 DOI: https://doi.org/10.12349/iser.v6i1.4479

Discussion on computer network information security and prevention strategy in the background of big Data

Nan Yu

Zhongyi Tietong Co., Ltd., Jiangsu Branch, Nanjing, Jiangsu, 210000, China

Abstract

Thanks to the rapid development of information technology, big data has become an important force to promote social progress and economic development. However, the problem of computer network information security is becoming increasingly prominent with the wide application of big data technology, and has become the focus of global attention. While threatening personal privacy and corporate secrets, computer network information security incidents such as network attacks, data leakage and privacy infringement occur frequently, which also pose a serious threat to national security. Therefore, it is of great significance to ensure the security of information resources and maintain the stability of network space, and to discuss the information security and prevention strategies of computer network under the background of big data. It is expected that the research of this paper will provide valuable reference for people in related fields to jointly promote the development of computer network information security technology and build a more secure digital world.

Keywords

big data; computer network; information security; problem; prevention strategy; discussion

大数据背景下计算机网络信息安全及防范策略探讨

于楠

中移铁通有限公司江苏分公司，中国 · 江苏 南京 210000

摘　要

得益于信息技术迅猛发展，大数据成为推动社会进步和经济发展的重要力量。但计算机网络信息安全问题也随着大数据技术的广泛应用而日益突出，并成为全球瞩目的焦点。在威胁个人隐私和企业机密的同时，网络攻击、数据泄露、隐私侵害等计算机网络信息安全事件频发，也对国家安全构成严重威胁。因此，保障信息资源安全以及维护网络空间稳定，就大数据背景下探讨计算机网络信息安全与防范策略意义重大。期望通过本文的研究，为相关领域的人员共同推动计算机网络信息安全技术的发展以及构建更安全的数字世界提供有价值的参考。

关键词

大数据；计算机网络；信息安全；问题；防范策略；探讨

1 大数据背景下计算机网络信息安全防范意义

随着信息技术的飞速发展，尤其是大数据、云计算及人工智能等技术的广泛应用，计算机网络信息安全的挑战愈加严峻。大数据背景下，数据量、数据种类及其处理的复杂性都达到了前所未有的程度，这使得传统的网络安全防护措施面临极大的压力。大数据背景中的信息安全不仅关系到企业的商业秘密与数据隐私，也涉及社会、国家的安全与稳定。大数据的快速增长和多样化为信息安全防护带来了新的挑战 [1]。首先，大数据的收集和存储往往跨越多个平台与系统，传统的安全防护策略往往侧重于单一环境，无法有效应对跨平台的安全威胁。其次，数据的共享与交换使得安全漏洞的传播路径更为复杂和难以控制，攻击者通过各种手段入侵并窃取敏感数据的风险增加。再者，数据本身的种类和结构复杂，如何在庞大而多样的数据中精准筛选出潜在的安全威胁，成为一项巨大的技术挑战。因此，面对大数据带来的信息安全风险，必须采取更加科学、系统的防护措施，以确保信息的完整性、保密性和可用性。

【作者简介】于楠（1979–），男，中国江苏南京人，本科，助理工程师，从事网络信息安全研究。

2 大数据背景下计算机网络信息安全面临的主要问题

2.1 数据存储和传输中的安全隐患

在大数据背景下，计算机网络信息安全的核心环节就是数据的存储和传输。但是，传统的存储技术和加密机制已经不能在数据量越来越大的情况下有效地保证数据的安全。

大数据的存储一般分布在多个数据中心或云平台上，如此一来在存储过程中数据的安全问题也会变得更为复杂。即数据的加密、访问控制及备份措施等多个方面难以实现全面覆盖，特别是数据存在多平台间传送情况，可能会有未加密的传送路径，这样一来极易发生数据传送过程中被攻击者盗取或篡改。另外，数据存储中也存在着安全管理问题。结合实践来看，大数据通常包含着大量非结构化和结构化数据，在这种情况下怎么样对它们开展有效地分类、标记和保护便成为数据安全中的关键问题。一旦存储介质受到恶意攻击或是物理损坏将会造成大量敏感信息的泄露，从而对企业或个人隐私安全构成严重危害。

2.2 大数据分析中的隐私泄露问题

从海量数据中提取有价值的信息是大数据分析技术的核心，但与此同时，隐私保护在数据分析中的问题也越来越凸显。大数据分析过程中，数据的匿名化、去识别化处理并非百分百安全，只需通过数据挖掘技术使用户身份信息得以恢复，因而隐私泄露的可能性是存在的。特别是数据泄露的风险，在与第三方平台共享、交换数据时更容易出现 [2]。比如大量涉及个人敏感数据的医疗、金融等行业，如果其数据不妥善处理或存储会造成严重的隐私侵害后果发生。虽然大数据分析提供精准预测和个性化服务，但相应的其被不法分子借助数据分析窃取用户隐私数据的概率大大增加。隐私数据泄露在给个人造成损害的同时，更有可能对整个行业乃至社会带来广泛负面影响。

