大数据技术在计算机网络安全中的应用策略探究

朱春燕[1] 蒲 海[2]

（1. 苏州托普信息职业技术学院，江苏 苏州 215300；

2. 中船奥蓝托无锡软件技术有限公司，江苏 无锡 214000）

摘要：在大数据技术发展背景下，数据量呈现出井喷式增长趋势，使得传统网络安全措施显得力不从心。大数据技术能够高效收集存储与分析海量数据，系统掌握网络的安全态势，进而制定出更为精准的管理策略。将大数据技术应用于计算机网络安全工作具有重要意义，本文针对相关应用展开研究，分析其应用价值，指出存在的问题，提出相应的应用策略，旨在为提升计算机网络安全防护水平，充分发挥大数据技术在网络安全领域的作用提供理论参考与实践指导。

关键词：大数据技术；计算机网络安全；应用策略

引言：

在信息技术迅速发展的当下，计算机网络已深度融入社会生活的各个层面，所产生的数据量呈指数级增长，使其面临着愈加严重的挑战。传统网络安全防护手段在应对新型、复杂的安全威胁时，逐渐显露出局限性。大数据技术的引进，能够为计算机网络安全提供有力支持，对海量网络数据进行深度挖掘和实时监测，有效识别潜在的安全威胁，及时采取应对措施，在计算机网络安全领域展现出巨大的应用潜力。深入研究其应用，对保障网络完全稳定运行等具有重要现实意义。

一、大数据技术在计算机网络安全中的应用价值

（一）有助于提升网络安全监测全面性

大数据技术的应用有助于实现对网络安全监测的全面覆盖，应用分布式计算框架和数据采集工具，实时收集网络中的各类数据，将其实时传送至大数据分析平台，进行快速处理和分析。比如利用流量计算技术对网络流量数据进行实时监测，发现流量异动时能够及时发出警报，促使安全人员能够及时察觉潜在攻击，对网络中的各个节点和各类型数据进行全面采集和分析，实现对网络安全监测的全方位覆盖。

（二）有助于精准识别网络安全威胁

大数据技术有着强大的数据挖掘和分析能力，通过建立复杂数据分析模型和机器学习算法，对海量数据进行深度挖掘，进而提炼出有价值信息，识别网络安全威胁。大数据可以学习正常的网络行为模式和用户操作习惯，并以此为基准判断行为模式，及时发现异常行为，精准识别与正常模式偏差较大的行为。大数据技术能够分析已有的网络安全威胁案例，总结出攻击特征和规律，当新的数据中出现类似特征时，能够准确识别出潜在的安全威胁类型，为后续的应对措施提供精准依据。

（三）有助于完善网络安全防御体系

大数据技术的应用为完善网络安全防御体系提供了有力支持，通过分析大量网络安全数据发现现有防御体系的薄弱环节，以不断完善与优化防御体系。该技术能够根据不同安全威胁类型和风险等级制定差异化防御策略，针对高风险行为能够采取立即阻断和隔离等措施，针对风险相对较低的行为能够继续监测和分析。大数据能够与其他网络安全技术形成协同整体，实现多种安全技术的合作工作，共同提升网络安全防御能力。

二、大数据技术在计算机网络安全中的应用问题

（一）数据收集安全问题

在大数据技术应用过程中需要对海量数据信息进行收集，这一过程往往面临着诸多风险。收集渠道较为广泛，包括网络设备、用户终端和各类应用程序等，信息数据来源不一，容易收集恶意数据，比如黑客恶意伪造的数据、虚假信息等，导致信息收集不够全面，收集效率低下，对后续的分析和判断形成干扰。例如，在某平台进行用户行为数据收集时，黑客通过分布式拒绝服务（DDoS）攻击，向数据收集服务器发送大量虚假请求，导致服务器资源耗尽，攻击高峰期正常数据收集量下降了 70%，大量有价值的用户行为数据丢失，

（二）数据存储安全问题

数据存储是大数据技术应用的关键环节，随着数据量的不断增长，其安全隐患问题逐渐凸显。在存储过程中，大量数据集中于数据库或存储设备，对存储条件提出了更高的要求，需要可靠且具有可拓展性的系统，如果出现硬盘故障、存储设备老化等，可能导致数据丢失或损坏。以某云存储服务提供商为例，曾因权限管理漏洞被黑客入侵，黑客利用了存储系统中弱密码策略以及权限分配不合理的漏洞，在短短 24 小时内，访问了超过 500 万条用户数据记录。

