基于网络信息安全技术管理的计算机应用研究

井 轩 廖家勇
汉江水利水电（集团）有限责任公司网络信息中心 湖北 武汉 430000

摘 要：随着信息技术的迅猛发展，网络信息安全面临前所未有的挑战，包括网络攻击手段日益多样化与复杂化、新技术带来的未知安全威胁、用户安全意识薄弱以及企业安全管理不到位等问题。本文探讨了信息安全技术在计算机应用中的关键应用，包括数据加密技术、防火墙技术、入侵检测技术和身份认证与访问控制技术。这些技术的应用有助于提升计算机系统的安全防护能力，保护用户数据的安全与隐私。

关键词：网络信息；安全技术管理；计算机应用

引言

随着计算机技术的广泛应用，网络攻击手段日益多样化与复杂化，给信息安全带来了巨大挑战。新技术的不断涌现也带来了新的安全威胁，如云计算、大数据、人工智能等技术的应用，使信息安全问题更加复杂。此外，用户安全意识薄弱和企业安全管理不到位也加剧了信息安全风险的产生。加强信息安全技术在计算机应用中的研究与应用，对于保障信息安全具有重要意义。

1 网络信息安全面临的挑战

1.1 网络攻击手段多样化与复杂化

网络攻击手段的不断演变和复杂化，给网络信息安全带来了前所未有的挑战。传统的网络攻击手段如病毒、木马、蠕虫等，已经不足以满足攻击者的需求。如今，黑客们利用更加先进的技术和工具，通过钓鱼攻击、勒索软件、DDoS攻击等多种方式，对政府机构、企业、个人等目标进行攻击。这些攻击手段不仅技术性强，而且隐蔽性高。黑客们利用社会工程学、心理学等手段，精心设计各种诱饵和陷阱，诱骗用户点击恶意链接或下载病毒文件。一旦用户中招，攻击者就能轻松窃取用户的敏感信息，如账号密码、银行卡信息等，进而实施从而的犯罪活动。此外，网络攻击往往是有组织、有目的的。一些黑客团伙或国家背景的网络间谍组织，利用漏洞和弱点进行入侵，窃取敏感信息，破坏系统正常运行。这些攻击行为不仅给受害者带来严重的经济损失和声誉风险，还可能对国家安全和社会稳定造成威胁。

1.2 新技术带来的安全威胁

近年来，云计算、物联网、人工智能等技术的广泛应用，无疑是科技领域的重大突破。它们不仅提升了数据处理能力，也优化了人们的生活体验。每项新技术的诞生，都伴随着潜在的安全隐患。其一，云计算技术的兴起使企业可以方便地将大量数据存储在云端。这为企业提供了弹性、可扩展的数据存储和计算能力[1]。其二，数据在云端的安全问题也日益凸显。由于云环境的多租户特性和边界模糊性，数据泄露和被黑客攻击的风险大大增加。攻击者可能会利用漏洞或社交工程手段，窃取敏感信息或篡改数据，给企业带来巨大损失。其三，物联网设备的普及也给网络信息安全带来了新挑战。从智能家居到工业自动化，物联网设备已经渗透到生活的方方面面。这些设备往往缺乏足够的安全防护措施，使攻击者可以轻易地入侵并控制它们。一旦攻击者掌握了这些设备的控制权，他们就可以窃取个人信息、干扰系统运行，甚至可能引发更严重的安全问题。其四，人工智能技术的快速发展也给网络信息安全带来了新的难题。人工智能技术具有高度的复杂性和不确定性，使安全专家难以完全掌握其工作原理和潜在风险。这导致了一些黑客利用人工智能技术的漏洞进行攻击，如利用深度学习模型进行恶意软件生成或绕过安全检测等。人工智能技术的广泛应用也使攻击者可以更加智能地进行攻击，增加了防御的难度。

1.3 用户安全意识薄弱

在当前的数字化时代，网络信息安全的重要性日益凸显。尽管技术和政策在不断完善，但网络信息安全仍面临着诸多挑战。其中，用户安全意识薄弱是尤为突出的问题。用户，作为网络使用的主体，他们的行为直接关系到网络信息的安全性。但遗憾的是，许多用户对于网络安全的认识并不深刻，甚至可以说是相当匮乏。这种安全意识的缺失导致了他们在日常的网络使用中，常做出一些看似微不足道但却潜藏巨大风险的行为。比如，有些用户会随意点击不明链接或下载不明文件。这些链接或文件可能携带着恶意软件，一旦点击或下载，用户的设备就有可能被病毒或木马入侵，进而导致个人信息泄露，甚至整个系统被攻击者控制。另外，许多用