2.3 大数据平台的安全漏洞

大数据技术发展到今天，凭借着自身独特优点利用其平台处理分析海量信息的企业和组织越来越多。但这些平台通常由若干个复杂程度较高的部件及技术组成，这就意味着在不同环节中容易产生安全漏洞。特别是采取开放式设计大数据平台会因系统更新、防护软件等更新不及时出现很多安全漏洞，它们便成为潜在的攻击点。不法分子在攻击大数据平台时通常会利用这些安全漏洞开展针对性攻击，以达到窃取或篡改数据目的。而若大数据平台被攻破，由于其中涉及海量数据造成的损失将是灾难性的。另外，大数据平台中访问权限若存在管理不当或者身份认证机制不健全，也为攻击者提供了一个可乘之机。因此，如何加强大数据平台的安全性，防止被不法分子通过各种漏洞进行攻击是目前面临的一大挑战。

3 大数据背景下计算机网络信息安全问题的防范策略

3.1 强化数据存储和传输中的安全措施

为了保证数据的安全性，在大数据的存储与传输过程中首先要采用多层次的安全防护措施。为了保证数据在静态存储状态下的安全，数据加密是第一技术手段，计算机网络可以采用 AES-256 等符合行业标准的加密算法。另外在数据传送的时候，为了防止数据外泄和篡改，计算机网络除了继续使用传统的 SSL/TLS 协议（该协议已包含基于公钥加密和数字证书的身份验证机制）外，还可以探索和应用其他先进的端对端加密技术，以满足特定场景下的安全需求。同时，可以强化身份验证机制，如实现严格的双向身份验证，以进一步提高通信的安全性。为了进一步提高访问控制的精确性，同时又须保证只有合法用户可以访问数据，就必须结合多方面的身份认证技术。在用户身份验证后，计算机系统会以最小权限原则实施严格的权限分配，对用户的访问行为进行动态监控，同时内部和外部潜在威胁及时进行识别和防范 [3]。除了强化加密措施以外，数据备份与恢复同样关键。对此，我们可以以下几个方面着手，先要选择增量备份、差异备份等高效可靠的备份策略，在保证备份数据与原始数据采用相同加密算法进行保护的同时，定期将重要数据存储到不同的物理位置或云端上，以防止不法分子在获取数据后对备份数据进行破坏。除常规备份外，异常情况下建立数据恢复的清晰流程，确保数据在紧急情况下能较快恢复到正常业务操作状态。另外，考虑单点失效的可能冲击，采用分散式存储系统是重要的降低此类风险的重要手段。同时通过在多个节点分散数据存储时，实行数据冗余技术，可以有效避免由于某一节点故障而造成的所有数据丢失或者泄露。同时针对存储系统的安全性，除了硬件保护之外，还要定期对存储系统进行漏洞扫描和修复，确保计算机系统没有安全漏洞。最后，计算机网络中诸如防火墙、入侵侦测系统（IDS）、入侵防御系统等网络安全软件都需要与数据存储和传输方案紧密集成，以实时安全监控和威胁识别。同时为了提高计算机网络整体安全性，我们还可以采用人工智能和机器学习技术，如深度学习算法（如卷积神经网络 CNN、循环神经网络 RNN）或监督学习算法（如支持向量机 SVM、随机森林 RF），实时审计数据访问日志对潜在非正常活动进行识别，以及时做相应处理避免数据泄露或被破坏。另外，在数据存储和传输的全过程中，为了避免不必要的敏感信息泄露，应该始终坚持数据最小化原则，计算机网络只有对必要的数据进行存储和传送。

3.2 提升大数据分析中的隐私保护能力

大数据分析中，计算机网络信息安全要对数据处理与分析过程采取多层次措施，从而保证用户个人隐私信息得到有效保护。首先，数据去标识化与匿名化技术是隐私保护手段的基础，特别是通过删除或替换数据中的可辨识信息（如：姓名、身份证号等），这样计算机网络在处理用户个人数据时能够确保其无法追溯到具体个人，从而达到隐私保护目的。另外，为了保证数据的隐私性，计算机网络仍须严格按照数据最小化的原则，即只对分析和采集与任务有关的数据集，避免其他与任务不相关的敏感信息被采集和存储。采用同态加密技术、加密计算等针对医疗、金融等涉及高隐私领域的数据进行加密处理，这能够对隐私数据进行有效保护。

