基于大数据技术的计算机网络安全问题分析

王斌
广州工商学院，广东 广州 510000

DOI: 10.61369/TACS.2026090046

摘　　要： 随着大数据、云计算、人工智能等数字技术的深度融合普及，计算机网络的普及率越来越广泛，这使得网络传输结构愈发复杂，数据交互频次持续提升。传统网络安全防护体系已难以适配大数据环境下多元化、隐蔽化、动态化的网络安全风险。基于此，本文基于大数据技术视角，深入探讨计算机网络安全问题与防护路径，以期为新时代计算机网络安全建设提供理论参考。

关 键 词： 大数据技术；计算机；信息化；网络安全；防护

Analysis of Computer Network Security Problems Based on Big Data Technology

Wang Bin
Guangzhou College of Technology and Business, Guangzhou, Guangdong 510000

Abstract: With the in-depth integration and popularization of digital technologies such as big data, cloud computing and artificial intelligence, computer networks have gained increasingly wide application, which leads to more complex network transmission structures and continuous growth of data interaction frequency. Traditional network security protection systems can hardly adapt to the diversified, concealed and dynamic network security risks under big-data environment. From the perspective of big-data technology, this paper deeply discusses computer network security problems and corresponding protection paths, so as to provide theoretical references for the construction of computer network security in the new era.

Keywords: big data technology; computer; informatization; network security; protection

引言

在数字信息化高速发展的时代背景下，大数据技术凭借高效的数据采集、存储、挖掘与分析能力，全面渗透于各行各业的计算机网络运行体系之中，推动计算机网络朝着规模化、复杂化、智能化方向快速发展。大数据架构下的网络安全风险更具隐蔽性、动态性与扩散性，这不仅极大地增加了计算机网络的安全运行压力，同时各类网络攻击手段不断迭代升级，病毒入侵、非法访问、数据窃取、网络漏洞攻击等各种各样的安全隐患层出不穷，对网络系统的稳定运行、用户的数据隐私以及行业信息安全，构成严重的威胁。探索科学有效的网络安全防护策略，有助于完善新时代计算机网络安全防护体系，提升网络安全风险抵御与应急处置能力。

一、大数据技术下计算机网络的主要特征

（一）网络数据体量海量化，具有风险覆盖面广特征

大数据技术的快速发展，使得计算机网络数据生成具备不间断、规模化、爆发式的运行特点，网络数据存量、实时流量、交互频次均处于持续高位运行状态。海量化的数据运行特征，彻底重构了计算机网络的承载边界与运行逻辑，进而推动计算机网络从传统轻量化数据处理模式转向海量数据集约化处理模式[1]。另外，海量数据的持续流转使得网络资源利用率长期处于高位，网络链路、服务器节点、存储设备长期承载高负荷数据运算与传输任务，导致计算机网络数据安全边界被拓宽，推动网络安全体系从封闭稳态向开放动态全面转型，从而提升整个数据生态安全风险。

（二）安全隐患动态实时化，具有隐蔽性特征

大数据网络具备高速实时的数据传输与动态交互能力，海量数据不间断上传、流转、更新、交互，网络链路、终端节点、数据状态、访问行为时刻处于动态变化之中，对应的安全隐患也随之实时生成、快速演变、高频迭代。网络异常访问、数据篡改、

本文受广州工商学院校级质量工程（校外实践教学基地）项目（项目编号：XWSJJXJD2024001）资助。

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

链路漏洞、恶意入侵等各类安全隐患容易快速扩散[2]。同时，高频动态的网络运行模式使得安全隐患具备突发性、瞬时性、随机性的特点，安全状态随时发生波动，无固定演变规律，这进一步增大了计算机网络安全防护难度。

（三）计算机网络实现动态交互，具有数据传播速度快特征

大数据技术赋能下的计算机网络具备高速化、实时化、动态化的传输交互特征，可以实现网络数据的高速传输与实时交互，推动网络数据迭代速度大幅提升，数据流转的实时性、高效性达到全新层级[3]。

一方面，大数据场景下的计算机网络始终处于动态流转、持续更新的运行状态，网络数据内容、数据体量、传输链路、交互节点随时处于动态变化之中。这使得网络数据能够快速完成采集、传输、解析、应用的全流程闭环，进而提升网络数据资源的利用效率。另一方面，高频动态的数据交互使得网络链路始终处于高活跃运行状态，网络节点、传输通道、算力资源的负载状态实时波动，网络运行的动态性、不确定性显著提升。

