大数据在计算机网络安全风险中的应用分析

关　博[1,2] 王伟光[1,2]　曲鸿祥[1,2]　정양권[1]
1. 东新大学校　韩国全罗南道罗州　58245
2. 北华大学　吉林省吉林市　132013

摘　要：随着网络技术的飞速发展，大数据逐渐进入人们的视野，尤其是在企业的经营活动中，大数据技术已经成为一种重要的技术手段。同时，大数据已经深入到了人们的生产和生活中，通过计算机网络进行数据和信息的传递与共享，提高了计算机网络的运行效率。因此，在大数据时代，一定要高度重视计算机网络的安全风险，并采取相应的预防措施，以改善计算机网络的安全性。文章主要阐述了大数据的概念、计算机网络存在的安全风险问题以及大数据在计算机网络安全风险中应用的必要性，并提出了一些应用策略以期可以消除计算机网络的安全风险。

关键词：大数据；计算机网络安全风险

Application analysis of big data in computer network security risk

Bo Guan[1,2]　Weiguang Wang[1,2]　Hongxiang Qu[1,2] 정양권[1]
1. 동신대학교 ,DONGSHIN UNIVERSITY　Naju, South Jeolla Province, South Korea 58245
2.Beihua University　Jilin City, Jilin Province 132013

Abstract: With the rapid development of network technology, big data has gradually come into people's view. Especially in the business activities of enterprises, big data technology has become an important technical means. At the same time, big data has penetrated into people's production and life. The transmission and sharing of data and information through computer networks improve the operation efficiency of computer networks. Therefore, in the era of big data, we must attach great importance to the security risks of computer networks, and take corresponding preventive measures to improve the security of computer networks. This paper mainly expounds on the concept of big data, the security risk of computer networks, and the necessity of big data application in computer network security risk and puts forward some application strategies to eliminate the security risk of computer networks.

Key words： Big data; Computer network security risks

随着计算机网络技术的不断发展，人们的生产和生活都在发生着变化，人类社会也步入了大数据时代。在大数据系统的大环境下，计算机网络安全风险日益引起人们的重视，在实际的使用过程中，既要及时有效的发现计算机网络中的各种安全风险，又要对其进行科学的处理，这样才能有效地保障计算机网络的安全性和可靠性，促进计算机网络的健康和长远发展。

一、大数据的概念

随着网络技术的迅速发展和计算机网络技术的应用领域的不断扩展，系统中的数据量越来越多，这给人们的工作带来了一定的困难，并在一定程度上影响着人们的日常生活。大多数现象的产生都与大数据时代有着密切的联系。大数据是指在特定的时间里，不能用常规的工具来获取和处理大型数据。大数据是指在特定的时间里，不能用常规的工具来获取和处理大型数据。其最显著的特征就是数据种类丰富、传播速度快、数据量大，可以反映到大部分工业领域。与传统的数据相比，大数据有其自身的特点，包括：海量的数据类型、较高的数据处理方式、海量的数据信息量等。因此，在实际测绘地理信息规划中，要强化对海量数据的理解，从多个视角去考察测绘地理信息在大数据环境中的作用，从而促进地理信息在大数据时代的发展，以达到与时代发展相适应的目的。

二、计算机网络存在的安全风险问题

1. 网络病毒

网络病毒是当前计算机网络安全风险的一个重要原因。一旦计算机受到网络病毒的侵入，将会给计算机的安全带来很大的危害，而网络病毒则会从计算机中盗取资料，严重时会使计算机无法正常工作而发生故障，从而危及计算机的网络安全。特别是近几年，互联网上出

现了许多新的病毒，其中包括非法分子使用计算机病毒进行非法竞争、窃取公司经济发展资料等，对社会经济发展和个人工作生活造成了更大的危害。

2. 黑客攻击

因为计算机网络的开放性，使得很多行业都可以共享和获取计算机中的信息，所以黑客攻击的问题也越来越突出。在这个过程中，往往会产生大量的利润，这些利润就会被犯罪分子利用，在计算机网络层面上寻找突破口，从而在计算机网络层面形成了诸多不同风格的安全风险问题。在目前信息共享、开放的背景下，一般采用 TCP/IP 协议来实现信息的自我防护，但这种保护方式的效率比较低，无法满足各种信息的传输要求，使得网络信息的安全性有一定的缺陷。计算机储存着企业和个人的大量工作资料，是人们工作和生活的重要辅助工具，而黑客则是利用一定的网络技术，非法攻击他人的计算机，从而窃取需要的信息数据，往往这些信息数据具有一定的利益价值。而且黑客攻击也一个很大的特征，那就是广泛性，这也与黑客的计算机技术有关。

