

数字图书馆计算机网络安全技术分析

舒明兆

宁波图书馆（宁波少年儿童图书馆） 浙江 宁波 315000

摘要：数字化赋能推动数字图书馆快速普及，依托网络化架构实现海量文献资源共享与智能化服务。但开放的网络环境使其面临网络攻击、数据泄露、系统漏洞及人为操作失误等多重安全风险。本文结合数字图书馆网络运行特点，系统分析各类安全风险成因，阐述防火墙、数据加密、身份认证及智能防护等关键安全技术的应用，并从技术、管理、人员及应急层面提出优化对策，为提升数字图书馆网络安全防护水平提供有效参考。

关键词：数字图书馆；计算机网络；安全技术

引言：互联网与大数据技术的普及，推动数字图书馆快速发展，打破传统图书馆服务时空限制，实现文献资源实时共享与线上智能服务。数字图书馆承载海量文献资源与用户隐私数据，网络运行环境复杂多变。各类网络入侵、数据篡改、非法爬虫窃取等安全问题频发，严重威胁系统稳定与数据安全。基于此，本文分析其网络安全风险与防护技术，制定全方位保障方案，为数字图书馆安全运维提供参考。

1 数字图书馆计算机网络安全概述与风险分析

1.1 数字图书馆网络系统概述

（1）数字图书馆网络架构主要由四大核心模块构成，各模块协同支撑平台稳定运转。资源存储模块是核心载体，负责海量电子文献、期刊、影像等资源的分类存储与备份；用户访问模块面向全网用户，提供检索、阅览、下载等基础服务；数据传输模块承担系统内外、模块间的数据交互工作，保障资源流转通畅；后台管理模块用于管理人员维护系统、管控权限、监控运行状态，是平台运维的核心支撑。（2）其网络运行具备鲜明的数字化特征，一是数据资源海量性，涵盖各类数字化文献资源，数据体量持续动态增长；二是用户访问开放性，面向全社会用户开放，访问群体分散且身份复杂；三是数据传输高频性，日常检索、下载、浏览操作频繁，数据交互流量大；四是资源共享实时性，可实现跨区域、跨终端即时资源共享，大幅提升资源利用率^[1]。

1.2 数字图书馆网络安全的核心内涵

（1）数据安全是核心基础，需全面保障馆藏文献资源、用户注册及浏览隐私数据、平台运营数据的安全，确保数据不被泄露、篡改，维持数据完整性、保密性与正常可用性。（2）系统安全是运行保障，涵盖网络设备、服务器、操作系统及图书馆服务平台，需规避软硬件漏洞、系统故障等问题，保障系统全天候稳定运行，

筑牢基础运行防线。（3）访问安全是管控关键，通过分级分类设置用户访问权限，规范用户操作行为，有效拦截非法访问行为，杜绝越权操作，规避人为访问引发的安全隐患。

1.3 数字图书馆面临的主要网络安全风险

（1）网络攻击风险常态化存在，常见病毒入侵、木马植入、DDoS流量攻击等恶意行为，同时恶意爬虫会批量窃取馆藏资源，造成资源侵权与流失。（2）数据安全风险隐患突出，在数据传输、存储过程中易出现数据泄露、篡改、丢失问题，用户手机号、借阅信息等隐私数据极易被盗用，侵害用户权益。（3）系统漏洞风险难以杜绝，软硬件系统迭代更新不及时、后台程序代码缺陷、长期使用的设备老化等，都会形成安全短板，成为网络入侵的突破口。（4）人为操作风险随机性较强，管理员运维操作失误、普通用户违规访问高危链接、内部人员恶意篡改泄露数据等，均会对网络安全造成直接威胁。

2 数字图书馆核心计算机网络安全技术应用

2.1 防火墙与入侵检测技术

（1）防火墙技术是数字图书馆网络边界防护的基础核心技术，主要部署在图书馆内网与互联网的衔接边界，构建起一道物理与逻辑兼具的安全屏障。该技术可实现内外网络的有效隔离，依据预设的安全策略对进出网络的数据包进行全面筛查，精准拦截端口扫描、非法接入、恶意访问等违规请求，严格管控各类网络数据的进出权限。同时，防火墙可屏蔽内网设备信息与资源架构，避免内部网络结构暴露在公共网络中，有效抵御外部网络的基础性入侵威胁，从网络边界层面筑牢数字图书馆的安全防线，保障内网资源与系统的基础安全^[2]。（2）入侵检测技术属于动态主动防护技术，可弥补防火墙静态防护的局限性，实现全天候网络运行状态监测。该技术能够实时捕捉、分析网络流量与用户操作行为，

