第 2 卷◆第 3 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

公共卫生信息网络数据安全的研究

张晓卓
天津市医学科学技术信息研究所
DOI:10.12238/acair.v2i3.8605

[摘　要] 在信息技术快速发展的时代背景下,公共卫生信息网络已然成为维护国家安全、保障全球公共卫生体系稳健运行的关键。然而,伴随着数据安全问题日渐凸显,严重威胁着公共卫生数据系统运行服务质量。本文基于此,阐述公共卫生信息网络数据安全现状,对数据泄漏、篡改、网络攻击等安全挑战展开分析,并从数据加密、身份验证、访问控制、定期安全审计及法规遵循等角度,研究维护数据安全的策略,旨在构建安全、高效的公共卫生信息网络数据保护体系。
[关键词] 信息网络；公共卫生；数据安全
中图分类号：TP309.2　文献标识码：A

Research on Information Network Data Security in Public Health

Xiaozhuo Zhang
Tianjin Health Information Research Center

[Abstract] In the context of rapid development of information technology, public health information networks have become the key to maintaining national security and ensuring the stable operation of the global public health system. However, as data security issues become increasingly prominent, they pose a serious threat to the quality of public health data system operations and services. Based on this, this article elaborates on the current situation of data security in public health information networks, analyzes security challenges such as data leakage, tampering, and network attacks, and studies strategies for maintaining data security from the perspectives of data encryption, identity verification, access control, regular security audits, and regulatory compliance, aiming to build a secure and efficient public health information network data protection system.
[Key words] information network; Public Health; data security

立足于数字化时代的浪潮,公共卫生信息网络的应用和规模化推广,对于确保公共卫生安全至关重要,能够迅速而灵活地应对突发性公共卫生事件。然而,在医疗数据迅猛增长、广泛共享的新时代背景下,我们也面临着数据泄漏、数据篡改和网络攻击等多重挑战,这些问题对公共卫生决策的科学性、个人隐私的保护乃至国家安全的稳固都构成了严重威胁。因此,当前公共卫生领域迫切需要组织专业力量,加大公共卫生信息网络数据安全的研究力度和深度,积极探索并应用有效的数据保护策略和技术手段,以应对这些严峻的挑战。

1 公共卫生信息网络数据安全现状

1.1数据泄漏风险

当前,大数据在公共卫生事件防控中扮演着举足轻重的支撑角色。然而,其中黑客攻击作为最严峻的威胁形式,他们利用先进的技术手段非法入侵医疗服务系统,窃取、篡改甚至破坏敏感数据,导致严重的数据信息泄露,这无疑对公共卫生决策结果的准确性和可靠性构成了严重威胁。此外,内部工作人员在系统操作过程中,若存在疏忽大意、操作失误或恶意行为等不当行为,同样可能导致数据信息的泄露,给系统安全带来巨大隐患。

1.2数据篡改风险

恶意攻击者篡改关键数据信息,企图误导公共卫生决策,此举构成了极其严峻的安全风险。这种数据篡改的风险,将使得公共卫生政策在制定时基于错误的数据,进而引发资源分配失衡、疫情控制不力、公众健康受损等一系列严重问题。攻击者通过技术手段侵入公共卫生信息系统,擅自修改疾病发病率、疫苗接种率等关键数据,导致决策层在判断和决策时产生方向性错误。更为严重的是,数据篡改还严重损害了公众对公共卫生机构的信任,削弱了公共卫生事件中的合作与响应能力。

1.3网络攻击威胁

网络攻击威胁,特别是勒索软件、病毒以及拒绝服务攻击(DoS/DDoS),对公共卫生信息网络的稳定运行能力构成了严重挑战。知名的勒索软件,如WannaCry、NotPetya等,可在用户毫

文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

无防备的情况下,利用系统漏洞入侵,破坏公共卫生信息网络中的数据信息。此外,CIH、Conficker等病毒不仅可感染系统文件,还可通过网络传播的方式对系统造成破坏。至于SYN Flood、UDP Flood等拒绝服务攻击(DoS/DDoS),它们可通过发送大量无用请求,使目标服务器不堪重负,最终导致服务中断。这些网络攻击对公共卫生信息网络的稳定与安全构成了巨大威胁。

