计算机网络安全的现状及网络安全技术措施

刘影超　周云飞
河北方维网络技术有限公司　河北　石家　050000

摘　要：计算机网络安全现状严峻，网络攻击手段多样、数据泄露频发，新兴技术也带来新挑战。为此，需采取加密、防火墙等技术措施，并建立安全制度、定期评估扫描、加强技术集成协同。展望未来，人工智能将在网络安全中深度应用，零信任安全架构有望推广，同时，加强网络安全国际合作，共同应对全球性挑战、推动技术创新。

关键词：计算机网路安全；现状；网络安全；技术措施

引言：在数字化浪潮席卷全球的当下，计算机网络安全已成为关乎个人、企业乃至国家安全的关键议题。当前，网络攻击手段愈发多样频繁，数据泄露问题严峻，新兴技术也带来全新挑战。为应对这些威胁，加密、防火墙、入侵检测等技术措施应运而生，同时其有效实施与优化也至关重要。展望未来，人工智能在网络安全领域将深度应用，零信任安全架构有望推广，国际合作也将不断加强。本文将深入剖析现状、探讨技术、展望趋势。

1 计算机网络安全现状

1.1 网络攻击手段多样化且频繁

近年来，网络攻击态势愈发严峻，攻击手段持续迭代更新，呈现出高度多样化与复杂化的显著特征。传统类型的病毒、木马攻击仍保持着较高的活跃度，它们借助恶意软件捆绑、系统漏洞利用等途径，悄无声息地侵入用户系统，肆意破坏关键数据或窃取敏感信息，给用户造成难以估量的损失。与此同时，依托人工智能、区块链等新兴技术的新型攻击手段不断涌现，其攻击逻辑更为隐蔽、破坏力更强。此外，钓鱼攻击也在持续进化升级，通过伪造高度逼真的网站、邮件等精心设计陷阱，诱骗用户主动泄露账号密码等敏感信息，进一步加剧了网络安全的防护压力。

1.2 数据泄露问题严峻

在数字化浪潮席卷之下，数据已然跃升为现代社会最具战略价值的核心资产，其重要性与日俱增，也因此成为网络攻击者觊觎的重点对象。当前，众多企业和机构由于网络安全防护体系存在漏洞、安全管理制度执行不严等安全防护措施不到位的问题，数据泄露事件频发且呈高发态势。数据泄露的后果极为严重，不仅会严重损害企业的品牌形象与市场声誉，导致客户信任度大幅下降，还可能使企业面临违反数据保护法规的法律风险，进而遭受巨额罚款与诉讼赔偿。长此以往，将给企业的可持续发展带来难以估量的负面影响与损失。

1.3 新兴技术带来新的安全挑战

人工智能、物联网、云计算等新兴技术的迅猛发展，在极大推动社会数字化转型、为人们生活带来诸多便利的同时，也衍生出一系列前所未有的网络安全挑战。在人工智能领域，深度学习模型易遭受对抗样本攻击，导致模型误判，且可能被恶意利用生成虚假信息、实施自动化网络攻击等，造成严重不良影响。物联网领域，海量设备接入网络，但多数设备安全防护能力薄弱，存在诸多安全漏洞，极易被攻击者利用作为入侵网络的关键跳板。云计算环境下，多租户共享计算与存储资源，数据存储和处理呈现高度分散化特征，这无疑大幅增加了数据安全管控的复杂性与风险系数[1]。

2 网络安全技术措施

2.1 加密技术

加密技术作为保障数据安全的核心基石，通过特定的算法将原始的明文数据转换为密文形式，确保仅持有正确密钥的授权用户能够成功解密并读取数据内容，从而有效抵御未授权访问与数据泄露风险。在数据传输环节，采用如SSL/TLS等加密协议，能够构建安全的数据传输通道，保障信息在网络环境中的保密性、完整性与真实性，防止数据在传输途中被窃取或恶意篡改。而在数据存储层面，全盘加密或文件级加密技术的应用，使得即便存储设备遭遇丢失、被盗等意外情况，攻击者因缺乏解密密钥仍无法获取数据实际内容，进一步增强了数据存储的安全性。此外，量子加密技术作为新兴领域，依托量子力学原理，理论上可实现无条件安全的通信，为未来关键领域的数据安全防护提供了新的可能。