精准识别病毒攻击、木马植入、越权访问、异常数据传输等各类恶意入侵行为。当检测到高危风险操作时,系统可自动触发预警机制,通过后台提示、消息推送等方式告知运维人员,同时可自主拦截异常访问、阻断攻击链路,快速遏制风险扩散,有效提升数字图书馆网络系统对突发攻击行为的应对能力,形成边界防护后的二次安全保障。

2.2 数据加密与备份恢复技术

(1) 数据加密技术是保障数字图书馆数据安全的核心手段,主要针对馆藏核心文献资源、用户隐私信息、平台运营数据等关键数据进行加密防护。目前主流应用对称加密与非对称加密两种核心算法,适配不同类型数据的防护需求。其中对称加密运算速度快、效率高,适用于海量文献资源的批量加密处理,保障资源传输与存储安全;非对称加密安全性更高,多用于用户手机号、身份信息、借阅记录等隐私数据的加密防护。通过加密处理,可将原始数据转化为不可直接读取的密文,即便数据出现泄露情况,非法人员也无法破解获取有效信息,从根源上规避数据泄密、篡改风险。(2) 数据备份与恢复技术是应对数据丢失、损坏的兜底防护手段,是数字图书馆数据长效安全的重要保障。当前数字图书馆普遍搭建增量备份与异地备份相结合的双重备份机制,增量备份可定期更新新增、修改的文献与用户数据,减少备份冗余、提升备份效率;异地备份将核心数据同步存储至异地服务器,规避本地设备故障、自然灾害、网络攻击导致的全盘数据丢失问题。当出现数据误删、恶意篡改、资源损坏等问题时,运维人员可依托备份数据快速完成数据还原,最大限度降低数据安全事故带来的损失,保障馆藏资源的完整性与连续性^[3]。

2.3 权限访问与身份认证技术

(1) 身份认证技术是杜绝非法用户接入、保障访问安全的第一道关卡,能够有效验证登录用户的真实身份。数字图书馆结合运营需求,采用多重身份认证方式,基础的账号密码认证适配普通用户日常登录,操作便捷、适配性强;短信验证、人脸识别等进阶认证方式,可有效防范账号被盗、密码破解等问题。多重认证模式相互配合,能够精准甄别合法用户与非法访问人员,杜绝匿名登录、盗号登录等违规行为,从源头规避非法用户入侵系统、窃取资源与数据的安全风险。(2) 权限分级管理技术以身份认证为基础,实现对用户操作行为的精细化管控。该技术按照用户身份、岗位职责与使用需求,将系统访问权限划分为普通用户、运维管理员、超级管理员等多个层级。普通用户仅拥有资源检索、阅览、下载等基础权限,无法操作

系统后台与核心数据;运维管理员具备日常运维、数据审核权限;超级管理员拥有最高操作权限。通过分级授权、权责划分,可有效管控各类人员的操作范围,杜绝越权查询、篡改、删除数据等违规操作,规避内部操作引发的安全隐患。

2.4 网络安全防护新技术应用

(1) 云安全技术是适配云端数字化建设的新型防护技术,契合当下数字图书馆云端资源存储、共享与传输的运行模式。该技术依托云端安全平台,可对云端存储的海量文献资源、用户数据进行动态化防护,实时监测云端数据传输、存储、调用过程中的异常风险。同时云安全技术具备集群防护、动态防御优势,能够统一拦截云端恶意攻击、非法爬虫、数据异常流转等风险,解决传统防护技术适配性不足的问题,全面保障云端数字图书馆的资源与数据安全。(2) 人工智能安全技术依托智能算法与大数据分析能力,实现网络安全防护的智能化升级。该技术可自主学习数字图书馆网络运行的正常数据模型,快速识别非常规访问、高频攻击、漏洞隐患等风险问题,实现全天候智能风险识别与自动拦截。同时能够自主检测系统软硬件漏洞、程序缺陷,并完成简易漏洞的智能修复,减少人工运维压力。相较于传统被动防护模式,人工智能安全技术可提前预判潜在风险,实现主动防御,大幅提升数字图书馆网络安全防护的智能化、精准化水平。

3 数字图书馆计算机网络安全优化策略与保障措施

3.1 技术层面优化策略

(1) 升级安全防护体系是提升网络基础防御能力的关键举措。数字图书馆需建立常态化设备与系统更新机制,定期升级防火墙、入侵检测系统等核心防护设备的程序版本与安全策略,适配新型网络攻击特征。同时持续排查服务器、网络设备、业务平台的软硬件漏洞,及时完成补丁修复,弥补传统防护体系的滞后性问题,避免老旧设备和系统漏洞成为网络入侵突破口,构建动态更新的基础安全防护体系。(2) 优化数据防护机制可实现数据全生命周期安全管控。针对数据存储、传输、使用、备份全流程完善加密体系,结合对称与非对称加密算法,对馆藏资源、用户隐私数据进行分层加密保护。同时优化数据备份方案,合理调整增量备份、全量备份的频次,优化本地与异地结合的存储方式,规避数据丢失、篡改、损坏等风险,全面提升数据存储的稳定性与安全性^[4]。(3) 引入智能防护技术推动安全防御由被动转为主动。积极落地人工智能、大数据风控技术,依托大数据分析用户访问行为、网络流量数据,精准识别异

