应用视角下计算机网络安全技术创新与应用

左双左
上海震旦职业学院，上海市 201900
DOI: 10.61369/SSSD.2025170036

摘　　要： 随着数字化转型的深度推进，计算机网络已成为社会经济运行的核心基础设施，其安全防护能力直接关系到个人隐私、企业生存与国家战略安全。因此，本文从应用视角出发，本文从应用视角出发，系统分析计算机网络安全技术的应用现状与面临的挑战，重点探讨其创新方向，并结合企业级防护、云服务安全、大数据平台防护等典型应用场景，阐述技术落地路径，通过协同机制，构建适应数字化时代需求的网络安全防护体系，为数字经济的健康发展提供坚实保障。

关 键 词： 计算机网络安全；应用视角；技术创新；技术应用

Innovation and Application of Computer Network Security Technology from the Application Perspective

Zuo Shuangzuo
Shanghai Aurora College, Shanghai 201900

Abstract: With the in-depth advancement of digital transformation, computer networks have become the core infrastructure for the operation of social economy. Their security protection capabilities are directly related to personal privacy, enterprise survival and national strategic security. Therefore, from the application perspective, this paper systematically analyzes the application status and facing challenges of computer network security technology, focuses on exploring its innovation directions, and combines typical application scenarios such as enterprise-level protection, cloud service security and big data platform protection to elaborate on the technology implementation paths. Through a collaborative mechanism, it constructs a network security protection system that meets the needs of the digital age, so as to provide a solid guarantee for the healthy development of the digital economy.

Keywords: computer network security; application perspective; technological innovation; technology application

引言

在5G、云计算、大数据、人工智能等新一代信息技术的驱动下，人类社会已全面迈入数字文明新阶段。然而，网络空间的开放性与复杂性也带来了前所未有的安全风险，网络攻击呈现出“智能化、产业化、隐蔽化”的新特征。在此背景下，从应用视角重新审视网络安全技术的创新方向与落地路径，成为学术界与产业界的共同课题[1]。本文探讨技术应用的实践策略，旨在为构建“场景化、智能化、全链条”的网络安全防护体系提供理论参考与实践借鉴。

一、计算机网络安全技术应用现状与挑战

当前，计算机网络安全技术已形成“基础防护 + 专项管控 + 智能升级”的应用格局，在不同领域呈现出差异化的落地特征。在基础防护层面，防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等传统技术仍是网络安全的“第一道防线”，广泛应用于企业园区网络、政务外网等场景。数据安全领域，加密技术与数据防泄漏（DLP）系统成为应用热点。在智能化升级趋势下，AI技术开始与传统安全技术融合，部分头部企业已部署 AI 驱动的威胁检测平台[2]。尽管已经实现了不少网络安全技术应用成果，不过随着数字化的持续深入，挑战还有很多。首先便是智能隐藏型的攻击模式增加了防御难度。黑客使用人工智能技术产生对抗样本，从而绕开基于特征代码的传统 IDS/IPS 的检测规则；无文件攻击、内存马等新型攻击手段不依赖于硬盘上的文件，基于特征代码的检测策略不再适用。其次则是混合工作环境与云边缘协作环境打破了传统的安全防御环境。随著远程工作的广泛运用，企业人员开始通过个人设备和私有网络访问公司内部数据，而这种“内外网隔离”的安全防御架构失效；云计算由于其分布式架构，

数据存储和处理资源被分散，造成云服务商和服务用户之间对安全责任的界定变得模糊。

二、应用视角下计算机网络安全技术的创新发展

（一）AI 智能网络安全技术

AI 技术为网络安全防护注入了“智慧大脑”，其创新应用主要体现在威胁检测、恶意软件分析、自动化响应等方面。与传统网络安全技术相比，AI 驱动的网络安全技术具有优势，见表1。在威胁检测领域，基于深度学习的异常检测技术突破了传统特征码检测的局限性。恶意软件分析方面，AI 技术实现了从“静态分析”向“动态行为分析”的转变。传统静态分析依赖反编译技术提取恶意代码特征，易被加壳、混淆技术规避[3]；而 AI 驱动的动态分析通过沙箱环境运行恶意软件，捕捉其在内存、注册表、网络连接等方面的行为特征，结合卷积神经网络（CNN）、图神经网络（GNN）等模型进行分类识别。

表1 AI 与传统网络安全技术对比

对比维度	传统网络安全技术	AI 驱动网络安全技术
威胁检测	依赖已知特征码 / 规则	分析行为异常，识别未知威胁
响应效率	人工分析，小时 / 天级响应	自动化闭环，分钟级处置
误报控制	阈值固定，误报率高	动态学习基线，自适应调整
适应性	手动更新规则，响应滞后	自主学习新威胁特征