2.2 防火墙技术

防火墙作为网络安全架构中的首要屏障，承担着监测、限制与调控跨越网络边界数据流的重任。它通过精细的策略配置，有效对外部网络隐藏内部网络的信息细

节、拓扑结构及运行状态，从而构建起稳固的安全防护层。防火墙技术主要分为包过滤防火墙、状态检测防火墙及应用层网关防火墙三大类。包过滤防火墙依据数据包的源/目的IP地址、端口号等基本信息进行初步筛选；状态检测防火墙则在此基础上，深入跟踪网络连接状态，提升对连接型攻击的防御能力；应用层网关防火墙则对应用层协议进行深度解析与控制，有效抵御针对应用层的各类复杂攻击。企业和机构需结合自身网络特性与安全需求，科学部署防火墙，并定期更新规则库，以确保对新兴网络威胁的持续有效防御[2]。

2.3 入侵检测与防御技术

入侵检测系统（IDS）与入侵防御系统（IPS）是网络安全领域中实时监控网络流量、精准识别并有效阻断入侵行为的关键工具。IDS通过深度分析网络流量特征或系统日志记录，敏锐捕捉可疑活动或潜在攻击迹象，并即时触发警报机制。其中，基于特征的IDS依托庞大的已知攻击特征库进行比对识别，而基于异常的IDS则通过构建正常行为基准模型，有效甄别偏离常态的异常行为。相较之下，IPS在具备检测能力的同时，还能在发现入侵行为时自动启动阻断措施，实现攻击的即时防御。实践中，IDS与IPS的协同部署可构建起多层次、立体化的安全防护网。此外，随着人工智能技术的深入应用，智能入侵检测与防御系统逐渐崭露头角，其利用机器学习算法对海量数据进行深度挖掘，能够更精准地识别新型攻击手法与未知威胁。

2.4 身份认证与访问控制技术

身份认证作为网络安全防护的基石，承担着确保仅合法用户能够访问受保护网络资源的重要职责。鉴于传统用户名与密码认证方式存在易遭受暴力破解、用户易遗忘等安全隐患，多因素认证技术应运而生，并逐渐成为主流。多因素认证通过融合知识因素（如密码）、拥有因素（如动态令牌）及生物特征因素（如指纹识别）等多种身份验证手段，显著提升了身份认证的可靠性与安全性。访问控制技术则依据用户的身份标识及预设权限，对其访问网络资源的行为进行精细化管控。通过严格遵循最小权限原则，即仅授予用户执行其工作职责所必需的最低权限级别，可有效缩减潜在攻击面，降低因用户账号泄露或滥用而引发的安全风险，为网络环境构建起一道坚实的权限管理屏障。

3 网络安全技术措施的实施与优化

3.1 建立完善的安全管理制度

企业和机构若要切实落地有效的网络安全技术防护举措，首要任务是构建一套系统完备、科学规范的安全管理制度体系。这一制度需清晰界定各部门及岗位人员在网络安全保障中的具体职责，确保责任到人、任务到岗，形成齐抓共管的良好局面。同时，要制定详尽且具可操作性的安全操作规范与流程，涵盖网络访问控制、数据加密存储、系统漏洞修复等关键环节，为日常网络安全管理提供明确指引。此外，应严格规范员工在使用网络资源时的行为准则，通过定期组织网络安全专题培训，不断提升员工的安全防范意识与实际操作技能，使其能够熟练掌握常见的网络攻击手法及应对策略。为有效应对可能发生的网络安全事件，企业和机构还需建立健全安全事件应急响应机制，明确应急处置流程、责任分工及资源调配方案。一旦遭遇网络安全事件，能够迅速启动应急预案，采取针对性措施进行高效处置，最大限度降低事件对业务运营及数据安全的负面影响，确保企业和机构的网络安全稳定运行[3]。

3.2 定期进行安全评估与漏洞扫描

为保障网络安全技术措施持续发挥效能，企业和机构需将定期安全评估与漏洞扫描纳入常态化安全管理工作。具体而言，应借助专业的安全评估工具与成熟技术方法，对网络架构、核心系统、关键应用程序等开展全方位、深层次的安全评估，精准识别潜在的安全风险点与系统漏洞。通过实施渗透测试，模拟真实黑客攻击场景，全面检验网络系统的安全防御能力，并依据测试结果生成详细的安全改进建议报告，为后续安全加固提供有力支撑。同时，企业和机构应建立定期漏洞扫描机制，运用自动化扫描工具，及时发现操作系统、数据库、中间件及各类软件应用中存在的已知漏洞，并严格按照安全规范及时安装官方补丁进行修复，从源头上消除安全隐患。此外，还需密切关注权威安全厂商发布的安全通告与漏洞预警信息，动态跟踪最新安全态势，对可能波及自身网络安全的潜在威胁提前制定防范策略，确保网络安全防护体系始终处于最佳运行状态。

