大数据时代计算机网络安全技术及防范措施探讨

余嘉怡

西安科技大学 高新学院，陕西 西安 710300

DOI: 10.61369/TACS.2025090003

摘　　要： 大数据时代，计算机网络成为信息交互与数据存储的核心平台，其安全性面临诸多挑战。本文聚焦大数据时代计算机网络安全，深入探讨加密技术、访问控制与身份验证、数据脱敏与匿名化等关键安全技术，并从安全防护、监测、反应及恢复四个维度提出针对性防范措施，旨在为构建安全可靠的计算机网络环境提供理论支撑与实践指导。

关 键 词： 大数据时代；计算机网络安全；安全技术；防范措施

Exploring Computer Network Security Technologies and Preventive Measures in the Big Data Era

Yu Jiayi

High-Tech College, Xi'an University of Science and Technology, Xi'an, Shaanxi 710300

Abstract: In the era of big data, computer networks have become the core platform for information exchange and data storage, facing numerous security challenges. This paper focuses on computer network security in the big data era, delving into key security technologies such as encryption techniques, access control and authentication, data de-identification, and anonymization. It proposes targeted preventive measures across four dimensions—security protection, monitoring, response, and recovery—aiming to provide theoretical support and practical guidance for building a secure and reliable computer network environment.

Keywords: big data era; computer network security; security technologies; preventive measures

引言

随着大数据技术的飞速发展，随着计算机网络的普及和社会生活的方方面面，数据规模呈现爆炸性的增长，网络环境也变得越来越复杂。互联网上海量数据的传播和存储，既具有重要的经济和社会意义，又是许多犯罪分子垂涎的目标。随着数据泄漏和网络攻击等事件的发生，计算机网络的安全问题越来越突出，给个人、企业甚至国家造成了巨大的损失。为此，对大数据环境下的计算机网络安全问题进行深入地研究，并提出相应的对策，具有重要的现实意义与紧迫性。

一、大数据时代计算机网络安全技术

（一）加密技术

加密技术是保证信息安全的重要方法，在大数据时代背景下，数据以电子方式在互联网上流通，容易被盗取、篡改。对称加密算法采用同一密钥，加密和解密都是一种高效的加密方法，适合于海量数据的快速加密。非对称加密算法基于公钥和私钥相结合的不对称密码体制，通过公开密钥和私有密钥进行加密，可以实现密钥的加密和解密，从而可以很好地解决密码体制中的密钥分配和管理问题，在数字签名和保密电子邮件等方面具有广阔的应用前景。哈希算法通过不可逆转换产生一个定长的哈希值来检验数据的完整性，从而保证了在传送过程中没有被篡改[1]。比如，在传送文件时，发送者将文件的散列值计算出来然后一起传送，接收者再次计算收到的文件的散列值，并和发送者提供的散列值进行比较，如果相同就表示该文件是完全正确的。

（二）访问控制与身份验证

访问控制和身份验证技术是阻止非法使用者对系统资源的一道重要防线，访问控制通过制定严格的访问策略，限制用户对系统资源的访问权限，即通过建立一套有效的网络安全机制来实现对网络资源的有效访问。基于角色的存取控制（RBAC）通过对用户的角色进行授权，从而简化权限的管理，增强系统的安全性和管理性。比如，在一个企业的网络中，各个部门的工作人员扮演着不同的角色，比如财务人员、销售人员等，系统会按照他们的角色对其进行对应的访问，而财务人员只能够对与财务有关的数据进行存取，而对于销售人员来说，他们只能够存取与销售有关的资源。身份认证是一种对用户进行身份认证的技术，常用的认

作者简介：余嘉怡（2004.02—），女，汉族，陕西西安人，本科，研究方向：计算机科学与技术。

证方法有用户名和密码、数字证书、生物认证等等。用户名称和密码是进行身份认证的基础手段，但是也有可能被人窃取密码。电子证书是由第三方权威机构进行认证，为使用者提供了更为可信的身份认证。以指纹和人脸识别为代表的生物识别是一种基于人体特有的生物特征的认证方法，由于其高精度和高安全性，已被广泛用于高级别安防领域[2]。