户还习惯于使用弱密码或重复使用密码。弱密码容易被破解，而重复使用密码则意味着一旦某个平台的账户被攻破，攻击者就可以尝试在其他平台使用相同的密码登录，从而获取更多的个人信息[2]。它们不仅增加了个人信息泄露的风险，也为网络攻击者提供了可乘之机。提高用户的安全意识，教育他们如何正确使用网络、如何保护个人信息，是当前网络信息安全工作中亟待解决的重要问题。

1.4 企业安全管理不到位

在当今数字化时代，网络信息安全的重要性日益凸显。众多企业在实际运营过程中，往往忽视了网络安全管理的关键性，从而暴露出一系列严重的问题。其中，企业安全管理不到位是一个尤为突出的挑战。首先，企业可能缺乏完善的网络安全管理制度和流程。网络安全是一个系统性工程，需要从制度层面进行规范和保障。一些企业往往忽视制度建设，导致安全管理存在明显的漏洞和盲区。没有明确的安全责任划分、缺乏有效的安全监管机制，以及应对安全事件的应急预案不足，都使企业在面对网络攻击时显得力不从心。企业对员工的安全教育和培训不够重视。员工是企业网络安全的第一道防线，他们的安全意识和技能直接关系到企业的安全状况。企业往只关注业务发展和经济效益，忽视了员工的安全教育。员工缺乏必要的安全意识和技能，容易成为黑客攻击的目标，甚至可能无意中泄露企业的敏感信息。企业在技术防范方面也存在不足。网络安全是一个技术密集型领域，需要采用先进的技术手段进行防范。企业由于资金、技术等方面的限制，往往未能及时更新安全补丁、采用有效的安全防护措施。这使企业的信息系统在面对新型网络攻击时显得脆弱不堪，容易受到攻击者的利用和破坏。

2 信息安全技术在计算机应用中的关键应用

2.1 数据加密技术

数据加密技术，顾名思义，是对数据进行加密处理的一种技术手段。这种技术的核心目的是确保数据在传输和存储过程中不被非法获取或篡改，从而保护数据的机密性、完整性和可用性。当前，市场上存在多种数据加密算法，每种算法都有其独特的特点和适用场景[3]。其中，对称加密算法是一种常用的加密方式。它采用相同的密钥进行加密和解密，因此要求通信双方必须事先共享密钥。这种算法具有加密速度快、效率高的优点，但在密钥管理上存在一定的风险。另一种重要的加密算法是非对称加密算法。与对称加密算法不同，非对称加密算法使用一对密钥，即公钥和私钥。公钥用于加密数据，而私钥则用于解密数据。这种算法在密钥管理上更为安全，因为公钥可以公开传播，而私钥则由持有者自己保管。非对称加密算法在数字签名、身份验证等领域有着广泛的应用。还有一些其他的加密算法，如哈希算法、混合加密算法等。这些算法可以根据不同的应用场景和需求，提供不同级别的安全保护。例如，哈希算法可以用于验证数据的完整性，而混合加密算法则可以结合多种算法的优点，提供更为强大的安全性能。在实际应用中，数据加密技术广泛应用于各种领域，如金融、医疗、电商等。通过对敏感数据进行加密处理，可以确保数据在传输和存储过程中的安全性，防止数据泄露和非法访问。数据加密技术还可以用于构建安全的通信渠道，保护通信双方的隐私和权益。数据加密技术既能保护数据的机密性和完整性，还可以为各种应用场景提供强大的安全保障。

2.2 防火墙技术

防火墙，作为网络安全的第一道防线，发挥着至关重要的角色。在计算机应用中，防火墙可以实时监控和控制进出网络的数据包，有效阻止非法访问和攻击。防火墙的工作机制相当复杂，它通过分析数据包的来源、目的地、端口号等信息，来判断是否允许数据包通过。对于可疑或恶意的数据包，防火墙会进行拦截，从而保护内部网络不受攻击。防火墙还能记录和分析网络流量，帮助管理员了解网络的使用情况和潜在的安全风险。随着技术的不断进步，现代防火墙技术已经实现了智能化和自适应化。它们能够根据网络流量、用户行为等信息动态调整安全策略。例如，当某个IP地址在短时间内尝试多次连接内部服务器时，防火墙可以自动将其加入黑名单，阻止其从而的访问。这种动态调整的能力大大提高了防火墙的安全防护效果。防火墙还可以与其他安全设备和技术进行集成，形成多层次的安全防护体系。例如，防火墙可以与入侵检测系统（IDS）或入侵防御系统（IPS）进行联动，当IDS或IPS检测到攻击行为时，可以通知防火墙进行拦截[4]。这种协同工作的方式能够从而提高网络的安全性能。需要注意的是，防火墙并非万能的。它只能根据预设的规则和策略进行防护，对于一些新型或复杂的攻击手段可能无法有效应对。除部署防火墙外，还需要结合其他安全技术和措施，如加密技术、身份验证等，共同构建全面、高效的信息安全体系。防火墙技术在计算机应用中扮演着举足轻重的角色。通过不断更新和升级防火墙技术，可以更好地保护网络免受攻击和威胁，确保信息的机密性、完整性和可用性。

