在出现问题时进行有效的调试和修正。而且，这种黑盒特性也为攻击者提供了可乘之机，攻击者可以利用算法的不可解释性，通过注入恶意数据等方式操纵算法的输出结果，干扰医疗决策[4]。

此外，随着人工智能技术的不断发展，新的算法不断涌现，而相应的安全标准和评估机制却相对滞后。缺乏统一的安全规范，使得不同厂家开发的人工智能医疗器械软件在算法安全方面存在较大差异，增加了整体的安全风险。同时，对算法的更新和维护过程也可能引入新的安全漏洞，如果在更新过程

中没有进行严格的安全测试，可能会导致软件在更新后出现新的安全问题，给患者的医疗安全带来潜在威胁。

## 3 人工智能医疗器械软件网络安全技术

### 3.1 数据加密技术

数据加密技术是保障人工智能医疗器械软件数据安全的核心。在数据收集阶段，可采用AES等对称加密算法对患者敏感数据进行即时加密，防止其在传输过程中被非法拦截并破解。

在数据存储环节，可采用非对称加密技术保护服务器中的医疗数据，使用公钥加密、私钥解密，即使服务器遭攻击也能保障数据安全。同时，定期备份数据并存储于加密介质中，如加密硬盘或磁带库，实现双重防护[5]。

在数据处理阶段，可运用同态加密技术直接在密文上进行计算，无须解密即可完成分析建模，有效降低处理环节的数据泄露风险。例如，在对患者基因数据进行复杂分析时，同态加密能在保证隐私的前提下完成精准运算。

此外，应采用密钥管理系统集中管理密钥，定期更换以防止泄露。通过设置多级访问权限，严格限制密钥使用，确保仅授权人员可解密数据。

### 3.2 入侵检测与防范技术

针对网络攻击，入侵检测与防范技术能实时监测人工智能医疗器械软件网络的运行状态。通过部署入侵检测系统（IDS）和入侵防御系统（IPS），可以对网络流量进行实时分析，及时发现异常的流量模式和攻击行为。

入侵检测系统主要通过事件产生器、事件数据库、事件分析器和管理控制台等对网络中的各种事件进行分析和判断。事件产生器利用传感器收集网络中的各类数据，如数据包的来源、目的地址、传输时间等信息，并将这些数据传送到事件数据库中进行存储。事件数据库则通过审计记录库分为行为数据库和入侵数据库，并利用检测器对数据进行深入分析，检测出潜在的入侵事件，并向事件分析器发送警报。事件分析器将根据警报信息进一步验证这些警报的真实性，区分合法行为和异常记录，并将结果反馈给管理控制台。管理控制台作为入侵检测系统的用户界面，为用户提供操作界面，进行操作和管理。当检测到入侵事件时，管理控制台会及时通知相关人员，以便采取相应的措施。

入侵防范系统则是在入侵检测系统的基础上，具备主动防御功能。当检测到人工智能医疗器械软件网络入侵行为时，它能自动采取措施阻止攻击，避免软件系统受到损害。当发现分布式拒绝服务（DDoS）攻击时，入侵防范系统可通过识别并过滤掉大量虚假请求，保证服务器能够正常响应合法用户的请求，维持软件系统的稳定运行。对于中间人攻击，它能实时监测数据传输的完整性，一旦发现数据被篡改，立即中断异常连接，并向医生、护士等相关人员发出警报。

### 3.3 算法安全增强技术

为保障人工智能医疗器械软件的算法安全，在训练前需严格筛选和处理数据，确保其完整性、准确性与代表性，通过清洗、去噪、归一化等手段提升数据质量。例如，医疗影像数据的标注需准确一致，防止算法习得错误信息。算法设计应注重可解释性，避免黑盒模型带来的安全隐患。采用基于规则的算法或可解释性技术，使诊断结果可追溯，决策过程更透明，帮助医生判断结果的可靠性。此外，需建立统一的算法安全标准与评估流程，在产品上市前进行全面审查与多轮测试，确保无重大漏洞。算法更新应遵循严谨的流程，事先开展充分的安全测试，严格控制访问权限，并建立回滚机制，以便在更新出现问题时迅速恢复稳定版本。

## 4 结束语

综上所述，人工智能医疗器械软件在医疗领域发挥着重要作用，但面临着数据泄露、网络攻击和算法安全隐患等诸多网络安全挑战。通过数据加密技术，对数据全生命周期进行加密保护并严格管理密钥；利用入侵检测与防范技术，实时监测网络状态并主动防御攻击；采用算法安全增强技术，从数据筛选、算法设计、标准制定到更新维护等多方面保障算法安全。未来，需持续加强技术创新与标准完善，不断提升人工智能医疗器械软件的网络安全性，为医疗服务的安全与高效提供坚实保障。

## 参考文献

[1]冯金玲.医疗器械PC端软件的网络安全测试技术分析[J].中国信息界,2025(9):241-243.

[2]林香,侯建勋,古锐鹏,等.浅谈医疗器械软件网络安全[J].网络安全技术与应用,2024(8):109-110.

[3]罗维娜,李澍,王晨希,等.移动医疗网络安全监管策略研究[J].中国医疗设备,2017,32(6):20-22,31.

[4]陈钿,曾祥卫,孙志刚,等.人工智能医疗器械软件网络安全技术考量[J].中国医疗器械信息,2022,28(15):5-7.

[5]肖斌,陆晓琳.医疗器械的网络安全质量控制途径分析[J].中国设备工程,2023(10):247-249.

（本文编辑 杜宇琪）