比如，同态加密技术的应用可以直接在已经被加密的数据上进行计算，而不需要解密，这样在处理过程中便可避免了数据所暴露出来的危险性；加密计算则先是进行数据加密处理后再执行分析任务，如此一来即便不法分子在任务分析过程中攻击获取到部分数据，但重要的敏感数据却不能被读取或者恢复。与此同时，计算机网络中还需引入精细的访问控制机制和数据审核功能，以增强数据共享过程中的隐私保护[4]。计算机网络每次数据分享或交换都要经过严格的权限验证，确保只有经授权的用户才能访问数据，同时为杜绝未经授权的数据外泄情况发生，计算机网络还需对数据共享过程中要对数据进行实时监控记录数据使用日志。最后，计算机网络还应当利用差分隐私技术，为数据分析提供隐私保障。简单而言，通过在数据分析结果中加入噪声以及模糊处理敏感字段等手段，确保即使计算机网络中存在多个数据访问者共同分析时，单个用户隐私信息仍能得到有效的保护不被揭示出来。另外，计算机网络采用数据脱敏技术通过对敏感字段进行模糊处理，这样避免在数据显示或生成相关报告时有效降低隐私外泄风险，从而最大程度地保护用户隐私信息不被泄露。

3.3 加强大数据平台的漏洞修复与安全防护

针对计算机网络中大数据平台存在的安全漏洞，我们可以实行以下几方面防范策略。一是为发现计算机系统中潜在的网络漏洞而定期开展大数据平台组件安检工作。这一过程既包括对计算机操作系统、数据库及应用程序的审查，也包括扫描第三方插件、数据库的漏洞工作。同时为促使漏洞检测的效率及精确性都将得到提高，我们还可以引入自动化的安全测试工具。二是在大数据平台的安全架构中设计包括入侵检测系统（IDS）、入侵防御系统（IPS）在内的多层防护机制，以实现从外部威胁的角度对平台防线进一步增强。这样一来计算机网络的大数据平台便可以借助设置不同层次的保护来有效阻止 DDoS 攻击、SQL 注入等多种攻击类型。三是针对大数据平台的计算机网络接入控制必须实行严格的身份认证机制，其中包含多种身份验证方式，包括多因素认证（MFA）以及用户名、密码、指纹、动态口令等多种身份的验证方式，确保只有授权用户才能对平台数据进行访问[5]。同时，为了进一步降低潜在的安全隐患，平台要采用基于角色的访问控制策略，保证用户在权限范围内可以访问相应的数据和服务。四是 API 安全设计也是大数据平台安全防护中的关键一环，平台应采用 API 网关，以主流安全协议（如 OAuth 2.0）和 JWT（JSON Web Token）的安全验证为基础，实施基于 HTTPS 及 JWT 的安全验证，避免数据访问和未经授权操作。五是为了提高大数据平台的实时安全监控能力，我们在计算机网络中应用人工智能和机器学习技术对平台中相关行为开展实时监控和分析。比如，我们通过对计算机网络开展机器学习模型的训练，使用像 GPT、BERT 等预训练大模型，并在安全数据集上进行微调，能够有效识别非正常流量、权限滥用等异常行为，并对潜在的安全威胁进行快速反应。另外，大数据平台还应建立安全事件响应的灵活机制，这能确保一旦发现计算机网络漏洞或安全事件出现就能很快定位问题并实施修复操作。

4 结语

综上所述，计算机网络信息安全面临的挑战在大数据技术不断进步和应用领域深入背景下日益扩大。通过对当前计算机网络信息安全所面临的主要问题及其在大数据背景下的防范策略展开分析可以看出，信息安全不单单是技术层面的问题，更重要的是管理、法律以及伦理等多方面问题的综合反映。因此大数据时代信息安全所带来的挑战，只有通过强化技术、管理、法律等多方面的共同努力才能得到有效的应对。

参考文献

[1] 孙玮.大数据背景下计算机网络信息安全及防范策略研究[J].数字通信世界, 2022(12):169-171.

[2] 钱利君.大数据背景下计算机网络信息安全与防护策略探析[J].商情, 2023(17):0149-0152.

[3] 李华龙,陈力超.大数据时代的计算机网络信息安全问题及防范策略[J].中文科技期刊数据库（全文版）工程技术, 2023.

[4] 杜永聚.大数据背景下的计算机网络信息安全问题及防护措施[J].Electronic Communication & Computer Science, 2022, 4(5).

[5] 任剑洪,郭子军.大数据背景下的计算机网络安全及防范策略[J].信息产业报道, 2023(11):0034-0036.