3. 用户的计算机网络安全风险意识薄弱

由于用户的计算机网络安全风险意识薄弱，也会给计算机网络安全造成一定的影响。比如，不法分子会通过邮件、新闻等方式，给计算机使用者发送垃圾短信，不仅会给计算机使用者带来麻烦，还会以垃圾邮件为媒介，通过高科技的手段，窃取计算机中的信息，虽然不会对计算机的正常工作造成很大的影响，但会对计算机的网络安全产生不利的影响。因此，计算机使用者要加强计算机网络安全风险意识，并要定时对计算机进行病毒的查杀，增强对计算机安全的管理。目前，对计算机网络进行科学、合理的控制是保障信息安全的重要途径，但目前的情况是，在计算机网络系统中，使用者的操作水平参差不齐，文化、专业等各方面的差异，使用户在使用计算机过程中的使用习惯也不尽一致，并且存在着不熟练、不规范的现象，造成了网络安全风险的频发。此外，一些是酸碱使用者对安全防护的认识还不够充分，很可能因为自己的失误，而把密码输入错误，或者泄漏出其它的安全信息，这就给了不法人员违法犯罪的可乘之机。

4. 自然灾害

在计算机网络的运作中，网络与通信设备、网络设备有着密切的联系，但这些设备并不能有效地抵御自然灾害，因而会在计算机网络中引起一系列的安全问题。比如，当发生地震、暴风雪等自然灾害时，计算机网络中的相关设备都会受到一定程度的损伤，这种损伤很有可能会危及到系统的安全，比如在数据传输过程中，会出现数据中断、丢失等问题。

5. 计算机网络系统自身的不足所导致的安全风险

目前的计算机网络系统并不是很完善，都有一些 BUG 和漏洞，比如 Windows 和 Limux，它们都有自身的弱点，所以都无法避免来自于系统本身的安全隐患，而且还会从硬件上造成安全隐患。在这种情况下，计算机使用者在下载、安装软件时，也会对系统产生一些安全风险。其实，如果是计算机本身的安全问题，那还好说，但如果是在下载和安装程序的时候，出现了一些安全风险，那么就会给计算机的安全带来很大的影响，特别是在这个时候，一旦有黑客入侵，那么就会影响到整个系统的安全性，甚至会导致用户的个人信息被泄露。

三、大数据在计算机网络安全风险中应用的必要性

1. 大数据为计算机网络安全提供数据资源

随着我国互联网用户规模的不断扩大，在人们的日常生活和学习中互联网信息技术的地位已经无法取代，因此出现了大量的网络安全问题。我国近半数的计算机用户都受到了不同程度的网络安全威胁，个人的计算机信息利用状况也依然不容乐观。在众多的安全问题中，木马、病毒、密码或账号被盗的现象越来越多，而消费者遇到的诈骗行为也越来越多。因此，在计算机网络使用中，加强网络安全是十分必要的，根据大数据，可以为网络安全提供一些技术资源的支持。大数据的多样性、海量的数据和信息结构，为计算机安全提供了丰富的数据，既具有独特的创新性，又具有很高的应用价值。通过大量的数据，可以还原出计算机网络受到侵犯的画面，并运用大量的数据，制作出动画，让用户体验到计算机网络信息病毒攻击计算机的缺陷，让用户可以发现计算机被盗过程会出现的漏洞。

2. 大数据为计算机网络安全提供技术支持

在大数据环境下，计算机网络安全学习都可以数据平台上呈现。在大数据的支撑下，用户以及企业可以利用云传送技术，与相关负责人进行信息交流。云计算在我们的日常生活中是非常普遍的。在社会的发展进程中，这一类是最具代表性的。在此项技术的发展中，大数据技术的准确性必须是高效率的，而在当今的发展进程中，它可以持续推动大量的数据技术。大部分人对这种技术很熟悉，但却无法完全了解它的意思。这是一种基于多种计算方式的计算机数据的分类和统计。大数据技术的发展，主要是由于云计算技术的发展，使得计算机能够有效地整合信息系统的安全性需求，从而达到适合的保护目的。云计算技术可以持续改进计算机的运算能力。在发展的过程中，要不断地扩展信息系统的应用领域。数据信息空间将会得到有效的发展，将会推动大数据技术应用于计算机网络信息安全方面。

在当前的发展阶段，人们的生活已经和以前大不相同了。信息技术的高效发展，使人们的生活得到了持续的提高。目前计算机工作的重点是信息安全。有效地利用资料备份技术，可以增加多个安全网络到讯号传输的讯号强度。同时，也为数据的利用奠定了坚实的基础和保证。保证信息的安全传递是非常关键的。与此同时，大数据在人们的日常生活中也得到了广泛的应用。很多

企业都在努力使自己的信息系统安全。通过高效地实施大数据技术，信息安全等级可以不断提升，这样就可以继续保持业务的发展，并且在开发期间为储存信息节约大量的内存。运用正确的数据备份技术，可以有效地处理日常数据的流失。同时，还能减少在传播中的信息和资料的损失。

四、大数据在计算机网络安全风险中应用的策略

1. 建立虚拟私有网络

针对计算机网络系统自身的不足所导致的安全风险，建立一个虚拟私有网络是一种比较切实可行的方法。这种技术是指在一个公用的网络体系结构中，建立一个专门的网络系统，它不是一个单独的，是基于一个公用的网络结构，是一个公共的网络系统的一部分。具体而言，建立虚拟私有网络，是基于计算机网络的通讯协议，在企业内部网络和远程客户机之间建立一条多协议的虚拟专用线，从而达到与企业内部网络和远端客户端的高效连接，同时还可以通过网络系统自身进行隐秘的通讯，从而防止数据信息的泄漏。