（三）数据安全管理问题

在大数据时代下，数据量庞大且来源复杂，给数据安全管理带来较大考验。数据管理涉及流程、技术等多个方面，其中流程管理如果出现数据访问权限管理混乱，部分员工获得超出工作需要的过高权限，则会给数据泄露埋下隐患；数据安全审计机制不够完善时，则难以及时追求和记录数据操作行为，导致违规行为难以及时发现。以某金融机构为例，由于内部数据管理流程不完善，在半年内共检测到 52 起异常访问记录，涉及 3000 多名客户的金融信息。

三、大数据技术在计算机网络安全中的应用策略

（一）完善网络安全管理制度，强化计算机网络系统监督

网络安全管理工作是保障计算机网络安全的重要工作，应注重完善相关管理制度，加强对系统的监督管理，从多方面入手加强管理。第一，完善人员管理。明确相关人员的网络安全职责，细化其职责范围；定期开展网络安全培训与教育活动，讲解最新网络安全法规、常见的攻击手段等知识，提升工作人员的安全意识和应急处理能力；及时更新相关管理人员的网络权限，清除离职人员权限。第二，加强访问控制。根据员工工作职责和任务需求，设置相应的网络访问权限；采用多因素身份认证方式，采用基于角色的访问控制（RBAC）策略，根据不同的数据收集任务和人员职责，精确分配访问权限，限制非法访问，防止非法用户冒用身份获取网络访问权限。利用 SSL/TLS 等加密协议，对数据在传输过程中的每一个数据包进行加密处理，确保数据在网络传输时，即使被黑客截获，也无法轻易解析出其中的内容，保障数据的完整性和保密性。第三，加强数据管理。制定数据分类分级标准，根据数据的敏感程度和重要性进行分类，如分为公开数据、内部数据、敏感数据等；针对不同级别的数据，采取不同强度的

加密措施，确保数据在存储和传输过程中的安全性；建立数据生命周期管理流程，对数据传输过程进行加密，防止数据在各个环节出现安全问题。第四，强化系统维护。建立系统巡检机制，按照规定时间间隔对网络设备、服务器等进行全面检查，及时发现并处理故障问题；制定系统学习计划，及时安装操作系统、应用软件和安全软件的补丁。第五，加强监督审计。实时监控网络流量、用户行为等，及时发现异常情况；建立健全网络安全审计制度，详细记录用户对网络资源的访问操作、系统运行状态等信息；分析总结审计结果，及时发现问题并进行调整和完善。

（二）引进先进存储管理技术，确保大数据信息存储安全

数据存储是计算机网络安全中的重要环境，应注重应用先进存储管理技术，保证大数据的信息存储安全。首先，引进分布式存储技术。分布式存储技术能够通过网络将数据分散存储在多个独立的存储节点上，形成一个虚拟的存储资源池。以 Ceph 分布式存储系统为例，其借助分布式哈希表等技术进行数据存储管理，提高数据的可用性和可靠性，保证业务的连续性，满足大数据时代海量数据存储需求。其次，对存储的数据进行高强度加密处理。数据在存储过程中可能会出现被窃取、篡改等情况，应采用高强度的加密算法对其进行管理。例如，使用 AES（高级加密标准）算法对敏感数据进行加密后再存储，确保数据在存储设备上处于加密状态，即使存储设备丢失或被盗，数据也难以被破解。再比如针对金融领域中客户的账户信息、交易记录等敏感数据进行加密处理，使其即便被非法获取，也无法解密密钥获得其内容。此外，还可建立定期备份机制，避免数据因硬件故障、软件错误、人为误操作或自然灾害等原因丢失。比如针对重要业务数据，每天进行一次全量备份，每周进行一次增量备份；选择合适的备份存储介质，如磁带库、专用备份存储设备等；定期对备份数据进行恢复测试，确保备份数据的可用性和完整性。最后，监控和审计工具。利用监控和审计工具实时监测存储系统的运行状态，发现异常情况时应及时发出警报。审计工具详细记录所有数据访问操作，包括访问时间、访问内容等，能够在出现安全问题时追溯操作过程，查明原因和职责，为大数据应用和发展提供支持。