（三）数据脱敏与匿名化

数据脱敏与匿名化技术是保护数据隐私的重要手段。在大数据时代背景下，海量数据的分享与分析是必不可少的，而这些数据中往往蕴含着个人身份、健康等敏感信息。数据脱敏是将敏感数据经过形变后，既不能直接识别，又能保持数据本身的特性。比如，在不暴露使用者身份的前提下，对使用者的身份进行局部替代或加密，仅保留一些重要的资料供资料分析使用。而数据匿名化技术就是指在不确定的情况下，移除或替代数据中的直接识别信息。比如，在分享医疗数据时，去掉病人的姓名、身份证号等直接识别信息，仅保留间接识别信息（如年龄、性别、疾病类型等），既能保障病人的隐私，又能确保数据的可用性。

二、大数据时代计算机网络安全风险

（一）数据泄漏风险加剧

随着大数据时代的到来，数据逐渐成为企业的核心资产，其数量和价值都呈现出几何倍数的增长，同时也引起了不法分子的觊觎，数据泄漏的风险也随之增大。在大数据时代，数据的采集、存储、传输、处理等过程中，涉及到各个方面的利益，若在其中一个方面存在着安全缺陷，就有可能造成数据的泄漏。比如，在数据采集过程中，如果采集工具或者采集界面有安全性上的漏洞，则有可能被黑客所利用；在资料储存上，如果储存系统的安全性较低，若没有经过加密或加密算法不够强，则会造成资料被盗取或篡改。除此以外，集中式的大数据存储方式在提升数据处理效率的同时，也成了数据聚合的“靶心”，一旦被入侵就会有海量的隐私信息被窃取，如果不采取安全的传送协议或者加密机制，在公共网络上进行数据传送，很可能会被拦截、窃取。数据泄漏不但会导致个人隐私受到侵害，而且会导致诸如欺诈、身份盗用等行为，导致企业信誉受损，商业秘密泄漏，进而影响企业的竞争能力、市场地位，乃至国家安全。

（二）恶意软件攻击多样化

大数据背景下，恶意程序攻击方式日趋多样，对网络安全提出了巨大的挑战。随着大数据时代的到来，病毒、木马等传统恶意软件的演化与升级，呈现出新的蔓延模式与破坏性。比如，某些恶意程序会借助大数据平台上的脆弱性，在大数据簇内传染某些节点，并向整体簇内扩散，造成海量数据被篡改或盗取。与此同时，大数据环境下的勒索软件越来越多。勒索软件通过对用户的信息进行加密，并在解密前向用户索要一定的赎金，从而给公司和个人带来了很大的经济损失，勒索软件的攻击对象也从个人用户扩展到了企业用户以及重要的基础设施。除此以外，大数据背景下的恶意程序还表现出更加隐蔽、智能的特点，其能够利用高级密码、混淆等手段躲避安全软件的探测与拦截，长期潜伏于系统内部，搜集敏感信息，伺机发动攻击。部分恶意程序还可以通过大数据分析等手段，依据用户的行为习惯、网络环境等因素，对其进行智能调整，从而达到增强攻击的目的。

