 DOI: https://doi.org/10.26549/bdai.v3i4.11950

Data Network Security Strategy in the Context of Big Data

Haiqin Lu

Shanghai Energy Technology Development Co., Ltd., Shanghai, 200233, China

Abstract

With the continuous improvement of China's economic level, big data technology, as a new technology in the information age, has gradually been widely promoted and used in the field of people's production and life, which is convenient for people's life and further accelerates economic development. With the deepening of the concept of resource sharing, people are paying more and more attention to the network security problems in data governance in the process of applying big data technology, so this paper will mainly focus on data governance in the context of big data, and discuss the main strategies of network security governance through diversified analysis, so as to provide feasible suggestions for relevant staff.

Keywords

big data background; data management; cybersecurity issues; manage policies

大数据背景下数据网络安全策略

陆海琴

上海能源科技发展有限公司，中国·上海 200233

摘　要

随着中国经济水平的持续提升，大数据技术作为信息化时代的一种新型技术，逐渐在人们的生产生活领域得到了广泛的推广和使用，方便人们生活的同时也进一步加速了经济的发展。伴随着资源共享理念的不断深入，人们在应用大数据技术的过程中，也愈加关注数据治理中存在的网络安全问题，因此论文在实际研究中将主要围绕大数据背景下数据治理工作展开，通过多元化分析，探讨网络安全治理的主要策略，以此为相关工作人员提供可行性建议。

关键词

大数据背景；数据管理；网络安全问题；管理策略

1 引言

随着计算机网络技术的深入发展，大数据技术逐渐应用到社会生产生活的各个领域，在方便人们的同时也带来了巨大的安全隐患。大数据中往往涵盖着一些比较敏感和隐私的内容，因此在现阶段对网络安全进行治理的时候，尤其应该看到大数据技术的应用对整个信息安全的破坏，进而从实际出发，采取有效的手段和措施，提高数据安全，真正将大数据的价值发挥到最大化。借助计算机网络可以在一定程度上帮助企业对相关数据进行分析整合，从而优化企业的资源配置，提高企业的核心竞争力，为其实现可持续发展提供积极有力的思路。大数据技术在某种层面上已经成为企业发展的重要推动力，在这种环境和背景下，需要切实保障数据网络安全，从而确保大数据技术在实际运用中的不良影响降到最低水平。

2 大数据的产生和发展

近年来伴随着科学技术的不断发展，大数据技术已经渗透到社会各行各业，开始融入人们的生产生活活动中，这使得中国有关大数据技术的研究也开始深化。现阶段人们有关大数据的认识仍然不够透彻和全面，甚至有关大数据技术还没有形成一个统一的概念，大数据通常是大量数据和复杂数据的结合，在它的作用和影响下，可以帮助用户实现对海量数据的整合分析，而且在实际参与数据处理的过程中，必须依赖于云计算的相关数据库技术。大数据由于在社会层面推广的不断深入，有关该技术的研究也受到国内外学者的普遍关注，在实际工作中必须加强对数据的治理，确保数据传输安全，从而将整个技术的价值发挥到最大化。

3 大数据环境下的网络安全问题分析

随着大数据技术在现代社会应用的不断普及，在方便人们生产生活的同时，由于数据的持续增长，在一定程度上影响并干扰了网络信息安全，现阶段数据网络安全问题已经成为急需解决的事情，为了最大限度发挥大数据技术的优势作用，确保数据传输的安全性，需要从实际出发，对当前大数据影响下的数据安全问题进行更加系统和深入的研究 [1]。

3.1 大数据成为网络黑客攻击对象

网络黑客入侵从某种意义上看，就是导致网络信息传

【作者简介】陆海琴（1988–），女，中国江苏南通人，本科，工程师，从事数据管理研究。

输出现安全的严重隐患之一，黑客在实际入侵的时候，主要是借助计算机网络通信协议中存在的缺陷和漏洞进行攻击，与此同时用户安全配置不完善同样会导致黑客的攻击，进而影响整个计算机系统的正常运行，使得用户难以从事自己需要的网络服务。黑客攻击对网络数据的安全性破坏巨大，会使得整个网络变得十分不通畅，更是会造成网络系统的瘫痪。大数据在一定程度上方便了资源共享，为人们的工作生活提供了便利，但是需要注意的是，在应用大数据的时候，由于整个数据传输的网络环境具有开放性，因此这也使得其成为网络黑客攻击的对象 [2]。

