大数据时代下计算机网络安全及防范措施

李 可 武 凯 唐懋钧 王 力 谢 梅
北京计算机技术及应用研究所 北京 100854

摘 要：大数据时代，计算机网络安全成为守护数据价值、维护社会秩序的关键。然而，数据泄露、网络攻击形式多样化及网络设备与软件漏洞等威胁日益严峻。为应对这些挑战，需采取数据加密技术、网络访问控制及入侵检测与防御系统等防范措施。同时，加强数据加密与传输安全、建立安全运维体系及制定应急响应计划也至关重要。这些措施旨在确保数据安全、提高网络安全防御能力，并构建安全可靠的数字生态环境，以应对大数据时代的网络安全挑战。

关键词：大数据时代；计算机网络；安全防范；措施

引言：在大数据时代，计算机网络安全成为维护数据价值、保障社会秩序和促进数字经济发展的基石。然而，随着数据量的激增，网络安全面临前所未有的挑战，包括数据泄露风险、网络攻击形式多样化以及网络设备与软件漏洞等。这些威胁不仅影响个人隐私和企业利益，更可能危及国家安全。因此，深入探讨大数据时代下的计算机网络安全防范措施，加强数据加密、网络访问控制、入侵检测与防御等技术防护，并建立健全的应急响应机制，对于确保数据安全、构建安全可靠的数字生态环境具有重要意义。

1 大数据时代计算机网络安全的重要性

在当今这个信息爆炸的时代，大数据已成为推动社会进步与经济发展的关键力量。其核心价值在于通过复杂而精细的分析手段，从浩瀚无垠、类型繁多的数据海洋中提炼出具有深刻洞察力的信息和知识，为政府决策、企业经营、科学研究乃至个人生活提供强有力的智力支撑。然而，大数据的双刃剑特性不容忽视：一方面，它是创新与效率的源泉；另一方面，其蕴含的海量敏感信息，如个人隐私、企业核心机密乃至国家安全战略数据，一旦泄露或被恶意利用，将可能引发严重的社会问题乃至国家安全危机。因此，计算机网络安全在大数据时代背景下显得尤为重要，它是守护数据价值、维护社会秩序、促进数字经济健康发展的基石。（1）计算机网络安全是大数据合法合规使用的前提。在数据的全生命周期——从采集、存储、处理到传输和应用，每一步都必须严格遵循法律法规，确保数据主体的合法权益不受侵犯。网络安全技术，如加密技术、访问控制机制、数据脱敏处理等，为数据的合法收集与处理提供了技术保障，有效防止了未经授权的访问和数据滥用，确保了数据活动的合规性。（2）网络安全是维护数据完整性的关键。数据的完整性意味着数据在传输或存储过程中未被篡改或损坏，这是数据分析和决策有效性的基础。通过实施强有力的网络安全措施，如采用哈希校验、数字签名等技术手段，可以及时发现并阻止数据篡改行为，保障数据的真实性和可靠性，为大数据应用提供坚实的基础。（3）保密性是大数据安全的核心要素之一。对于涉及个人隐私、商业秘密及国家机密的数据，必须采取严格的保密措施，防止数据泄露给未经授权的第三方[1]。这要求构建多层次、立体化的安全防护体系，包括但不限于防火墙、入侵检测系统、安全审计等，确保数据在存储和传输过程中的高度保密性。（4）计算机网络安全还关乎数据的可用性。在保障数据安全和隐私的前提下，确保数据能够高效、便捷地被授权用户访问和使用，是大数据价值实现的关键。通过优化网络安全策略，如实施细粒度的访问控制、采用分布式存储和计算技术等，可以提高数据处理效率，降低因安全限制导致的服务中断风险，促进大数据资源的有效开发和利用。

2 大数据时代计算机网络安全面临的威胁

2.1 数据泄露风险

大数据环境下，数据的集中存储与频繁流动使得数据泄露成为一大隐忧。企业为了高效处理和分析海量数据，往往构建复杂的数据库系统，而这些系统一旦存在漏洞或管理不当，便可能成为黑客攻击的目标。例如，系统配置不当、权限管理不严、员工安全意识薄弱等因素，都可能为黑客提供可乘之机，导致敏感数据如客户身份信息、交易记录等被非法获取。此外，随着云计算技术的普及，越来越多的企业选择将数据迁移至云端，以享受弹性扩展、成本节约等优势。然而，云服务提供商的安全防护措施若不到位，或用户在使用云服务时未能遵循最佳安全实践，都可能引发数据泄露事件。云存