（二）零信任安全架构创新

零信任安全架构以“永不信任，始终验证”为核心理念，颠覆了传统“边界信任”的防护模式，其创新点主要体现在身份认证、访问控制、动态风险评估三个维度。在身份认证方面，零信任架构采用“多因素认证 + 持续认证”的模式，替代传统单一密码认证。MFA 结合密码、生物特征、硬件令牌等多种因素，提升身份认证的安全性；持续认证通过实时分析用户行为、设备状态、网络环境等信息，动态判断身份合法性。访问控制领域，零信任架构引入“最小权限原则”与“细粒度授权”机制。通过基于角色的访问控制（RBAC）、基于属性的访问控制等技术，实现对资源的精细化管控。动态风险评估是零信任架构的核心支撑技术，通过构建风险评估模型，实时计算访问请求的风险值[4]。评估指标包括用户行为偏差度、设备漏洞数量、网络威胁等级等，当风险值超过阈值时，自动增强认证强度或拒绝访问。

（三）数据安全全生命周期防护技术

该技术以数据为中心，覆盖数据生成、传输、存储、使用、共享、归档与销毁七个阶段，形成闭环式安全管控。在数据生成阶段，通过分类分级技术对数据按敏感程度进行划分，为后续防护提供依据。数据传输阶段，除传统 SSL/TLS 加密外，量子密钥分发（QKD）技术实现了“无条件安全”的加密传输，我国“京沪干线”量子保密通信网已在金融、政务等领域实现应用。数据存储阶段采用加密存储与数据脱敏技术，透明加密技术可对文件、数据库进行自动加密，脱敏技术则通过替换、屏蔽等方式将敏感数据转换为非敏感数据，满足数据共享与测试需求[5]。数据使用阶段，动态数据脱敏根据用户权限实时替换敏感字段，数据水印技术则在数据中嵌入不可见标识，实现泄漏溯源。数据共享阶段，区块链技术通过记录共享的主体、时间与内容等信息，确保共享过程可审计、防篡改。在归档与销毁阶段，采用符合国家标准的存储介质与销毁技术，确保数据彻底清除，防止残留数据泄露。

三、应用视角下计算机网络安全技术的应用

（一）企业级网络安全防护应用

在数字化业务高度依赖信息系统的今天，构建坚实的企业级网络安全防护体系已成为企业稳健运营的基石。此类防护应用通过整合多种技术手段，旨在构建一个纵深防御体系，以应对来自外部和内部的各种安全威胁。网络安全防护产品是基于多层次协调技术的集合，主要包括以下几个方面：第一，企业防火墙是网络边界的安全堡垒，通过执行安全策略控制网络访问[6]。第二，IDS/IPS 旨在对网络流动和系统活动持续监控识别和阻止不法行为；第三，SIEM 是安全运行的重要支点，可以集中集约各类日志和警报从全局范围内收集和分析，快速发现并应对复杂的攻击链路；第四，终端安全方案应用于服务器、PC、手机等各类终端，可以实现防病毒、漏洞管理的全面防护，并且结合数据加密技术和严格身份认证确保数据传输、存储过程中的机密性以及用户授权合法性。

（二）云服务提供商的网络安全防护应用

在数字化时代，云服务提供商承担着保障用户数据与业务安全的核心责任。为构建可信赖的云环境，提供商致力于从技术防护和安全管理两个维度建立系统化的网络安全体系。在技术层面，云服务提供方推出了高效能的保护策略，例如对网络流量进行24小时实时监控和对非法攻击行为的防护措施、广泛采用下一代防火墙、入侵监控与防御系统等最新网络安全技术等；此外，采用人工智能等新技术对海量安全日志等信息进行智能处理，提升对新型威胁的预警反应速度。在数据安全方面，针对基础、架构和程序层面进行严格的限制和加密处理，确保客户数据在整个生命周期内的安全性和可靠性[7]；此外，通过定期漏洞检测、渗透测试和安全审计工作等帮助企业提前发现安全隐患并加以解决，增强防护能力。从管理角度来看，重视企业这个最重要的“人”这一维度。推出了长线安全培训和意识提升活动，向所有内部员工开展常年的网络安全指南、操作规程和应急预案、典型安全场景或情景演练等方面的系列课程，在基础层面不仅涵盖简单安全常识如禁止用私人 U 盘复制加密文件等，同时也涵盖更高级别如新型高精尖威胁类型鉴别及应对等内容，辅之以模拟训练等方式，以提高员工学习的成效，最终的目的是要在企业内部形成一种浓厚的安全文化氛围，让员工始终能够站在企业的立场作为一道安全防线，尽可能避免因失误带来的安全问题。云服务商网络安全防护的基本思路是重在技术和重在管理，同时重在防御、重在运营，以系统的思路开展工作，可以保证云平台的稳定和有