3.3 加强安全技术的集成与协同

在网络安全威胁愈发呈现出多样化、复杂化与隐蔽化特征的当下，单一安全技术已难以独立应对日益严峻的安全挑战，加强安全技术的集成与协同成为提升网络安全防护能力的关键路径。企业和机构应将加密技术、防火墙技术、入侵检测与防御技术、身份认证与访问控制技术等各类核心安全技术进行深度融合与有机整合，构建一个紧密协作、高效联动的综合性安全防护体系。具体而言，加密技术可为数据传输与存储提供坚实的安全保障，防火墙技术则作为第一道防线过滤非法访问，入侵检测与防御技术实时监测并阻断潜在攻击，身份认

证与访问控制技术严格管控用户访问权限。各安全技术之间通过信息共享、策略联动与协同响应机制，实现优势互补与功能叠加，形成对网络安全的全方位、多层次、立体化防护格局。这种集成协同的安全防护模式不仅能够显著提升对已知威胁的防御效能，还能有效应对未知威胁与新型攻击，为企业的网络安全稳定运行提供有力保障。

4 网络安全未来发展趋势与展望

4.1 人工智能在网络安全中的深度应用

展望未来，人工智能必将在网络安全领域占据愈发核心的地位，发挥不可替代的关键作用。其一，在攻击检测与预测方面，人工智能凭借强大的数据处理与模式识别能力，可对海量的网络流量数据、系统日志等进行深度学习与精准分析。智能安全系统借此能够自动捕捉异常行为模式，精准识别潜在的攻击威胁，并提前发出预警信号，为安全团队争取宝贵的应对时间，将损失控制在最小范围。其二，人工智能可赋能自动化安全响应。一旦检测到攻击行为，智能系统能迅速自动触发预设的防御机制，如阻断恶意连接、隔离受感染设备等，大幅提升安全响应的速度与效率。此外，人工智能还能依据网络环境的动态变化以及攻击态势的持续演变，自动优化调整安全防护策略，实现网络安全管理的智能化与自适应化。

4.2 零信任安全架构的推广应用

传统网络安全架构秉持边界防护理念，默认网络内部为可信区域，外部则为不可信区域，通过构建防火墙等边界防护设施来保障安全。但随着网络攻击手段的持续进化，如内部人员违规操作、高级持续性威胁（APT）攻击等，这种边界防护模式的局限性日益凸显，难以应对复杂多变的网络安全挑战。零信任安全架构则颠覆了传统观念，它秉持“默认不信任，始终要验证”的原则，假定网络内部和外部的所有用户、设备及应用均不可信。在访问网络资源时，无论请求来自何处，都需进行持续的身份验证与动态授权，并基于实时风险评估结果调整访问权限。未来，随着企业数字化转型步伐的加快以及网络安全需求的不断升级，零信任安全架构凭借其更精细的访问控制与更强的安全防护能力，有望在更多行业和企业中得到广泛推广与应用[4]。

4.3 加强网络安全的国际合作

网络安全问题具有全球性，一个国家或地区发生的网络安全事件可能迅速波及全球。因此，加强网络安全的国际合作成为未来的发展趋势。各国政府、企业和安全机构将加强信息共享和技术交流，共同应对全球性的网络安全挑战。通过制定国际网络安全规则和标准，规范网络空间行为，营造安全、稳定、有序的网络空间国际环境。同时，在关键技术领域开展国际合作，共同推动网络安全技术的创新和发展。

结束语

网络安全现状严峻，网络攻击多样、数据泄露频发、新兴技术带来新挑战。但通过加密、防火墙等多样技术措施，以及完善制度、定期评估、技术协同等实施优化手段，可筑牢安全防线。展望未来，人工智能将深度应用于安全领域，零信任架构有望广泛推广，国际合作也将不断加强。各方需紧跟趋势，持续创新与完善网络安全体系，以应对不断变化的威胁，共同营造安全可靠的网络空间，护航数字化时代稳健发展。

参考文献

[1]范清永.试论当下计算机网络安全现状及对策[J].信息记录材料,2021(5):58-59.

[2]刘超南.计算机网络安全现状及防御技术[J].通讯世界,2019(1):123-124.

[3]赵小波.计算机网络安全技术的影响因素与防范策略探讨[J].赤峰学院学报(自然科学版),2021,(09):44-47.

[4]朱粤.大数据时代计算机网络安全技术探讨[J].信息与电脑(理论版),2021,(13):58-60.