储的开放性特征，使得数据在传输、存储过程中面临更多潜在的安全威胁，如数据截获、篡改、删除等。

2.2 网络攻击形式多样化

大数据时代的到来，不仅促进了数据量的激增，也催生了新型网络攻击手段，使得网络安全防御更加困难。分布式拒绝服务（DDoS）攻击便是其中的典型代表。攻击者通过控制大量“僵尸”设备（如被感染的计算机、物联网设备等），同时向目标服务器发送大量请求，以耗尽其资源，导致服务中断。这种攻击方式不仅规模大、隐蔽性强，而且难以追踪攻击源头，给目标系统带来极大的威胁。此外，高级持续性威胁（APT）攻击也日益猖獗。APT攻击者通常具备较高的技术水平和长期潜伏的能力，他们通过精心设计的攻击链，逐步渗透进目标网络，持续窃取敏感数据而不易被察觉[2]。这类攻击往往针对特定的高价值目标，如政府机构、大型企业等，其危害性和持续性远超一般网络攻击。恶意软件的进化同样不容忽视。勒索病毒等新型恶意软件，以其快速传播、加密用户数据并索要赎金的方式，给全球范围内的企业和个人用户带来了巨大损失。这些恶意软件不仅破坏性强，而且往往利用系统漏洞或社会工程学手段进行传播，使得防御工作更加复杂。

2.3 网络设备与软件漏洞

随着计算机网络技术的快速发展，网络设备和软件的更新换代速度加快，但同时也带来了新的安全隐患。在开发过程中，由于时间压力、技术限制或设计缺陷，网络设备和软件往往难以避免地存在一些漏洞。这些漏洞可能成为黑客入侵的入口，威胁整个网络系统的安全。例如，操作系统的安全补丁更新不及时，可能导致已知漏洞被黑客利用；网络路由器的配置错误或存在弱密码，可能使网络门户大开；一些应用程序在追求功能多样性和便捷性的同时，忽视了安全设计，存在缓冲区溢出、SQL注入等常见漏洞，使得用户在使用过程中面临数据泄露和恶意攻击的风险。面对这些挑战，加强网络安全防护显得尤为重要。企业需建立健全的网络安全管理体系，加强员工安全意识培训，定期更新系统和软件补丁，采用先进的加密技术和访问控制机制，以及建立应急响应机制，以应对可能发生的网络安全事件。同时，政府和相关机构也应加强监管和指导，推动网络安全技术的研发与应用，共同构建安全可靠的数字生态环境。

3 大数据时代计算机网络安全防范措施

3.1 数据加密技术

数据加密是保护数据安全的核心手段之一。（1）在大数据时代，数据加密技术的应用显得尤为重要。通过对敏感信息进行加密处理，可以确保数据在存储和传输过程中的安全性，防止数据泄露和非法访问。（2）数据加密技术主要分为对称加密和非对称加密两种。对称加密算法，如AES（高级加密标准），以其高效性和安全性得到了广泛应用。在数据存储时，采用对称加密算法对数据进行加密，可以确保数据在本地存储介质上的安全性。然而，对称加密的密钥管理是一个难题，因为密钥需要在通信双方之间安全地共享。这时，非对称加密技术，如RSA（Rivest-Shamir-Adleman）算法，就发挥了重要作用。非对称加密使用一对公钥和私钥，公钥用于加密数据，私钥用于解密数据[3]。在数据传输过程中，双方可以使用非对称加密算法进行密钥交换，确保密钥的安全传输，然后再使用对称加密算法对数据进行加密传输，以提高传输效率和安全性。（3）为了进一步提高加密的安全性，应定期更新加密密钥。密钥的更新周期应根据数据的敏感程度、系统的安全需求以及密钥管理的复杂性来确定。通过定期更新密钥，可以降低密钥被破解的风险，提高数据加密的安全性。

3.2 网络访问控制

网络访问控制是保障网络安全的重要措施之一。（1）通过建立严格的网络访问控制机制，可以根据用户的身份、角色和权限，对其访问网络资源进行精细化管理。这不仅可以防止未经授权的访问，还可以防止内部人员越权访问敏感数据，从而降低网络攻击的风险。（2）为了实现精细化的网络访问控制，应采用多因素身份认证技术。多因素身份认证技术结合了多种身份验证方式，如密码、指纹、动态验证码等，提高了身份验证的准确性和安全性。通过多因素身份认证，可以确保只有经过合法验证的用户才能访问网络资源，从而有效防范网络攻击。（3）还应设置防火墙来阻止外部非法网络访问。防火墙可以对进入内部网络的流量进行监控和过滤，防止恶意流量进入内部网络。同时，对内部网络访问也应进行监控和过滤，防止内部人员利用漏洞进行越权访问。通过防火墙的设置，可以构建一个安全的网络边界，保护内部网络免受外部威胁。

