大数据在医院网络安全防御中的应用

周 震
（深圳市第二人民医院，广东 深圳 518037）

摘要：医院因每天需要接待大量患者，各种信息层叠，使得网络承载量较多，网络信息数据更是涵盖了诊断治疗、电子病历 、医学影像、检查检验、财务管理、药房管理以及远程诊疗等。大数据技术的发展为医疗行业带来了革新的契机，但虽然医疗诊断服务水平有所提升，不过还是无法避免木马或病毒的攻击，这些对于医院的网络安全产生了深远影响。基于此，笔者认为医院相关人员要重视网络安全，采取必要的防御措施，抵御可能产生的信息安全。文章首先阐述了网络安全技术，随后对网络安全防御技术的现状进行了分析，最后针对医院网络安全如何防御，提出了四点建议，以此提升医院的网络安全防御水平。

关键词：大数据；医院；网络安全防御；应用

大数据技术的发展，使人们很快进入了信息化社会，而其在医疗领域的应用也更加广泛，如电子病历数据、医学影像数据、实验室检验数据、健康管理数据等，可以说覆盖到了各行各业，这些都促使社会的很多单位开始走向办公自动化、智能化与共享化。但是，随之而来的就是网络系统可能会面临频繁攻击，如蠕虫病毒、勒索病毒以及变异木马等，这些都会影响医院信息系统的正常使用，造成患者信息泄露。部分人员利用大规模互联网漏洞攻击网络，造成网络陷入瘫痪。由于网络和人们的生活融合已经越来越深，网络接入用户量猛增，随着互联网软硬件资源不断增多，网络防御要求也就更高。本文结合大数据背景，对医院网络安全防御现状和大数据在其中发挥的作用、具体应用进行了阐述，希望促使医院的信息化改革更加顺利。

一、网络安全技术分析

（一）信息加密技术

根据当前技术的发展，信息加密技术中最为常见的有对称性与非对称性两种。对称性具有较为显著的反推性，能够在密钥解密过程中进行反推，保证加密处理和解密处理的结果能够保持一致。对称加密技术的应用，可以实现对数据信息的保护，在这方面具有特殊功能，同时还能预防所存储的信息数据被无端篡改，又或是被非法窃取。非对称性在保护网络安全时，最大的特点就是解密加密密码是能够同步出现的，这就形成了共同密钥。信息加密技术包含了私有性和公开性，二者可以互换位置，交换方要以已经生成的密钥为基础，处理私有密钥。

（二）防火墙技术

1. 应用性

该类型的防火墙技术主要是将计算机网络信息安全系统的应用作为了关键，由此延伸开发的一种管理技术。

2. 过滤性

过滤性防火墙技术指的是在数据包中以合理方式应用端口、源地质或是目的地地质等，就此判断数据包是否可以通过原来设定。该技术不需要太多资金，在成本方面可明显节约，并且具有较强的安全性和可靠性，因此拥有海量用户，很多用户在防火墙技术中会优先使用这种。

3. 智能化

智能化防火墙技术也是防火墙技术的一种，其同样已经被广泛渗透于医院的数据信息中。该技术结合实际情况，合理应用统计学以及概率算法等方面的知识，可以进行数据识别，同时计算量与算法更新成正比，会随之进行简化。智能化防火墙技术应用后可以有效减少计算机系统的危险。智能化防火墙技术的优势在于不但可以识别且阻断发现的电脑病毒，而且也可以对一些恶意的数据流量进行调控，使医院系统免收侵害，由此保护医院数据信息的安全，增强安全效果。

（三）身份认证技术

上述我们已经说到，医院系统包含的信息较多，为了进一步保障数据信息的安全，还可以应用身份认证技术，其对于系统的正常运行同样有效。医院网络系统的环境下，设计人员预先根据用户信息设计相关数据，那么系统就可以对对应用户进行识别，而所授权的范围也可以限制在用户的身份范围内。合理应用身份认证技术的关键就是需要保障操作者的数字身份信息要和物理身份信息对应，这也是网络信息防御需要考虑的。