2 数据安全技术与措施

2.1数据加密

为解决网络通信安全问题,一系列先进技术相继问世,包括链路数据加密技术、数字签名技术、节点数据加密技术、密钥数据加密技术、人工智能技术、安全信息摘要技术以及端对端数据加密技术等[1]。这些技术在确保网络通信的安全性方面扮演着举足轻重的角色。在数据加密处理的过程中,常用的技术手段主要包括对称加密和非对称加密。其中,对称加密凭借其高效的运算速度和处理大量数据的能力,在实际应用中备受青睐。对称加密的原理如图1所示,它通过采用相同的密钥对数据进行加密和解密,确保了数据在传输过程中的安全性。

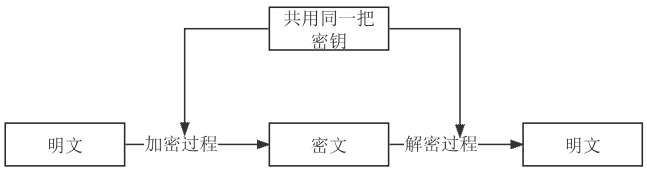

图1 对称加密

在这一背景下,非对称加密技术的优势逐渐显现。通过公钥和私钥的配对使用,不仅为解决密钥分发问题提供了可行方案,而且极大地提升了系统安全性。具体来说,公钥在传播过程中需公开以完成数据加密,而私钥则需严格保密以用于解密。即便出现公钥泄露的情况,私钥依然能够保障数据信息的安全。非对称加密的原理如图2所示。

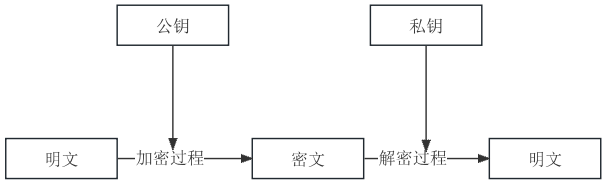

图2 非对称加密

在公共卫生信息网络中,当利用非对称加密方式进行数据信息的传输时,客户端首先会采用预先分配的公钥对敏感数据进行加密处理,确保数据的安全性。紧接着,这些加密后的数据信息将被安全地传输至服务端,服务端随后使用私钥对加密数据进行解密,从而还原出原始的数据内容。尽管非对称加密在安全性方面表现出色,但其运算速度在处理数据时,特别是在处理大量数据信息时,显得相对较慢,这一点尤为突出。

2.2身份验证与访问控制

随着医疗保健现代化的快速演进,个性化的电子病历已成为衡量个体健康状况的关键参考。然而,传统的电子病历管理方案在保障用户身份和数据隐私安全方面存在不足,亟待改进以满足当前的安全需求[2]。传统的静态口令机制,作为一种常见的身份验证方式,要求用户预先设置用户名和登录口令,并将这些信息存储在系统内部数据库中。尽管这种方法成本低廉、操作简单且长期有效,但其安全性却面临挑战,容易被解密和破解。相较之下,动态口令机制通过每次登录生成不同的口令,实现了“一次一密”的安全管理目标,有效避免了静态口令的安全隐患[3]。动态口令基于时间同步、事件同步或挑战/应答机制等多种方式生成,不仅增强了系统的适应性和灵活性,也极大地提升了用户账户的安全性。

除了动态口令机制,密保问题同样是提升账户安全性的重要措施。密保问题通常由账户持有者自行设定,并在需要时用于验证用户身份。在设置密保问题时,建议避免选择过于普遍或易于猜测的问题,并推荐设置三个以上涵盖不同领域的密保问题。此举旨在增加猜测密保问题的难度,进而增强账户的安全性。同时,系统也应定期对用户的密保问题进行更新和验证,以确保其持续有效。此外,图形认证机制也是确保账户安全的重要工具。它通过图形验证码区分计算机程序与真实人类[4]。

生物识别技术作为另一种安全手段,其依据的是用户自身的生物特征信息,如指纹、面部特征、虹膜等。这些特征信息不易遗忘或丢失,防伪性能优越,难以伪造或被盗取,因此被视为一种极其安全有效的验证方式。

访问控制方面,RBAC(基于角色的访问控制)模型为管理工作带来了显著的效益。该模型通过将许可权与角色或用户组紧密相连,实现对用户访问权限的精确管理。在RBAC模型中,系统管理员负责角色的创建、删除、修改以及权利的明确定义,用户则根据所分配的角色获得相应的权利与责任。这种权限分配规则具有强制性,用户无法自行更改,也无法将自身权利擅自转授给其他用户[5]。