效，为用户的业务正常运转提供了安全保障[8]。

（三）大数据平台的网络安全防护应用

大数据平台汇聚了企业核心数据资产，其网络安全防护应用主要围绕风险评估、安全审计和主动防御三个关键层面展开，构建覆盖数据全生命周期的安全防线。一是风险评估。对安全性进行评估是保护系统的最关键环节。将大型信息处理系统中包含的各个装置都进行完整的安全隐患审计和配置稽查，查明技术漏洞的位置[9]。与此同时，利用数据分割等级的相关技术进行工作，自动地侦测并评估出敏感数据的数量和等级，预判出可能泄漏量和敏感数据的重要程度。该过程将一直处于循环监控模式，可以利用最新的危险警告信息来修正模式，作为准确的防护方案的依据。二是安全审计。为了获得数据安全合法性上的保障，安全审核意味着可以对每一个用户和每一个系统的行为数据使用情况进行跟踪记录并形成详细的数据使用历史文件。基于这些精确的数据使用历史文件，系统可以在第一时间及时检测出任何未被授权的异常数据访问方式，而一旦出现安全异常，也能够迅速查出问题根源，找出当事人，以满足越来越高的数据保护法要求。三是主动防御。主动防御智能安全系统以预先的保障方法应对安全隐患，在系统应用过程中，利用机器学习技术分析研究用户的行为特征，访问数据的使用模式，制定并构建出用户系统的正常行为标准，当偏离正常标准时发出警报并采取相应的举措进行阻拦。另外利用动态脱敏、差分隐私等技术，在对数据进行操作时按照权限级别自动对关键信息进行遮蔽，实现兼顾数据可用性及保证数据的安全性[10]。这三方面相互衔接，共同构成大数据平台的一体化防护体系，从而有效保障大数据环境的安全稳定运行。

四、结语

综上所述，数字化转型的深入推进，既为计算机网络安全技术带来了挑战，也催生了创新机遇。网络安全技术的创新不能脱离应用场景，需以解决实际问题为导向，实现“技术创新与场景需求”的深度融合。在实际应用中，应推进企业级网络安全防护、云服务提供商的网络安全防护、大数据平台网络安全防护应用，推进安全技术与业务系统深度融合，提升安全防护效果。面对日益复杂的网络安全形势，相关部门应协同发力，加快推进技术创新和标准建设，以营造出安全可控的网络空间。

参考文献

[1] 王飞，卢燕 . 计算机网络安全技术的影响因素与防范策略探讨 [J]. 江西电力职业技术学院学报 ,2024,37(10):25-27+41.

[2] 庄渊 . 计算机网络安全技术发展趋势——评《计算机网络安全实验指导》[J]. 中国安全科学学报 ,2024,34(10):248.

[3] 杨金玉，朱金杰 . 基于局域网环境的计算机网络安全技术分析 [J]. 网络安全技术与应用 ,2024,(10):5-7.

[4] 张伟 . 计算机网络安全技术发展趋势思考——评《计算机网络管理与安全技术研究》[J]. 安全与环境学报 ,2024,24(09):3705.

[5] 韩剑飞，朱政昊，苏凯旋 . 大数据下的计算机网络安全技术研究 [C]// 中国金属学会，中国金属学会青年工作委员会 . 第十二届中国金属学会青年学术年会暨首届“碳中和”冶金青年科学家沙龙论文集（二）. 鞍钢集团信息产业有限公司 .2024.023539.

[6] 尤笑歌 . 大数据时代下计算机网络安全技术的优化策略 [J]. 数字技术与应用 ,2024,42(08):78-80.

[7] 朱意，胡雪春 . 计算机网络安全技术在电子商务平台运维中的应用策略研究 [J]. 信息与电脑（理论版）,2024,36(14):124-126.

[8] 马艮娟，卜言彬 . 简析大数据时代计算机网络安全技术的优化策略 [J]. 数字技术与应用 ,2024,42(01):224-226.DOI:10.19695/j.cnki.cn12-1369.2024.01.71.

[9] 韩鹏军，曹慧，曹文桥 . 基于计算机网络安全技术的态势感知防御方法 [J]. 信息技术 ,2024,(03):188-194.DOI:10.13274/j.cnki.hdzj.2024.03.030.

[10] 崔晓萌，田思雨 . 计算机网络安全技术在电子商务中的应用 [J]. 信息与电脑（理论版）,2024,36(05):221-223.