二、医院网络安全防御技术现状

（一）访问控制系统

访问控制系统在医院的网络安全防御中是被广泛使用的技术之一，该技术可以满足医院的特殊化需求，其部署安全访问服务器后，那么服务器就像是医院网络的安全抠，可以根据需求设置黑名单或者是白名单，由此保障医院网络可以顺利运行。访问控制系统还能配置多种防御规则，有很强的灵活性，能够明显提升医院防御水平。访问控制系统还能给管理人员提供操作交互接口，管理者可根据医院的实际需求，设置相关的控制规则，如网络角色、用户信息、操作信息或是用户权限等，这些信息可以当作网络防御的一部分，和现有的其他防御体系结合起来，由此使访问信息具有对比性与匹配度，最后可访问信息加工。应用程序接口的灵活性体现在能采集不同网络传输要求，然后把请求传至请求判断模块，该模块会自动对这些数据信息进行分析和比较，进而得出结论，即数据信息是否在访问控制规则之内，若符合放行，反之就会限制其访问权限。

（二）防病毒系统

杀毒软件系统是与访问控制系统类似，在医院常用的防御手段之一。医院网络信息的日常运行中，很难完全避免木马或是病毒的侵害，如果网络安全不能保障，医院网络往往会采用杀毒软件，旨在查杀木马病毒。随着医疗行业的发展，很多大型企业由此诞生，这些大型企业致力于在 IT 行业发光发热，而且也会设计更先进的杀毒软件，其中融入了脱壳技术、修复技术，这些都能从很大程度上提高系统的脱壳能力，防止非法数据包以更为高深的技术侵入系统，导致数据内容无法保证真实性。

（三）深度包过滤系统

深度包过滤系统可视为访问控制系统的进阶版，这是防御研发企业所推出的一种具有电信特点的防御技术。深度包过滤一般会被布置在医院的局域网与 Internet 之间，基于包过滤路由器配置深度包过滤的安全防御规则。深度包过滤系统可以实现对不同医院网络数据的检查，不但可应用于应用层，同时也涵盖传输层与网络层，最大程度保护患者的信息安全。医院部门繁多，且机制

网络较为复杂，不论是门诊挂号、诊断治疗还是影像拍摄管理等，都部于服务器，没太工作站都能应用网络访问相关服务器。非医院内部访问者在进入医院网站时，就要经过包过滤系统，该系统对相关信息进行检查，且确认达到标准后，才可以进入，这一技术同样可以提高医院网络安全防御能力。

三、大数据在医院网络安全防御中的应用

（一）加强数据管理，保障信息安全

随着大数据技术的发展，我国的信息安全技术也在不断地提高，在建立和健全计算机网络信息系统的同时，为了保证数据的安全性和可靠性，必须加强对医疗机构的信息化管理。首先，要提高医务人员对患者数据的保护意识，防止计算机网络安全信息系统中发生的数据遗失，并采取防范对策。其次，医院要对患者的数据进行实时的备份。目的是防止因医疗机构计算机网络信息系统发生错误而造成信息遗失。通过提前备份重要信息和存储的内容，提高信息和数据的安全级别。以科研教育型医院为例，该类型医院指的是以医院为研究场所，而临床问题为导向，就此展开研究。因其中涉及到了临床，因而包含了大量患者信息，为保障患者信息，该类型医院就可充分利用大数据技术中的数据库脱敏技术。该技术既满足了企业的对内数据保护，同时也符合监管要求，可进一步保障用户的数据信息。

（二）优化病历管理，发挥网络功效

在大数据的支撑下，通过对计算机软件的适当运用，可以将医疗系统中的医疗数据进行集成，并通过云存储的方式来实现对数据的增强。另外，还可以通过访问权限设置来提高数据储存的安全级别。另外，通过对计算机网络中的信息安全技术的适当运用，可以迅速地找到病人的病历，便于工作人员随时掌握病人的真实状况，通过这种方法，可以提高病人对病人的信任度，从而最大限度地提高治疗的疗效。

在这一进程中，必须以大数据为基础建立完善的控制数据库体系，注重运用计算机网络的信息安全性，提高各部门之间的关联性水平，并将各诊疗学科之间的相关信息进行整合，建立基于网格化的信息数据管理模式，以提升管控数据库的使用效率和水平的目的。在此基础上，建立面向云服务的云接入、共享和存储体系。采用计算机网络信息科技，支持资料传送及资料的充分分享。医疗机构要合理地存储档案信息和病案信息等基本数据，在云计算的支撑下查找和下载有关的信息，同时还要解决数据传输的要求，从而达到充分的资源信息共享，为医学系统的诊断和治疗提供支撑。通过建立“电子病历档案云共享平台”来实现对数据和技术数据的高效、规模化和差异化利用。传统的电子病历存储方式，往往要购买很多的硬件储存装置，而通过对大数据和云计算技术的恰当运用，可以将其虚拟地储存起来，既可以节省硬件设施的投资，又可以提高其利用率。