常访问、恶意爬虫、高频攻击等风险。利用AI智能检测系统漏洞、预判潜在安全隐患,实现风险自动预警、自主拦截,有效弥补传统防护技术响应滞后的问题,大幅提升网络安全主动防御与精准防控能力。

3.2 管理层面保障措施

(1)完善安全管理制度是网络安全规范化运行的制度基础。结合数字图书馆网络运行特点,制定完善的网络设备运维、数据安全、用户权限管控、网络攻击防控等标准化制度,明确各项工作的执行标准与规范流程。通过制度化约束,杜绝管理混乱、操作随意等问题,为网络安全运维工作提供清晰的制度依据,实现安全管理标准化、规范化。(2)建立常态化巡检机制,实现风险早发现、早处置。安排专职运维人员定期开展全方位网络安全巡检,重点排查系统漏洞、设备运行故障、数据传输异常等问题,定期完成整体网络安全风险评估。对巡检发现的隐患分类登记、限时整改,形成巡检、排查、整改、复查的闭环管理模式,从源头降低网络安全事故发生概率^[5]。(3)规范人员操作流程,强化内部安全管控。细化管理员、运维人员、在岗工作人员的岗位职责与操作规范,明确系统运维、数据操作、权限管理等工作的操作流程与禁忌事项。严格约束内部人员操作行为,杜绝越权操作、违规运维、私自调取数据等行为,减少内部人为操作引发的安全风险。

3.3 人员层面提升策略

(1)开展常态化安全技能培训,提升专业人员防控能力。定期组织技术运维人员参与网络安全专项培训,学习新型网络攻击手段、前沿安全防护技术、漏洞修复方法及应急攻防应对技巧,更新专业知识储备,提升工作人员应对复杂网络安全问题的实操能力,打造专业化安全运维团队。(2)强化全员网络安全意识,降低人为安全隐患。面向图书馆全体工作人员开展安全科普教育,普及日常运维、数据管理中的安全注意事项;同时面向广大用户推送网络安全知识,引导用户规范访问、合规操作,杜绝违规下载、恶意入侵等行为,全方位减少人为因素带来的网络安全风险。

3.4 应急保障体系建设

(1)制定专项安全应急预案,明确突发风险处置规范。针对网络攻击、数据泄露、系统瘫痪、资源丢失等各类突发安全事件,结合数字图书馆运行实际制定细化应急预案,明确不同事故的处置流程、防控重点、责任分工,为突发事件处置提供标准化指导。(2)建立高效应急处置机制,提升突发事件响应速度。组建专属网络安全应急处置小组,明确成员分工与岗位职责,建立快速响应机制。一旦发生安全突发事件,小组可第一时间介入处置,快速阻断风险、控制事态,最大限度降低安全事故对系统运行、数据资源的损害。(3)定期开展应急演练,夯实实战处置能力。定期模拟数据泄露、DDoS攻击、系统故障等常见安全场景开展应急演练,让工作人员熟练掌握应急处置流程与操作技巧,积累实战经验,有效提升团队协作与突发风险应对能力,完善整体应急保障体系。

结束语

数字图书馆网络安全建设是数字化文化服务高质量发展的重要保障,关乎馆藏资源完整性与用户信息安全。本文全面梳理数字图书馆网络安全风险,详解各类网络安全防护技术的应用价值,从多维度制定安全优化与保障策略。网络安全防护并非一成不变,后续需紧跟网络技术的发展趋势,持续迭代防护手段、完善管理机制,全面提升风险防控能力,推动数字图书馆安全、稳定、智能化可持续发展。

参考文献

- [1]望宇.数字图书馆网络安全防护策略[J].辽宁师专学报(自然科学版),2024,26(3):31-34.
- [2]刘海泳.智慧校园的网络安全防护体系构建与研究[J].网络空间安全,2024,15(4):280-283.
- [3]车盈.图书馆网络信息安全防护研究[J].电子产品可靠性与环境试验,2022,40(6):114-116.
- [4]张赛男.高校图书馆网络安全管理策略研究[J].图书馆学刊,2024,42(8):95-99.
- [5]宋亭.数字图书馆的计算机网络安全与防护[J].现代信息科技,2023,3(21):147-149.