基于大数据及人工智能技术的计算机网络安全防御系统研究

万 震

（江西省天然气集团有限公司，南昌 330000）

摘 要：随着信息技术的迅速发展，计算机网络安全问题日益严重，网络攻击、数据泄露等安全事件给个人隐私和国家安全带来了极大威胁。基于此，各界探索和研究了多种网络安全防御技术，其中大数据及人工智能技术是当今最热门的技术之一，被广泛应用在网络安全领域。文章旨在探讨这些技术在计算机网络安全防御系统中的应用。

关键词：大数据；人工智能；网络安全

中图分类号：TP393 **文献标识码：**A

Research on computer network security defense system based on big data and artificial intelligence technology

WAN Zhen

（Jiangxi Natural Gas Group Co.，Ltd.，Nanchang 330000，China）

Absrtact: With the rapid development of information technology, the problem of computer network security is becoming more and more serious. Network attacks, data leaks and other security incidents have brought great threats to personal privacy and national security. Based on this, various circles have explored and studied a variety of network security defense technologies, of which big data and artificial intelligence technology is one of the hottest technologies today, and is widely used in the field of network security. This paper aims to discuss the application of these technologies in computer network security defense system.

Key words: big data，artificial intelligence，network security

在网络安全领域，应用大数据成为一种主流趋势。通过对海量数据的收集、分析和挖掘，有助于发现网络中的异常行为和入侵活动，从而提高网络安全的防御能力。通过综合应用大数据及人工智能技术，可以构建一个更加智能和高效的网络安全防御系统。

1 计算机网络安全的攻击类型

分布式拒绝服务攻击（DDoS）指恶意利用全球范围内不同网络节点上运行的受控制主机，对指定接受攻击的目标计算机关联发起频繁且过量的请求指令，从而耗尽或占据其网络带宽及系统计算资源，使得网络通道出现拥堵现象或目标计算机无法有效处理合法请求信息。

网页篡改是指攻击者借助各种高级的技术手法，有预谋地恶意篡改网站内部的各类文件或应用层次的相关数据。针对关键行业的重要单位，攻击行为通常从计算机网络系统的数据库入手，有选择地对其中的数据进行误改或篡改，甚至采用极为隐蔽的方式，通过劫持网络来建立木马链接[1]。

黑客通过引入不明来源的链接非法获取用户重要数据信息。由于设计过程中存在疏漏或运维过程中存在缺陷，计算机网络可能出现安全漏洞，对整个信息系统的安全性构成了巨大威胁。一旦服务器进程发生故障甚至崩溃，必然使得系统的可用性大打折扣，安全防护功能的有效性将大幅降低。

大规模数据泄露通常表现为海量敏感信息未经授权地被获取或公开，不仅对数据保护造成了极大的威胁，还极易引发国家安全危机、经济活动停滞、社会秩序混乱及公民权利受损等问题。这些泄露的数据涵盖了广泛的领域，如生产流程数据、个人隐私信息、政府管理数据、企业商业机密、系统源代码、配置文件、用户账户及密码等。

2 大数据及人工智能技术的计算机网络安全防御系统设计

2.1 构建人工智能防火墙

构建人工智能防火墙，使系统具备更强大的智能化、决策化水平。通过对海量攻击样本及正常网络活动的深度研究，新型推理机成功构筑出一座知识宝库，不仅囊括已知攻击的各种特征，还能持续更新内容，将新兴威胁的相关信息纳入其中。新型推理机的卓越学习能力使防火墙拥有识别各类攻击类型的本领，有效提升了整个系统的威胁检测效率。此外，新型推理机在进行实时推理时能对潜在威胁的危害程度进行精确评估。借助逻辑推理的力量，系统能够深入剖析网络活动的各种模式，判断是否存在异常行为，并对威胁的级别进行量化。这种实时的危害评估功能使得防火墙能够更为准确地做出相应反应，大幅降低了误报率，进一步提升了系统的整体运行效能[2]。