电子病历系统包括如下功能：对医院私有云提供支持的虚拟主机、云储存器以及软件服务 SaaS，提供平台服务的 PaaS 支持，开放基础设施服务 IaaS 支持，以及电子病历云储存与云计算、云共享。在移动云环境下，医疗记录管理采用层次化的结构，其由数据访问层、业务逻辑层和视图三大部分组成。在这种结构下，电子医疗记录使用者可以通过网页和 App 终端访问系统，还可以利用第三方数据库建立访问权利确认机制，对网络的安全接入起到了很大的保证作用。电子医疗档案的查询过程中，用户需要先提出查询申请，然后由系统读取所需资料，再通过相应的解析引擎分析这些资料，将这些资料以 CAS 的形式呈现给使用者。

（三）完善财务系统，创建财务体系

为了适应医院现代化构建的需要，对医院的财务管理进行了信息化改造。根据财务流程划分，我们可以将其分为两个主要的模块：业务财务系统和内部财务系统。医院财务管理的信息化建设要求将两者有机结合在一起。提供相关的数据信息，如业务数据、财务数据、资产数据、病历档案数据等都需要覆盖系统建设，以基于对数据波动的应用，对财务数据进行动态的剖析，起到对财务数据的监督作用，对成本配置、采购数据和资产消耗等各种数据信息进行综合分析，并不定期更具实际需要对财务系统进行更新，使整个财务管理体系的调节效率得到最大程度的发挥。医院可以从财务基础数据平台着手，主动应用云财务办公平台，重构财务规范化工作过程智慧财务信息系统可以建立集成财务管理平台，该平台实现了财务会计模型和其他有关业务模块的集成。医院应用云财务办公平台，建立面向医院、归口部门和各职能部门的三层预算管理工作系统，用全面预算管理来实现对成本的有效控制。

（四）注重界面访问，强化网络控制

访问控制功能的实现支持对访问计算机网络信息系统用户身份与权限进行限制。对于那些要进行互联网接入的用户，必须实施一种身份验证机制，判断他们有没有资格访问网络数据材料，并确定他们对这些资源的特定用途。在计算机网络的信息安全体系中，访问控制技术主要有属性权限控制、网络权限控制、入网访问等不同形式，因此，在医疗机构中，要充分利用这些技术，加强网络接口的访问控制，使存储在网络中的信息资源的安全性得到最大程度的保证。比如，根据医院的具体条件，建立权限管理模式，生成各种形式的医疗信息化系统，并建立相应的资料库文件。通过对医疗信息系统中的主体用户分类和信息资产的识别，建立了对象资源表和主体使用者表格，并对二者的特性进行了详细的说明。在该系统中，以入网访问控制策略作为第一层的安全保障，通过对用户的登录行为和网络资源的利用来实现对用户的接入和定位的控制。按照“用户名识别验证→用户口令识别验证→用户帐户预设权利认证”来实现对用户身份的控制。其中，默认权限要充分考虑到时间和空间等因素的约束作用，保证互联网平台可以对用户的网络登陆地点进行监控，并对接入的用户的终端进行限定，防止存在着角色的权利被滥用或使用的情况。

四、结束语

医院网络安全防御是一项系统性工作，需要管理者对此加强重视。大数据技术的发展极为快速，管理者和设计人员要更新自己的理念，采取先进技术，确保患者信息安全。本文结合目前存下的问题，提出了加强数据管理，保障信息安全；优化病历管理，发挥网络功效；完善财务系统，创建财务体系；注重界面访问，强化网络控制的建议，希望能够加强大数据技术和医院网络安全工作的融合，提高医院的防御水平。

参考文献：

[1] 崔冉 . 计算机网络技术在医院信息化建设和管理中的应用研究 [J]. 科学与信息化，2022（11）：163-165.

[2] 詹振坤 . 医院信息化建设中计算机网络安全管理与维护工作思考 [J]. 无线互联科技，2021，18（10）：25-26.

[3] 缪方宇 . 基于医院的计算机网络信息系统的安全风险思考及控制 [J]. 饮食保健，2021（39）：281-282.

[4] 吕安童 . 信息生态视角下互联网医疗问诊用户满意度影响因素研究 [D]. 郑州：郑州航空工业管理学院，2022.

[5] 程林广 . 医院信息化建设中计算机网络安全管理与维护研究 [J]. 计算机产品与流通，2022（3）：143-145.