（三）网络攻击手段智能化

随着大数据、人工智能等技术的不断发展，网络攻击手段也变得越来越智能化。攻击者可以利用大数据分析技术，收集和分析目标系统的各种信息，如系统漏洞、网络拓扑结构、用户行为模式等，从而制定更加精准和有效的攻击方案。例如，通过分析用户的上网行为和登录习惯，攻击者可以猜测用户的密码或利用社会工程学手段进行诈骗。人工智能技术在网络攻击中的应用也日益广泛，攻击者可以利用机器学习算法自动生成恶意代码，这些恶意代码能够根据目标系统的环境进行自适应调整，提高攻击的隐蔽性和成功率。而且，智能化的网络攻击还可以实现自动化和规模化，攻击者可以利用僵尸网络等工具，同时对大量目标系统发起攻击，造成大规模的网络瘫痪和数据泄露事件。除此之外，智能化的攻击手段还能够对安全防护系统进行反向攻击，通过分析安全系统的规则和算法，找到其漏洞并进行绕过或破坏，使得传统的安全防护措施面临巨大挑战。

三、大数据时代计算机网络安全防范措施

（一）安全防护机制

为了保证计算机网络的安全，必须建立健全的安全保护机制。防火墙是网络的第一道防线，需要根据具体的风险评估和业务需要，设计出准确而严密的访问控制策略，对进出网络的数据流进行全方位、多层次的监测和过滤，对非法接入和各种诸如端口扫描、恶意代码传输等攻击进行准确的拦截。入侵检测系统（IDS）与入侵防御系统（IPS）需要实时、不间断地对网络数据和日志进行实时、不间断的监控，利用高级的异常检测和行为分析方法，快速地识别出异常行为，并对其进行预警或阻止其蔓延[3]。安全网关需要对各种安全功能进行很高的整合，包括对防火墙的访问控制，对入侵检测的实时预警，对病毒的查杀和防止进行保护，以建立起一个完整的安全防御系统，为用户提供全方位、无死角的安全保护。与此同时，要制定标准化的升级机制，定期更新安全装备和软件的规则库、补丁，对当前的安全威胁信息进行跟踪，对发现的安全缺陷进行修补，保证系统总是保持在最新的安全保护状态。在此基础上，构建多层安全保护框架，根据数据的敏感性和服务的重要度，对网络进行安全分区，并根据各分区的访问权限、加密方式、监控频次等特点，实现细粒度、个性化的安全管控，从而提高计算机网络的总体安全水平。

（二）安全监测机制

安全监控机制对于及时发现网络安全隐患至关重要，这就需要在整个网络上部署一个具有高准确性和实时性的数据采集系统，从不同的协议、不同的端口、不同的应用，不同的业务类型进行采集。针对 DDoS 攻击导致的异常请求流量、端口扫描导致的端口检测流量异常等问题，采用机器学习等先进的流量分析方

法，对所采集的流量进行深层次挖掘，实现对异常流量的准确挖掘。同时还可配置一套专门的系统日志监控工具，对操作系统、各种应用程序和安全装置的日志进行集中采集。通过对日志进行有效的语法分析，对日志进行结构化处理，并利用关联分析的手段，对日志中存在的不合理登录时间、登录位置、登录失败次数频繁、更改权限时没有按照审批过程进行权限设置等安全隐患进行挖掘[4]。在此基础上，将行为数据、商业规则、安全策略等多个要素有机地结合起来，建立用户与系统的常态行为模型。通过对用户及系统的真实行为进行实时监控，并利用偏差探测技术，对与常规行为模式明显背离的异常行为进行快速识别，并对员工违规访问敏感数据、越权操作等行为进行有效的检测，并对外部攻击者进行有效的检测。安全信息和事件管理（SIEM）系统要充分发挥数据集成中心的功能，对各种安全监控工具的数据进行无缝集成，采用统一的数据格式和存储模式，对数据进行统一的管理和有效的分析，给安全管理者提供完整的、统一的安全视图，帮助其迅速地找到并应对安全事故。

