大数据时代计算机网络安全技术及防范措施

康小宇

蒙古民族大学（Mongolian National University）,蒙古国·乌兰巴托 99909715141

【摘 要】当前，大数据技术已经深度融入社会生产生活的各个领域，以海量的数据规模、高速的数据流转、多样的数据类型为经济发展、科技创新和民生改善注入了强劲动力。然而，大数据在释放巨大潜能的同时，也使计算机网络安全面临前所未有的严峻考验。本文分析了大数据时代常见的计算机网络安全技术，探讨了有效的防范措施，旨在为相关工作提供帮助，构建安全、高效、健康的网络生态。

【关键词】大数据时代；计算机网络；安全技术；防范措施

引言：

随着物联网、云计算、人工智能等技术和大数据的深度融合，计算机网络的数据交互规模持续增长，网络架构日益复杂，给网络安全风险的滋生和蔓延提供了条件。海量的数据汇聚打破了传统数据存储的边界，不同来源、不同类型的数据混杂在一起，增加了数据分类管理的难度，扩大了安全漏洞的排查范围。同时，大数据技术的发展也为黑客提供了更先进的攻击工具和方法，攻击者可以利用大数据分析技术挖掘网络薄弱环节，制定针对性的攻击策略，破坏力大，隐蔽性高，传统的安全防护体系难以应对。因此，探究大数据时代的计算机网络安全技术和防范措施，是保障数字经济健康发展，维护社会稳定的当务之急。

1 大数据时代常见的计算机网络安全技术

1.1加密技术

加密技术是通过特定算法将明文数据转换为不可直接读取的密文，仅授权主体凭借密钥才能解密还原的技术。

加密技术主要覆盖数据传输和存储两大环节。在数据传输过程中，常用的SSL/TLS协议可以对客户端和服务器之间的数据流进行实时加密，防止数据在网络传输中被窃听或者篡改。在数据存储环节，针对大数据分布式存储的特点，主要应用透明加密技术（TDE），该技术可以对数据库、数据仓库中的数据进行实时加密，即使存储设备被盗，非法获取者也不能读取加密数据。

大数据时代的加密技术分为对称加密和非对称加密。对称加密以同一密钥进行加密解密，加密速度快、效率高，适用于海量数据的加密处理。非对称加密以公钥加密、私钥解密的方式运作，安全性更高，不用担心密钥传输过程中的泄露风险。

1.2访问控制与身份验证

访问控制与身份验证是防范非法访问的关键技术，通过“确认身份合法性—限制访问权限”的流程，确保只有授权主体能访问特定数据，避免数据被越权查看、篡改或者删除。

身份验证是访问控制的前提，在大数据时代，身份验证已经从传统的单因素验证升级为多因素验证，通过结合密码、生物特征、硬件令牌等多种身份验证方式提升安全性。此外，基于大数据分析的行为验证技术也在逐渐普及，该技术通过分析用户的历史行为特征，判断当前的访问行为是否异常，防范账号被盗用后的非法访问[1]。

访问控制是在身份验证通过后，根据预设的规则限制用户的访问权限，核心在于“最小权限原则”，避免权限过度授予导致的数据风险。在大数据场景中，访问控制已经从“角色-Based访问控制”升级为了“属性-Based访问控制”，即结合用户属性、数据属性以及环境属性动态分配权限，提升了精细化程度。

1.3数据脱敏与匿名化

数据脱敏与匿名化技术的目的是保障数据“可用不泄密”，通过处理数据中的敏感信息，在保留原有格式和分析价值的同时，消除其识别个人或者实体的能力。

数据脱敏技术分为静态脱敏和动态脱敏，静态脱敏是在数据脱离生产环境前对敏感信息进行永久性处理，处理后的数据可以用于非生产场景；动态脱敏是在数据实时访问的过程中，根据用户权限动态隐藏敏感信息，同一数据对不同权限用户呈现不同形态。

数据匿名化技术通过去除或者替换数据中的标识信息，使数据无法关联到特定的个人或者实体，常见的方式包括删除标识字段、随机化处理、泛化处理等。删除标识字段是直接移除数据中的姓名、身份证号等显性标识，只保留年龄、职业等非标识信息；随机化处理是在随机替换标识信息的同时保持数据的统计特征不变；泛化处理是把精确的数据转化为模糊范围数据，确保数据不能精准定位到个人。

2 大数据时代计算机网络安全防范措施

2.1培养网络安全意识

首先，在企业和组织层面，要建立常态化的安全培训机制，结合大数据场景下的典型案例，定期开展安全知识讲座、技能培训和应急演练，让员工清晰认识到自身行为和数据安全的联系[2]。同时，还要制定明确的安全行为规范，明确员工在数据处理中的禁止行为，通过考核机制确保规范落地，让安全意识融入日常的工作习惯。