3.2 信息内容安全分析

在大数据环境下，信息内容安全从类型上进行划分，主要包括两方面，分别是信息的泄露和信息的破坏，前者指的是在利用计算机从事相关工作的时候，尚未经过合法用户的授权和许可，就对系统中存留的数据信息进行窃取和破译，从本质上属于违法行为，尽管在实际应用计算机网络的过程中，平台会设置用户的访问权限，从而起到一定的保护作用，然而由于整个数据保护机制本身就存在较大的缺陷和漏洞，大多数数据保护机制在实际运行中，仍然对操作系统存在较大的依赖，需要时刻保障整个操作系统的安全性。用户在具体的操作实践中，由于对相关隐私数据没有进行正当的使用，加上在相关数据的分析和研究过程中未对其中存在的敏感数据进行明确化界定，这就使得一旦出现隐私数据被泄露的现象，就会对用户的正常使用产生困扰，导致整个计算机网络受到安全隐患的侵袭。信息的破坏主要是由于系统故障和病毒入侵造成的，它会使得整个信息内容出现差错，影响数据的准确性和完整性，进而影响大数据技术的实际应用效果，导致其中的信息内容不能达到有效的用途 [3]。

3.3 信息传播安全分析

大数据背景下，数据信息的传输载体主要是各种通信协议，但是这些通信协议在实际建立的过程中并不是为了确保数据信息安全，这就导致整个通信协议本身就会存在所谓的安全漏洞，无法对相关数据实施高效化的保护。大多数非法入侵和黑客攻击的出现，都是借助通信协议的漏洞进行的，它会直接对整个网络系统进行干扰，使得其中的信息内容遭到破坏。如果信息数据在实际进行传输的时候遭受攻击，就会影响整个传输工作的顺利展开，甚至严重时会导致整个网络系统出现瘫痪 [4]。

3.4 自然灾害

计算机本身在运行的过程中，并不具备抵抗外界攻击的能力，这就容易导致整个系统在遭受攻击时，受到强烈的震动，进而使得整个计算机设备的安全性无法得到切实的保障。机房内的环境问题以及室内不同线路在距离上的远近，都会在不同程度上对计算机设备造成所谓的电磁干扰，无论是计算机设备的配置还是实际承受能力，在过大的电源电压上都会对整个计算系统产生不利影响，使其无法正常运行。

4 大数据背景下数据网络安全的策略

大数据背景下，各种数据的运行遭受外界影响和攻击的可能性进一步加大，会直接干扰整个数据传输的安全性，因此在具体的工作实践中，需要切实从实际出发，网络安全是大数据背景下最关注的工作内容，决定着大数据工作质量。网络安全的提高需要对系统进行更为全面的分析，才能根据系统问题制定出合理的安全防御系统，全方位保障系统运行的安全。

4.1 防火墙技术

防火墙技术是最传统的网络安全维护方式，主要的原理是在内网和外网之间设置一个人工隔离层来维护网络安全，防止和避免整个计算机网络遭受外界的攻击和破坏，进而最大程度提高整个数据维护的安全性。借助防火墙技术对计算机系统实施安全保护的过程中，主要对威胁网络安全的信息进行屏蔽工作，对于安全管理计算机数据可以起到一定的帮助和促进作用，切实有效地增强整个数据传输的保密性，最终实现对计算机网络数据安全防护的目的。

4.2 数据加密技术

数据加密技术在某种意义上已经成为数据网络安全的基础，对于保障网络信息安全具有一定的帮助作用。借助计算机网络进行对应的加密操作，可以确保其中的一些私密信息被有效地隐藏起来，从而有效防止外界设备对数据的干扰和窃取。针对不同数据进行管理的时候，应该具体问题具体分析，采取针对性的加密方法，确保其中的明文数据可以经过一定程度的更新和调整，真正转换为密文数据，这样在进行数据传输的过程中，就算整个加密数据遭受外界的窃取，但是窃取者也无法恢复整个数据内容，对数据传输安全可以提供必要的防护和保障 [5]。