2. 增强用户的身份认证和密码安全性

在很多时候，采用加密技术是一种很常见的方法，但是随着计算机技术的飞速发展，人们对加密技术的需求也在不断增加，传统的数字加密方法已经不适合于现在的网络安全要求，而是将数字和字母组合在一起反复设置密码，可以极大地增强加密防御的效率。同时，指纹识别、虹膜识别、面部识别等技术的应用也成为了当前的发展趋势。

3. 主动引进异常入侵检测

异常入侵检测技术是一种用于探测网络攻击行为的技术。该技术可以有效地解决由于用户操作造成的网络安全问题，也可以防止人为操作以及外部的入侵引起的计算机网络的安全问题，从而使计算机网络在受到外部和内部的威胁时能够得到及时的反应，从而提高计算机网络的安全性。

4. 建立安全防护系统

为了增强计算机网络的安全，需要建立相应的安全保护体系，提高网络安全指标，防止病毒入侵，提高计算机网络应用环境的清洁度，减少各种潜在的危险。各部门应建立与计算机网络安全有关的安全防范体系，运用各种计算机网络防御措施，从根本上改善病毒入侵问题，以全面提升计算机网络的安全性。特别是在大数据的不断发展下，在安全体系中设置防火墙是非常必要的，它不仅可以减少计算机网络受到威胁，而且可以有效地保护用户的隐私，防止重要的数据被泄露和窃取，从而保证计算机网络的正常和安全。另一方面，在使用计算机网络安全系统的时候，技术人员可以利用自身的各种新技术对计算机网络进行有效的维修和维护，防止各种网络病毒进入电脑的系统，给企业的生产和生活带来便利，也可以让各种计算机的运行更加有序。

5. 应用新型数字技术

计算机安全防护人员可以利用数字签名技术提高计算机网络的安全性，这种技术通过对电子文档的身份认证和身份识别，从而提高计算机网络的安全性和有效性。同时，技术人员也会使用解密密钥和加密密钥，这种方法相对于传统的数字签名技术来说，安全性不高，应用范围也不是很广。为了增强整个计算机信息的保密性，可以将各种数字签名技术巧妙地结合起来。在进行加密的时候，可以通过计算机或者人工智能的技术，使用多种算法来完善自己的计算机网络数据库，这种技术可以提高计算机网络的工作稳定性，也可以保证数据的安全性，在不断的完善数据库的同时，也可以防止被窃取和损坏。

6. 增强计算机网络安全风险意识以及安全管控

随着防火墙等多种保护手段的建立，计算机网络的安全性得到了明显的提高。但是在日常工作和生活中仍存在着一种网络安全隐患，特别是当黑客入侵计算机网络时，会使计算机的系统瘫痪，使内部的数据安全受到威胁，从而使国家和公司蒙受巨大的损失。为了改进目前的计算机网络运行状况，用户必须增强计算机网络安全风险意识，从根本上解决这类问题。在处理计算机网络的安全问题时，管理者需要及时地对其进行控制，即在日常工作和生活中，要注重计算机的网络安全，通过各种有效的手段，不断提高计算机网络安全管控水平，建立相应的安全管理体系，优化自身安全管控技能，从而使国家或企业的重要信息存储在安全环境中。随着信息技术的不断发展，技术人员在对计算机进行安全控制的时候，可以采取更简便、更灵活的方法，对计算机网络的安全控制也会得到进一步的改善，既能保证用户的使用，又能提高企业的生产效率。

五、结语

在大数据环境下，人们应充分认识到计算机网络的安全风险，并采取相应的对策，及时准确地解决各种问题，并根据不同的情况，对其进行科学的处理，使计算机网络的安全性得到全面的保障，从而有效地保障了计算机网络在大数据环境下的运行性能，提高计算机网络的准确性和安全性，提高社会生产和生活的便捷性。

参考文献：

［1］张贤秀．浅谈大数据在计算机网络安全教学中的应用［J］．网络安全技术与应用．2020（12）:84-85.

［2］苗敬峰．李强．大数据技术在计算机网络信息安全问题中的应用研究［J］．中国新通信．2021:77-78.

［3］何斌颖．大数据技术在计算机网络信息安全问题中的应用——评《计算机网络信息安全》［J］．电镀与精饰．2020（3）:47.

［4］李小康．大数据技术在计算机网络信息安全问题中的应用探析［J］．无线互联科技．2021（7）:86-87.

［5］董明．大数据与计算机网络的安全风险与应对措施［J］．电子技术．2022（8）:250-251.

［6］苏智华．试谈大数据时代的计算机网络安全及防范措施［J］．网络安全技术与应用．2018:65-66.

［7］解春升．大数据时代计算机网络安全技术应用风险分析［J］．网络安全技术与应用．2022（6）:59-61.