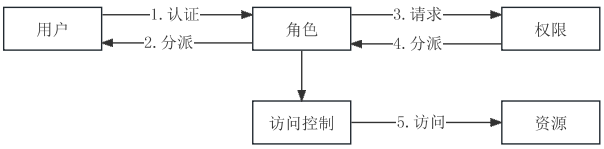

图3 RBAC模型

2.3定期安全审计与漏洞扫描

在确保系统安全性的过程中,定期实施安全审计和全面扫描系统漏洞,同时构建高效的安全事件应急响应机制,是维护系统安全稳定的核心举措。在此过程中,需依据实际情况精心制定详细而全面的安全审计计划,对审计的范围、频率及关键领域进行明确界定。通过集成人工分析与自动化工具,我们将全面审查网络设备、操作系统、应用程序及数据库等,以精准识别未授权访问、弱密码、配置错误等潜在风险。此外,我们应严格依据最新的漏洞信息和行业标准,对系统存在的漏洞进行详尽扫描,并

综合采用端口扫描、服务扫描和漏洞库比对等多种方法，以全面发现系统潜在的安全隐患[6]。当出现安全隐患时，务必在最短时间内启动修复流程，对漏洞的严重程度、影响范围等作出全面客观的评估。在此基础上，精准制定针对性的修复方案并迅速响应，以确保操作的准确性和有效性，同时避免引入新的安全风险。

3 案例分析

2020年，全球范围内突如其来的新冠肺炎疫情对全球公共卫生体系构成了严峻挑战。为了有效遏制疫情的传播，各国政府部门积极行动，借助先进的信息网络技术，构建起高效的疫情防控信息平台，以实现疫情数据的实时监测、精准分析和全球共享。然而，随着数据量的迅猛增长和数据流动速度的加快，数据安全问题也逐渐浮出水面，成为亟待解决的重要议题。

3.1数据安全挑战

在疫情防控的严峻形势下，涉及身份信息、健康状况、行程轨迹等敏感个人数据的安全至关重要。一旦这些信息被非法获取或泄露，个人隐私将受到严重侵害。此外，疫情防控信息平台作为信息汇聚的关键节点，也常成为黑客攻击的目标。若系统受到攻击，疫情数据将面临泄露、篡改或破坏的风险，从而严重影响疫情防控决策的准确性。鉴于国家和地区在数据隐私保护方面的法律法规存在差异，如何在跨境数据流动中确保合规性，成为了公共卫生信息网络数据安全面临的重大挑战。这一问题的解决，不仅关乎个人隐私权的保护，也直接影响到全球疫情防控的协作与成效。

3.2案例分析与应对措施

各国政府和公共卫生机构针对上述挑战，已采取了多项举措来确保信息网络数据的安全。首先，他们运用了先进的加密技术，对敏感数据的存储和传输进行了全面加密，同时实施了严格的访问控制策略，确保在实际操作中只有经过授权的人员才能访问这些数据。其次，通过部署入侵检测系统、安全审计等关键设施，他们能够实时监控网络攻击和数据泄露的风险，并制定应急预案，确保在发生安全事件时能够迅速作出反应并有效处置。最后，他们还加强了与国际组织和其他国家的合作，共同制定了一系列数据隐私保护的标准和规范，同时加强了内部合规性建设，确保疫情防控数据的收集、处理、共享和存储都符合相关法律法规的要求。

4 结语

本文深入探讨了公共卫生信息网络数据安全的保护问题，针对当前公共卫生数据安全管理中面临的数据泄漏、数据篡改及网络攻击等核心风险进行了全面分析。基于数据加密、身份验证、访问控制、定期安全审计及法规遵循等关键策略和技术手段，本文提出了一系列切实可行的应对措施，旨在构建一个既安全又高效的公共卫生信息网络数据保护体系，确保公共卫生数据的完整性和安全性。

[参考文献]

[1]徐战威.网络通信安全中数据加密技术的应用研究[J].通讯世界,2024,31(06):67-69.

[2]贾凯.基于区块链的医疗数字身份管理和数据访问控制研究[D].河北大学,2023.

[3]陈汝婕.社会生态系统视角下突发重大传染病事件医院抗逆力模型构建研究[D].中国人民解放军海军军医大学,2023.

[4]王璨.基于多源数据的厦门市医疗卫生服务设施空间布局与可达性优化研究[D].华侨大学,2023.

[5]宋豪宇.医疗资源配置与布局评价及优化研究[D].江西师范大学,2023.

[6]马莉珍,甄洪雪,刘润友.基于网络大数据监测和百度指数的四川省公共卫生舆情特点分析[J].中国公共卫生管理,2023,39(01):43-46.

作者简介：

张晓卓(1980--),男,汉族,天津市人,本科,天津市医学科学技术信息研究所,研究方向：信息网络安全。