3.3 入侵检测与防御系统

入侵检测与防御系统（IDS/IPS）是保障网络安全的重要工具之一。通过实时监控网络流量和系统行为，IDS能够及时发现网络中的异常流量和潜在的入侵行为，并发出警报。IPS则可以在检测到入侵时自动采取相应的防御措施，如阻断攻击源、隔离受感染设备等。在大数据时代，IDS/IPS面临着新的挑战。随着攻击手段的不断变化和复杂化，传统的基于规则的检测方法已经难以应对

新型攻击手段。因此，应采用大数据分析技术来提高IDS/IPS的识别能力。通过大数据分析技术对网络数据进行深度挖掘和分析，可以发现潜在的异常行为和攻击模式，并及时更新防护规则。这不仅可以提高IDS/IPS的准确性和效率，还可以增强其对新型攻击手段的防御能力。

4 深化技术防护与应急响应

4.1 加强数据加密与传输安全

在大数据时代，数据是企业和组织的核心资产，其安全性直接关系到业务的连续性和用户的信任。因此，加强数据加密与传输安全是防范数据泄露和非法访问的首要任务。（1）采用先进的加密算法对敏感数据进行加密处理，是确保数据安全的基础。对称加密和非对称加密技术的结合应用，既保证了数据传输的保密性，又实现了密钥管理的便捷性。在此基础上，实施端到端加密，即数据从发送方到接收方的整个传输过程中始终处于加密状态，即使数据在传输过程中被截获，也无法被未授权方解密和篡改[4]。这不仅增强了数据的机密性，还保障了数据的完整性和真实性。（2）随着量子计算技术的快速发展，传统加密算法面临被破解的风险。因此，研究和应用量子安全加密算法，如量子密钥分发等，是未来数据加密技术的重要发展方向。

4.2 建立安全运维体系

安全运维体系是保障网络安全的重要支撑。通过定期对系统进行安全检查和漏洞扫描，可以及时发现并修复潜在的安全隐患，防止黑客利用漏洞进行攻击。同时，结合日志分析、行为监控等手段，可以实时监测网络流量和系统行为，及时发现异常和可疑活动，提高安全事件的响应速度和处置能力。

在安全运维体系建设中，还应注重自动化和智能化的应用。通过引入自动化安全工具，如安全扫描器、漏洞修复工具等，可以实现对系统安全的快速检测和修复。而智能化安全分析技术，如机器学习、人工智能等，则可以提高安全事件的识别精度和响应效率，降低误报和漏报率。

4.3 制定应急响应计划

应急响应计划是应对网络安全事件的重要保障。它明确了应急响应的组织结构和职责，制定了应急响应流程，确保在发生安全事件时能够迅速响应、有效处置。在制定应急响应计划时，应充分考虑各类安全事件的场景和处置策略，包括数据泄露、网络攻击、系统瘫痪等。同时，建立应急资源库，包括应急工具、专家团队、备份数据等，为应急响应提供必要的资源和支持。此外，定期组织应急演练也是提升应急响应能力的重要手段。通过模拟真实的安全事件场景，检验应急响应计划的可行性和有效性，发现并改进存在的问题和不足。同时，应急演练还可以增强员工的应急意识和协作能力，提高整体应急响应水平。

结束语

综上所述，大数据时代计算机网络安全的重要性不言而喻，它不仅是数据合法合规使用的前提，更是维护数据完整性、保密性和可用性的关键。面对数据泄露风险、网络攻击形式多样化以及网络设备与软件漏洞等威胁，我们必须采取切实有效的防范措施，如数据加密技术、网络访问控制以及入侵检测与防御系统等，来筑牢网络安全防线。同时，深化技术防护与应急响应机制，加强数据加密与传输安全，建立安全运维体系，制定应急响应计划，也是提升网络安全防护能力的重要途径。只有不断适应网络安全形势的发展变化，持续优化和完善网络安全策略，我们才能确保大数据时代的网络安全，为数字经济的健康发展提供有力保障。

参考文献

[1]杨锋.计算机网络通信与网络服务体系搭建[J].计算机光盘软件与应用,2020,(15):21-63.

[2]徐海军.大数据时代计算机网络安全防范研究[J].信息安全,2019,(12):194.

[3]朱秋海.大数据时代计算机网络信息安全问题研究[J].信息与电脑（理论版）,2019,31(23):200-201.

[4]李宇泰.大数据时代计算机网络信息安全防护策略[J].无线互联科技,2019,16(23):22-23.