其次，在个人层面，要提升保护数据隐私的意识，避免因个人行为疏忽导致的安全风险。比如不要随意点击陌生链接、不下载来源不明的软件，防止设备被植入恶意程序；不在多个平台使用相同的账号密码，降低因单个平台泄露导致的连锁风险；谨慎授权APP的权限，避免过度授权导致个人信息被非法收集。此外，个人还要关注有关数据安全的法律法规，了解自身的数据权益，在遭遇信息泄露时可以及时采取维权措施，树立起主动防范、主动维权的意识。

2.2合理应用云计算技术

首先，选择具备完善安全资质的云服务商，优先考虑通过ISO27001信息安全认证、符合国家《云计算服务安全评估办法》的服务商，确保其拥有健全的安全防护体系。此外，利用云计算的弹性扩展特性，根据数据规模动态调整安全资源，在数据访问的高峰期增加防火墙节点、提升入侵检测系统的算力，确保安全防护能力和业务需求的精准匹配。

其次，构建“混合云”或者“多云”架构，避免把所有的数据集中存储在单一的云平台里，降低单点故障风险。比如，企业可以把非敏感数据存储在公有云，把核心敏感数据存储在私有云，通过云间数据同步技术备份多个平台的数据，在某一云平台遭遇攻击或者出现故障时，能够快速从其他平台恢复数据，确保业务的连续性。同时，要加强对云平台自身的安全管理，定期对云账号权限、安全配置进行审计，及时发现并修复配置漏洞，避免由于云平台管理疏漏引发安全风险。

2.3强化网络系统安全监控

首先，部署多维度的监控工具，覆盖网络流量、设备状态、数据操作、用户行为等场景。利用网络流量监控工具实时分析网络数据包，识别异常流量并自动触发拦截机制；通过服务器监控工具实时监测服务器的CPU使用率、内存占用、磁盘空间等指标，及时发现由于恶意程序占用资源导致的性能异常[3]。同时，整合各个监控工具的数据，构建统一的监控平台，实现对网络系统的全局可视化管理。

其次，引入人工智能和大数据分析技术，提升监控的智能化水平。通过训练AI模型分析历史安全数据，让系统具备识别新型攻击模式的能力；通过大数据关联分析，发现分散在不同监控维度中的碎片化风险信号。此外，还要建立分级预警机制，根据风险等级制定不同的响应策略，自动处理低风险事件，中高风险事件第一时间推送给安全团队，确保响应及时。

2.4加强电脑网络系统的维修管理

首先，组建专业的维修团队，确保成员具备扎实的网络技术和安全知识，能够快速定位并解决硬件和软件故障。在维修过程中，要严格遵守安全规范，维修前对涉及敏感数据的设备进行数据备份和加密，维修时使用正版的配件和软件，维修后对设备进行全面的安全检测。同时，建立维修档案，记录每次维修的设备信息、故障原因、解决方案和维修时间，为后续追溯和分析故障规律提供参考。

其次，完善系统配置管理，制定统一的配置标准，避免因配置不一致导致的安全漏洞。定期对系统配置进行审计，利用自动化工具对比当前配置和标准配置的差异，及时修正违规配置。同时，加强账号和权限管理，遵循最小权限原则，给用户分配账号权限，定期对账号进行清理，避免僵尸账号被利用[4]。

3 结语

综上所述，作为数字经济时代的核心生产要素，大数据价值的释放离不开安全的保障，网络安全的水平和数字化转型的深度息息相关。在具体的工作实践中，要充分发挥加密技术、访问控制与身份验证、数据脱敏与匿名化等网络安全技术，从培养网络安全意识、合理应用云计算技术、强化网络系统安全监控、加强电脑网络系统的维修与管理等方面入手对安全风险进行有效防范。从而为数字经济的健康发展和社会的稳定运行提供坚实保障，让大数据技术在安全的环境中充分释放价值，更好地服务于人类社会的发展进步。

参考文献：

[1]陈静.大数据时代的计算机网络安全技术及防范措施探讨[J].科技与创新,2025,(19):98-100+104.

[2]厉彦波.探究大数据时代的计算机网络安全及防范措施[J].信息与电脑(理论版),2024,36(11):103-106.

[3]徐琳娜.大数据时代下计算机网络安全与防范措施分析[J].信息与电脑(理论版),2024,36(11):180-182.

[4]周爽,吕宝海.试析大数据时代的计算机网络安全及防范措施[J].信息与电脑(理论版),2024,36(08):207-209.

作者简介：

康小宇（1992.8-），男，民族：汉族，籍贯：内蒙古巴彦淖尔，学历：硕士在读，职称:工程师，研究方向：计算机网络安全。