2.2 智能入侵监测、预警模块

应用大数据与先进的机器学习算法，智能入侵监测模块深度洞察并解析了日常网络活动的常态模式，成功构筑了网络行为的基准模型。一旦侦测到任何与基准模型显著偏离的异常活动，此系统就会立即触发警示信号，将其标记为可能存在的潜在入侵行为，不仅大幅提升了威胁检测的敏锐度，还显著降低了误报率，具备更为强大的自我防护能力。同时，在发现潜在威胁入侵后，预警模块会通过智能化的分析手段及模式匹配技术对威胁进行实时评估与分类。该系统能迅速识别出入侵行为的严重程度，并生成详细的预警信息，不仅为网络管理人员提供了及时且有效的应对策略，也为进一步的反应提供了关键性的参考依据，能助力防御系统强化前瞻性与主动性。

2.3 系统自动修复

系统自动修复模块的核心功能是实时且智能化地做出反应，精确应对各类网络攻击，并迅速采取有效的纠正措施。该模块可以借助先进的机器学习算法从以往的攻击事件中总结经验教训，针对特定威胁形成相应的应对策略。一旦网络系统监测到遭受攻击，自动修复模块就会立即启动，对攻击的破坏程度进行深入分析，从而自主选择最适合的修复方法（如将受感染的节点隔离或恢复已损坏的文件等），最终将系统恢复至正常运行状态。这种全自动化的修复流程大幅提升了网络系统的抗压性及自我修复能力，使得它在遭受攻击后能迅速自我修复，尽可能减少攻击带来的损失[3]。

2.4 传输加密系统

通过对海量网络流量与数据的深度解析，加密系统能够更加迅捷且精准地应对潜在威胁，实现实时安全监测。首先，人工智能技术在加密系统中得到了巧妙应用，极大提升了系统的自适应能力。同时，借助先进的机器学习算法，加密系统能够持续学习并适应各种日新月异的攻击手段，从而实现对未知攻击的高效应对。因此，智能化的加密系统不仅能持续优化加密算法，提升整体安全性，而且能迅速适应新型攻击，从而强化整个网络的安全防护。其次，大数据与人工智能的有机结合使得加密系统具备了更强的预测性。通过深入剖析历史数据及发展趋势，系统有能力预判未来易出现的网络威胁，从而预先采取针对性防御措施。在强化传输加密系统的同时，大数据与人工智能技术的引入为网络安全领域带来了更为全面且智能的解决方案。通过充分挖掘数据价值及应用智能算法，加密系统将持续进化，以适应网络威胁的不断演变，为构筑更安全可靠的计算机网络奠定坚实基础。

3 计算机网络安全防御系统设计与实现

3.1 综合大数据与人工智能技术的安全防御系统

通过对大规模数据的分析和对智能算法的应用，综合大数据与人工智能技术的安全防御系统能够实现对网络安全威胁的及时识别和有效防御，为网络安全提供更加全面和智能化的解决方案。通过收集、存储和分析大规模的网络数据，系统能够实时监测和分析网络流量、日志数据、用户行为等信息，从而识别网络异常行为和潜在安全威胁。其中，大数据分析技术有助于系统从海量数据中找出异常模式和规律，以提高网络安全监测能力和检测准确性；人工智能技术能够通过机器学习、深度学习等方法从大数据中提取有用的信息，并建立预测模型和规则，实现对网络威胁的预测和应对。综合大数据与人工智能技术，安全防御系统的架构设计应考虑到大数据存储、数据处理、模型训练和推断等环节的完整性和高效性，使系统具备分布式存储和计算能力，实现对大规模数据的实时处理和分析。此外，系统应集成各类人工智能算法，实现对不同网络攻击的智能识别和响应。在系统功能实现方面，综合大数据与人工智能技术的安全防御系统应具备实时监测和警报、自动化响应和修复等功能[4]。