（三）安全反应机制

安全反应机制是企业在发生安全事故之后，能够快速有效地对企业造成的损失进行有效控制的关键。为此，要建立一套完整的、详细的安全应急方案，根据安全事件的性质、影响范围和严重性，将其分为数据泄漏事件、网络攻击事件、系统失效事件等。根据不同的突发事件，对应急过程进行细化，从发现到初步评估到应急处置，再到随后的复原，并对各个参与部门和个人的职责进行明确的划分，以保证在突发事件中能够各司其职，协同工作。在出现安全事故后，安全应急小组要按照预案快速启动反应流程，立即对事故进行评价，利用专业的技术手段和分析手段，对事故的类型、规模及可能造成的危害进行精确的判定。在此基础上，可以通过改变网络拓扑结构、关闭相关端口等方法，来迅速隔离被感染的系统，以避免攻击向其他系统或网络区域蔓延[5]。与此同时，综合采集系统日志、网络流量、攻击轨迹等数据，对事故进行分析，确定责任。通过与相关安全组织、厂商等建立密切合作机制，及时获得最新的技术支撑与威胁情报，研究制定对策，形成强有力的应急合力。在安全事故的处置中，对沟通和协调工作给予高度重视，设立有效的信息交流通道，将事故的发展动态及时通知管理层、业务部门和用户，保证信息的透明度。

（四）安全恢复机制

安全恢复机制是在安全事件处理完成后，恢复系统正常运行与数据完整性的重要保障。数据备份作为安全恢复的基石，需建立科学完备的数据备份策略。依据数据的重要程度、更新频率及业务连续性需求，确定合理的备份周期，如对于核心业务数据可进行每日全量备份与每小时增量备份。同时，将备份数据存储于安全可靠的位置，优先选择异地数据中心，利用其独立的物理环境与安全设施，有效规避本地灾难对备份数据的破坏；也可借助云存储服务，依托云服务商强大的数据冗余与容灾能力，确保备份数据的可访问性与完整性。当遭遇数据丢失或损坏时，能依据预设的恢复流程，迅速从备份中精准恢复数据，最大程度降低数据损失。系统恢复计划应详尽无遗地描述系统恢复的步骤与方法，涵盖硬件设备的精准更换，依据设备型号、规格及兼容性要求进行选型与采购；操作系统的重新安装，确保安装版本与系统配置符合安全标准；应用程序的细致配置，包括参数设置、权限分配及接口对接等。在系统恢复过程中，必须开展严格的测试与验证工作，运用功能测试、性能测试及安全测试等多种手段，全面检查系统恢复后的运行状态，确保系统稳定可靠运行，且不存在任何安全漏洞。除此之外，对安全事件进行全面深入的复盘与分析，从事件起因、攻击路径、影响范围等多个维度进行剖析，总结经验教训，针对性地完善安全防护体系，优化安全策略与流程，防止类似安全事件再次发生。

四、结束语

大数据时代，计算机网络安全技术及防范措施的研究与实践至关重要。加密技术、访问控制与身份验证、数据脱敏与匿名化等安全技术为数据安全提供了技术保障，而安全防护、监测、反应及恢复机制则构建了全方位的安全防范体系。通过不断加强安全技术研发与应用，完善安全管理制度，提升人员的安全意识与技能，能够有效应对大数据时代下的网络安全挑战，保障计算机网络的安全稳定运行，为大数据技术的发展与应用创造良好的环境。

参考文献

[1] 贺箫逸 . 人工智能在计算机网络技术中的应用研究 [J]. 信息与电脑 ,2025,37(02):92-94.

[2] 刘承军 . 关于计算机网络安全防范技术的研究和应用 [J]. 中文科技期刊数据库（全文版）自然科学 ,2024(002):000.

[3] 赵玉梅 . 计算机网络安全技术的影响因素与防范策略分析 [J]. 集成电路应用 ,2024,41(11):412-414.

[4] 王磊 . 计算机网络搭建及安全防范技术要点研究 [J]. 电子技术与软件工程 ,2023(1):56-59.

[5] 冯理明 , 王月梅 , 韩国新 . 计算机网络攻击与防御技术发展趋势研究 [J]. 电脑知识与技术 ,2024,20(33):79-81.