二、传统计算机网络安全防护存在的问题

（一）安全防护具有滞后性

传统计算机网络安全防护具备极强的滞后性与补救性，无法实现对潜在风险、隐性漏洞、未知攻击的提前识别与预先阻断，整体安全运行高度依赖网络环境的固有稳定性。具体而言，传统网络安全认知普遍将安全防护界定为对已发生攻击、病毒入侵、数据泄露、网络异常等风险事件的拦截与修复，将工作重心放在漏洞修补、故障处理、攻击阻断与损失挽回层面，尚未形成全周期、全过程、常态化的安全防控思维[4]。

（二）防护技术体系单一固化

传统防护技术主要依托固定防火墙、常规杀毒程序、静态访问控制、固定密钥加密等基础技术模块构建防护体系，技术运行规则、识别标准、拦截逻辑均为预设固定模式，不具备动态调整、自主学习、智能研判的技术能力。比如，传统技术体系仅能够识别特征明确、模式固定的已知网络风险，对于变异型网络攻击、隐性渗透行为、复合型网络漏洞、未知风险威胁缺乏有效的识别能力与拦截手段。同时，传统防护技术模块之间相互独立、联动性弱、数据互通性差，难以适配复杂多变的现代化网络运行场景[5]。

（三）风险响应机制呈现静态化

传统网络安全监测多采用定时扫描、周期检测的工作模式，无法实现网络数据、网络链路、终端运行状态的全域实时监控，网络运行过程中的瞬时异常、隐性波动、细微漏洞难以被及时捕捉与识别。在风险处置环节，传统响应机制流程固化、环节烦琐、自主性差，从风险识别、信息上报、人工研判到处置落地需要多层流程推进，响应延时较长，无法实现瞬时预警、快速阻断、即时修复。

（四）安全管控机制碎片化

传统网络安全管理模式呈现分区化、模块化、阶段性的管控特征，网络设备、数据终端、传输链路、存储系统等不同环节的安全管控相互独立，各环节管控标准不统一、数据不互通、机制不联动，形成多处安全管控壁垒[6]。同时，传统网络安全管控多依托人工运维、人工核查、人工处置的模式开展，自动化、智能化、系统化的管控机制缺失，人工管控存在主观性强、覆盖面窄、持续性弱、容错率低的固有短板。

三、基于大数据技术的计算机网络安全防护措施

（一）构建智能防护体系，实现主动预判式安全防御

随着大数据时代的逐步到来，计算机网络安全所要面对的环境也变得愈发复杂。而换一个角度来讲，如果能够搭建起一套适配大数据动态网络架构，兼具自适应、智能化、主动式特征的防护体系，就可以进一步做到对网络安全风险的前置预判、动态拦截以及自主适配防护。

一方面，建立依托网络全时序运行数据的动态建模机制。简单来说，就是对网络流量特征、数据流转规律、终端访问行为以及系统运行状态开展持续的监测与管理，在此基础之上搭建出一套适配大数据网络动态迭代特征的专属安全防护模型。而后，可以结合当下网络运行负荷、数据交互节奏以及访问行为的动态变化，自主灵活地调整防护阈值、筛查精度与防御策略，这样一来就可以让防护机制和网络实时的运行状态做到精准适配、实时匹配[7]。

另一方面，对整个网络的运行态势开展持续性、全方位的全景监测。在此基础上，把海量的历史数据和当下产生的实时数据放到一起开展关联聚类分析，这样便能够精准捕捉到网络异常趋势、隐性行为偏差以及各类潜在的风险征兆，从而做到对安全风险的前置识别，并且在风险刚出现萌芽的时候就及时开展干预处置。

（二）加强数据访问控制，规范多端访问秩序

首先，系统需要持续采集网络访问主体的身份属性信息、终端设备运行状态、网络接入场景特征、地理位置信息、访问时段规律、历史操作轨迹、业务操作习惯等多维度的基础数据。在此基础上，完成访问权限的精准匹配、动态调整以及自适应管控，进而从根源上杜绝由权限过度分配、固定授权、交叉授权所带来的各类安全漏洞[8]。

其次，系统需要对全域范围内所有的网络接入终端、访问主体、访问路径以及各类操作行为开展全天候的动态审计工作。在此基础之上，借助大数据行为比对技术，就可以精准识别出越权访问、匿名接入、异常操作、权限溢出等各类违规行为，进而做到对异常访问行为的实时拦截、即时预警，并且完成后续的行为溯源工作。

最后，建立权限动态迭代与自动回收机制，可以依据用户岗位发生变动、设备运行状态产生变更、或是相关业务场景已经结束这些条件，自动对访问权限做出调整、缩减乃至回收处理，这样一来就能够从根源上化解传统模式下权限长期滞留、过期失效以及管控滞后等一系列问题。