2.3 入侵检测技术

入侵检测系统通过收集和分析网络流量、系统日志等关键信息，能够实时监控网络环境的动态变化。当检测到异常流量或行为模式时，系统会立即触发警报，并将相关信息发送给管理员或安全团队。这使安全人员能够迅速定位潜在的安全威胁，并采取相应的应对措施，如隔离被攻击的系统、阻断恶意流量等。入侵检测技术的应用范围非常广泛，不仅适用于大型企业网络的安全防护，也适用于个人用户的计算机和移动设备。在大型企业网络中，入侵检测系统能够保护关键业务数据和系统免受攻击者的侵害，确保企业的正常运营。对于个人用户而言，入侵检测技术可以帮助他们识别和防范各种网络诈骗、恶意软件等威胁，保护个人隐私和财产安全。随着人工智能和机器学习技术的不断发展，入侵检测系统也在不断升级和完善。通过引入先进的算法和模型，系统能够更准确地识别和分析网络中的异常行为，提高检测的准确性和效率。一些先进的入侵检测系统还能够实现自动化响应和处置，从而提升了网络安全的防护能力。入侵检测技术是信息安全技术在计算机应用中的一项重要应用，它能够帮助企业和个人有效应对网络威胁，保护信息安全。随着技术的不断进步和应用场景的不断扩展，入侵检测技术将在未来发挥更加重要的作用。

2.4 身份认证与访问控制技术

身份认证与访问控制技术是信息安全领域中至关重要的组成部分，它确保了只有经过合法授权的用户才能访问和使用计算机资源。这种技术的引入，为组织和企业提供了坚实的安全防线，有效地抵御了潜在的安全威胁。身份认证是验证用户身份的过程，它确保只有真实的用户才能访问系统。传统的身份认证方法可能仅限于用户名和密码，但这种方式存在被破解的风险。现代的身份认证技术通常采用多因素认证，这包括密码、生物识别（如指纹、面部识别）、手机验证码等多种方式的组合。这种方式显著提高了认证的准确性和安全性，使未经授权的用户难以进入系统。访问控制技术则从而确保了只有具有相应权限的用户才能访问特定的资源。这涉及到对用户的角色、职责和需要进行精细的权限管理。通过为不同用户分配不同的权限级别，访问控制技术可以有效地防止敏感数据被未经授权的用户获取或篡改。它还可以记录用户的访问行为，为审计和追踪提供有力的支持。身份认证与访问控制技术的结合，使组织和企业能够构建一个安全、可靠的计算环境。它既能防止外部攻击者的入侵，还可以防止内部人员的非法操作。这种技术的广泛应用，对于保护个人隐私、维护企业利益以及保障国家安全都具有重要意义[5]。随着技术的不断发展，身份认证与访问控制技术也在不断更新和完善。新的认证方式、更精细的权限管理策略以及智能化的安全防御机制等，都在不断提高信息安全防护的水平。

结束语

综上所述，信息安全技术在计算机应用中的关键作用不容忽视。通过数据加密、防火墙、入侵检测以及身份认证与访问控制等技术的综合应用，可以有效应对网络攻击、保护数据安全、提升系统防御能力。信息安全是一个长期且复杂的任务，需要不断的技术创新和管理提升。未来，应继续深化信息安全技术研究，加强用户安全教育和企业安全管理，共同构建安全、可靠的网络环境，推动信息化社会的健康发展。

参考文献

[1]马德慧.基于网络信息安全技术管理的计算机应用研究[J].科学与财富,2020(5):44.

[2]王莉红.基于网络信息安全技术管理的计算机应用研究[J].电子元器件与信息技术,2022,6(2):243-245.DOI:10.19772/j.cnki.2096-4455.2022.2.093.

[3]范东辉.基于网络信息安全技术管理的计算机应用研究[J].中外交流,2021,28(8):1223.

[4]刘斌.基于网络信息安全技术管理的计算机应用研究[J].电脑采购,2023(9):23-25.

[5]胡狄.基于网络信息安全技术管理的计算机应用研究[J].数码世界,2021(1):274-275.