3.2 系统架构设计

在综合大数据与人工智能技术的安全防御系统中，需将大数据分析模块和人工智能识别模块相互融合，形成一个完整的安全检测系统。大数据分析模块

负责处理海量的网络数据，以进行实时的数据分析和挖掘，识别异常行为和威胁，而人工智能识别模块则通过深度学习和模式识别技术来快速准确识别网络攻击和威胁。两者相互配合，可实现多层次的安全防御。在系统架构设计中，需要考虑到系统的扩展性和灵活性。由于网络安全形势可不断变化，需要确保系统能够及时应对新的威胁和攻击方式。在设计系统架构时，应考虑到模块化和可插拔的设计，以便系统扩展和升级。此外，系统应具有良好的灵活性，能够根据不同的网络环境和需求进行配置与调整，以满足不同的安全防御需求；应考虑安全防护机制，包括访问控制、身份认证、加密传输等，确保数据和功能不会被攻击者篡改或破坏[5]。

3.3　系统功能实现

系统功能实现部分包括功能模块的设计与开发、模块间的协调与整合。在基于大数据及人工智能技术的计算机网络安全防御系统中，具体功能需兼顾大数据处理、机器学习算法、网络安全协议、用户认证、数据加密等方面的工作。大数据技术可以用于实时监控网络流量、分析异常行为、识别潜在威胁等，因此需设计大数据处理模块（包括数据采集、数据清洗、数据存储、数据分析等）以快速高效处理海量数据，确保系统能够及时发现并应对网络安全威胁。人工智能技术在网络安全领域中的应用越发广泛，机器学习算法是其中的一项重要技术。在系统功能实现中，需要设计用于威胁识别、异常检测、行为分析等功能的机器学习模型，使其能够根据网络环境的变化及时更新并提升识别准确度，以提高对网络攻击的检测和防御能力。在网络安全防御系统中，用户认证是保障系统安全的关键环节，而权限管理则可以确保用户只能访问被授予权限的资源。在系统功能实现中，需要设计并实现用于用户认证、身份验证、权限控制等功能的模块。

4　结束语

本文详细探讨了计算机网络安全防御系统需具备的基本功能要素，深入剖析了以人工智能和大数据技术为核心基础的新型计算机防御体系的关键应用点，并精心整合了人工智能防火墙、机器学习及安全预警等先进技术手段，成功构建出一套自动化程度高且智能化特性显著的网络安全防御系统，全面提升了计算机网络安全防护的整体运行效能。

参考文献：

[1] 姜宇，黄芳.大数据时代人工智能在计算机网络技术中的实践[J].数字技术与应用，2023，41(11)：45-47.
[2] 刘毅.大数据时代人工智能在计算机网络技术中应用分析[J].网络安全技术与应用，2023(12)：167-169.
[3] 张艳艳.基于人工智能技术的计算机网络安全防护系统设计[J].信息与电脑(理论版)，2023，35(4)：233-235.
[4] 姜超.基于大数据的计算机网络安全防范措施分析[J].电子技术，2023，52(11)：112-113.
[5] 马肇云.人工智能技术在网络安全防御中的运用[J].智能建筑与智慧城市，2023(8)：101-103.

作者简介：

万震(1990—)，本科，助理工程师，研究方向：网络安全技术应用。

(上接第 184 页)

新，从而开发出更先进、可靠的故障定位方案，稳固电力系统运行，为社会经济稳定发展提供坚实的电力支撑。

参考文献：

[1] 袁扬，周源根，邵自成，等.计及FTU信息畸变情况下基于覆盖集理论的配电网故障定位[J].电气应用，2024，43(3)：37-44.
[2] 李思远，国力，许志元，等.基于多源报警信息贝叶斯网络与关联离散系数的配电网故障台区定位方法[J].山东电力技术，2024，51(3)：45-54.
[3] 胡桂荣，曹康栖，孟亚宏，等.基于全电流方向特征的低压配电网故障定位方法研究及分析[J].电力信息与通信技术，2024，22(2)：83-90.
[4] 李明恩，庚振新，李雁，等.基于自适应蚁群算法的含分布式电源配电网故障定位研究[J].东北电力技术，2024，45(1)：19-24.
[5] 黄强，李宽，丁敬明，等.含分布式光伏接入的有源配电网故障区段定位新方法[J].山东电力技术，2023，50(11)：68-74.

作者简介：

师延飞(1988—)，硕士，工程师，研究方向：电力工程技术。