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

（三）完善数据全周期安全机制，强化数据精准防护能力

计算机网络数据具有海量化、异构化、弥散化、高隐蔽风险的特征，会对不同阶段数据传播造成影响，因此建立数据全生命周期的闭环数据安全防护机制具有重要作用[9]。

在数据采集阶段，明确网络数据接入的格式规范、字段标准、合规阈值、数据来源准入范围，对所有拟接入网络平台的外部数据、终端交互数据、系统生成数据进行前置准入校验，严格界定合法数据、可疑数据与违规数据的准入边界。与此同时，对识别出的冗余数据直接批量剔除整合，对噪声数据进行标准化修正与格式规整，对高危异常数据、畸形数据、风险数据执行拦截隔离。

在数据传输阶段，搭建分层加密传输架构，对传输链路进行层级划分。比如，对普通公开数据采用基础协议加密传输，对一般涉密数据采用中层混合加密传输，对核心敏感数据采用深度高强度加密传输[10]。

在数据储存阶段，依据数据敏感程度、应用价值、涉密级别、使用场景将全网数据划分为公开级、普通级、内部级、机密级、核心绝密级五个层级，实现不同等级、不同类型数据的物理分区、逻辑隔离存储，杜绝高低风险数据、涉密与公开数据混杂存放，这样可以全程阻断跨数据关联泄露、越权访问、批量窃取等存储安全风险。

在数据运算与共享阶段，可以定期对数据运算行为、共享行为、访问行为进行后台审计研判，及时识别越权调用、异常访问、违规共享、批量导出等风险行为，实现数据运算与共享环节的可追溯、可审计、可管控。

（四）建立完善的网络安全管理体系，提升网络安全防护效度

大数据时代，网络攻击手段不断升级和变化，建立完善的网络安全管理机制可以快速检测和响应网络攻击事件，最大程度上降低网络攻击对系统的危害。

在智能研判层面，全面归集网络运行过程中的传统攻击样本、新型智能攻击特征、漏洞变异数据、隐性异常行为轨迹、复合型风险日志及各类隐蔽隐患数据，统一数据标注标准与样本分类规范，提升未知风险与新型风险的防控精度。

在预警处置层面，将全网安全风险划分为低危、中危、高危、紧急四级风险类别。比如针对低危风险开展后台静默记录与趋势监测，针对中危风险触发弹窗预警、行为提示与局部管控，针对高危风险启动实时告警、链路限流、权限冻结，针对紧急风险执行强制阻断、设备隔离、系统防护预案。

在全域协同层面，打通各类安全防护设备、监测系统、管理平台的数据接口与联动机制，实现前端感知设备、后台分析系统、终端防护模块、应急处置平台的全域数据同源，全面提升网络整体安全防御的协同性与整体性。

四、结语

综上，通过构建智能防护体系、加强数据访问控制、完善数据全周期安全机制、建立完善的网络安全管理体系等策略，可以使得计算机网络安全防护转向智能化预判、精细化治理、全域化防控的现代化治理模式，持续推动网络安全技术、管理制度与防控体系迭代升级，有效抵御各类新型网络安全风险。

参考文献

[1]. 李亮 . 大数据技术在计算机网络信息安全管理中的应用 [J]. 集成电路应用 , 2025, 42 (4): 130-131.

[2]. 王红岩 . 大数据技术的计算机网络信息安全防护对策 [J]. 中国宽带 , 2025, 21 (3): 52-54.

[3]. 侯英杰 . 大数据技术在计算机网络安全中的应用策略 [J]. 通讯世界 , 2024, 31 (11): 34-36.

[4]. 罗明挽 . 大数据技术在计算机网络信息安全防御系统中的应用 [J]. 信息与电脑 (理论版), 2024, 36 (19): 160-162.

[5]. 朱昊 . 大数据时代计算机网络技术的信息安全问题及其防范策略分析 [J]. 信息记录材料 , 2024, 25 (9): 43-45.

[6]. 张凌飞 . 基于大数据技术的计算机网络信息安全防护策略分析 [J]. 电子技术 , 2024, 53 (5): 184-185.

[7]. 孙瑜 . 基于大数据及人工智能技术的计算机网络安全防御系统设计分析 [J]. 网络安全和信息化 , 2024, (2): 143-145.

[8]. 董永杰 . 基于大数据技术的计算机网络信息安全策略分析 [J]. 电子技术 , 2024, 53 (1): 61-63.

[9]. 胡贤 , 霍怡雨 . 基于大数据技术的计算机网络信息安全防护对策分析 [J]. 电子技术 , 2024, 53 (1): 390-392.

[10]. 徐楚原 . 大数据及人工智能技术的计算机网络安全防御系统设计分析 [J]. 数字技术与应用 , 2023, 41 (7): 216-218.

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License