4.3 访问控制技术

在具体使用相关数据的过程中，通过控制数据的访问权限可以在一定程度上确保整个网络数据传输的安全性和稳定性，而在相关工作实践中进行访问控制主要是为了对用户访问的网络资源权限进行系统化的认证，借助实名认证工作的展开防止网络资源受到非法访问和使用。在对用户的访问权限进行控制的时候，从类型上进行划分，主要包括身份认证和口令加密这两种形式，它们的高效利用可以在很大程度上确保网络信息数据应用和访问的合理性和合法性，对维护网络系统的运行安全也可以起到一定的帮助作用。

4.4 数据备份

数据备份可以在一定程度上实现对数据的高效化保护，在实际进行数据管理的过程中，为了防止重要数据出现丢失。就需要采取数据备份的手段加强对数据的保护，将一些十分重要的数据复制到存储设备中，使其可以得到转移性存储，这样当系统在实际运行的过程中，即使遭受到外界设备的干扰和破坏，也能通过一定的方式和手段，第一时间恢复相关数据，全方位确保整个数据的真实性和有效性。就算在

具体的工作实践中，基于数据保护已经出现了所谓的防火墙设备，但是为了最大程度确保数据传输的安全，同样需要借助一定的方式对数据进行备份，防止整个系统在运行中由于受到黑客入侵等因素的干扰从而造成数据的是损坏和丢失，进而导致整个网络系统难以在正常的状态下运行[6,7]。

4.5 完善计算机网络管理制度

相关部门在加强计算机网络管理的过程中，需要统筹分析，从多角度着手，尤其应该在实际工作中建立健全相应的网络管理制度，只有这样才能最大限度确保整个计算机系统运行的安全性和稳定性，使其价值和优势可以实现最大化。网络安全建设在具体实施中，要求将技术和管理有机融合起来，不但要紧跟潮流，在技术层面进行探索和创新，研发先进的信息安全保护技术对整个数据的传输提供必要的支撑和保障，与此同时更是要加强规范化管理，通过制定个性化的网络管理制度，对软件和相关操作加强维护，进而规范计算机用户的日常行为操作，使其可以按照相关规范参与网络行为，真正确保大数据背景下数据网络安全管理可以达到理想的效果[8-10]。

5 结语

大数据网络安全在实际维护的过程中，需要综合考虑多种因素，统筹分析，它所应用和涉及的领域本身就具有广泛性，在一定程度上会引起各行各业的变革，但是从某种层面上看，网络安全问题也逐渐成为制约大数据发展的关键性因素，因此在现代化建设中，特别是伴随着科学技术的不断推广和持续深入，为了保障大数据背景下的网络安全，相关部门必须肩负起对应的责任意识，在现实工作中加强对大数据技术的研究和分析，在把握大数据技术特点的基础上，通过技术上的优化和完善，全方位确保整个网络信息传输的安全性和完整性，真正将大数据技术的优势作用发挥到位，与此同时有效规避大数据技术在实际应用中对整个网络系统运行产生的不良影响，在相关技术升级和制度健全的作用下，全方位确保网络系统的正常运行。

参考文献

[1] 谢林江,杭菲璐.大数据背景下数据治理的网络安全策略[J].科技资讯,2018,16(17):5-6.

[2] 唐童洲.浅谈大数据背景下数据治理的网络安全策略[J].网络安全技术与应用,2018(5):35-36.

[3] 高垣,侣洁.大数据背景下数据治理的网络安全策略[J].中国新通信,2018,20(6):165.

[4] 黄小丽,辛建官.大数据背景下数据治理的网络安全策略[J].数码世界,2017(11):269.

[5] 陈火全.大数据背景下数据治理的网络安全策略[J].宏观经济研究,2015(8):76-84+142.

[6] 戴训安,申有祥,潘丹.大数据背景下信息通信网络安全管理策略研究[J].中国新通信,2022,24(3):7-9.

[7] 王伟然,刘志波.大数据背景下数据加密技术在计算机网络安全中的应用分析[J].电子世界,2021(24):11-12.

[8] 李卫峰.大数据背景下计算机网络安全及解决策略[J].电脑知识与技术,2021,17(22):42-43.

[9] 杨景炜.大数据背景下网络安全策略探讨[J].网络安全技术与应用,2019(9):46-47.

[10] 江育锋.大数据背景下信息通信网络安全管理策略研究[J].长江信息通信,2021,34(3):158-160.