（三）细化大数据技术应用标准，发挥网络安全保障作用

在应用大数据技术过程中，应注重细化相关应用标准，切实发挥其网络安全保障作用。第一，明确数据采集规范。明确出数据采集的范围，哪些数据与网络安全相关等，比如针对企业网络安全监测，可采集网络流量数据、用户登录信息、系统操作日志等关键数据。明确数据采集频率，根据不同数据变化频率设置相应的采集周期，比如针对实时性要求高的网络流量数据，可采用秒级采集等。第二，统一数据处理和分析流程。确定数据处理的具体过程，包括数据清洗、转换、整合等，去除数据中的噪声和错误，将不同格式的数据转换为统一格式，便于后续分析。规定采用的分析模型和算法，根据不同的安全分析目标，选择合适的算法，关联分析算法挖掘数据之间的潜在关系。第三，建立统一的数据格式和接口标准。不同的网络安全设备和系统可能产生格式各异的数据，给数据整合分析带来困难。因此，应建立统一的数据格式标准和接口标准，确保不同来源的数据能够无缝对接和共享，使大数据分析平台能够方便地获取和处理来自各个数据源的数据，提高数据处理效率和安全性。

（四）加强计算机网络安全防御，促进大数据和人工智能技术应用

大数据技术和人工智能技术的应用能够强化计算机网络安全防御，实现系统运行效率的整体提升，全面落实安全防御工作。其中，大数据在海量数据方面具有优势，能够建立庞大的网络行为数据模型，准确识别出异常的网络访问行为、数据传输模式等，进而实现对网络攻击的精准预警。比如可对网络日志进行深度分析，快速发现恶意软件的传播路径、攻击手段以及潜在的安全漏洞。人工智能在计算机网络安全防御方面具有智能决策特征，其中机器学习算法能够自动学习正常的网络行为模式，能够对异常行为迅速发出警报。深度学习技术能够深度分析和准确识别复杂的网络攻击，即便是新型的、未知的攻击手段，也能够通过学习和推理做出有效判断。比如在入侵检测系统中，人工智能技术可以实时监测网络流量，提高对入侵的检测速度，自动采取反制措施，如封锁攻击者的 IP 地址、调整网络配置等，减轻攻击造成的损害。大数据技术和人工智能技术的结合，能够构建出更加智能、高效的计算机网络安全防御体系，提升安全防御能力，有效应对日益复杂多变的网络安全威胁。

（五）加大技术创新力度，拓展大数据技术应用途径

在大数据时代，网络安全形势复杂多变，应加大技术创新力度，拓展大数据技术应用途径。首先，创新计算机网络安全管理技术。应注重引进人工智能和机器学习技术，更新网络安全管理模式，对网络流量进行实时智能分析，有效识别潜在威胁。注重研发自动化的安全策略部署技术，根据网络环境和安全威胁的动态变化，自动调整和优化安全策略。相关人员应开展研发创新工作，运用先进经验和理论知识提升自身创新能力，助力网络安全技术不断优化。其次，利用数据信息挖掘技术。借助数据挖掘技术，对海量的网络数据进行深度剖析，从网络日志、用户行为数据、系统配置数据等挖掘出隐藏的安全问题线索。比如通过关联分析，找出不同数据之间的潜在联系，发现攻击者的行为模式和攻击路径，从而提前采取防范措施；针对挖掘出的安全漏洞，运用大数据分析技术评估其风险等级，确定修复的优先级，制定相应的修复计划，确保有限的安全资源得到高效利用。最后，处理和解决安全问题。注重建立安全问题快速响应机制，出现安全问题时应立即启动相应的应急处理流程，比如利用大数据技术整合安全资源，协调防火墙、入侵检测系统、加密设备等各类安全工具，形成协同防御体系；结合大数据分析结果，总结安全问题发生的规律和特点，为后续的安全防护提供经验参考。

结语

综上所述，当下计算机网络已渗透于社会各行业领域，在提供便利的同时也带来了信息安全风险。大数据技术在计算机网络安全方面有着不可忽视的应用价值，能够完善网络安全防御系统功能，维护网络数据安全。在实际应用中，可通过完善网络安全管理制度、引进先进存储管理技术、细化应用标准以及加大技术创新力度等，切实发挥大数据的网络安全保障作用。在后续应用中，应注重构建出更加智能高效的计算机网络安全防护体系，为数字经济发展筑牢坚实的安全防线。

参考文献：

[1] 闫军 . 基于大数据技术的计算机网络安全策略分析 [J].2024(5):220-221.

[2] 白玉芹 . 大数据与计算机网络安全技术的运用策略分析 [J]. 电子技术 , 2024(7).

[3] 李向阳 , 赵汉卿 , 王丽婧 . 大数据在计算机网络安全防范中的应用分析 [J]. 网络安全技术与应用 , 2023(2).