大数据给信息安全带来的新挑战及应对策略

陈春梅
重庆信科设计有限公司　重庆　400000

摘　要：大数据的存储和处理需要强大的技术支持，同时也增加了隐私泄露和数据滥用的风险。基于此，本文介绍了大数据技术在计算机信息安全中的关键技术，分析了大数据对信息安全所带来的新挑战，并提出了相应的应对策略，以期为网络信息安全管理提供参考。

关键词：大数据；信息安全；挑战；应对策略

引言

随着互联网的不断发展和信息技术的迅猛进步，大数据正成为各行各业的重要基础资源。然而，大数据的广泛应用也带来了信息安全方面的新挑战。因此，我们需要更加重视信息安全问题，采取措施应对新的安全威胁。

1 大数据在信息安全中的关键技术

1.1 云计算技术

云计算技术在信息安全领域为大数据技术提供了强大的支持。第一，云计算技术采用分布式存储的方式，将数据存储在不同的物理设备中。这种分布式存储模式摆脱了传统硬件设备的限制，使得数据可以被合理地划分和存储在多个节点上。通过数据的冗余备份和容灾机制，即使某个节点或设备发生故障，数据仍然可以正常访问和恢复。这样大大增加了数据的可靠性和安全性。第二，云计算技术提供了数据加密和隔离的功能。通过采用加密算法对敏感数据进行加密处理，即使数据被盗取或泄露，也无法解读其内容。同时，云计算平台能够为不同用户之间提供数据的隔离，防止未经授权的访问。采用访问控制和身份认证机制，只有经过授权的用户才能访问和操作数据，有效保障数据的安全性和完整性。第三，云计算技术还提供了安全监控和审计功能。通过实时监测和记录系统中的安全事件和操作行为，可以对潜在的安全威胁进行及时发现和预警。日志分析和行为识别等技术能够帮助识别出异常行为，从而提供相应的响应措施。审计功能可用于追踪和分析用户的操作记录，以保证数据的合规性和安全性。第四，云计算技术具有强大的弹性伸缩和容灾备份能力。根据需求的变化，可以动态调整资源的使用量，实现高效的资源利用。同时，利用虚拟化和容器技术，可以快速部署和恢复系统，以应对硬件故障、自然灾害等突发事件。这种弹性伸缩和容灾备份机制有效地提升了系统的稳定性和可用性。

1.2 数据备份技术

近年来，信息技术的快速发展对人们的生活产生了深远的影响，大数据技术的发展更是为信息技术的发展注入了新的动能。然而，随着信息量的爆炸式增长，信息安全问题日益突出，而数据备份技术的应用则成为了解决企业信息安全问题的关键技术。数据备份技术是指将企业重要数据进行定期备份，并将备份数据存放在安全的地方，以便在数据丢失或损坏时及时恢复数据。一方面，在企业系统的建设和应用过程中，数据备份技术是必不可少的一环，它能够为企业的重要数据提供可靠的保障，防范重要数据在各种突发情况下丢失的风险，从根本上保障企业的信息安全。另一方面，在大数据技术的应用过程中，数据备份技术具有重要的作用，它能够保障企业的业务数据完整性，避免数据丢失而带来的业务中断。此外，数据备份技术也能够帮助企业减少黑客攻击等安全隐患所带来的损失，因为一旦数据被攻击者删除或欺骗，则可以通过备份数据进行恢复，最终保护企业的信誉和商誉。此外，备份应根据实际情况定期进行，并将备份数据存储在多个位置以防止重要数据的丢失。同时企业应坚持数据备份的原则，确保数据备份的完整性、可恢复性、加密性、易用性等；最后，还需要定期对备份数据进行检查、销毁等后续处理。

2 大数据给信息安全带来的新挑战

2.1 个人信息泄露风险大

随着互联网的普及和数字化社会的加速发展，个人信息在各个方面得到了广泛应用。同时，也存在不法分子为了获取经济利益，利用各种手段侵犯他人的隐私并进行信息泄露的情况。这些不法行为包括黑客攻击、网络钓鱼、恶意软件等，都可能导致个人信息的被盗取和滥用。首先，一些企业没有充分重视信息安全问题，未采取足够的措施来保护用户的隐私。缺乏对信息安全的投入和管理，使得个人信息易受攻击，并容易遭受泄露

风险。此外，一些企业在信息安全建设方面也没有引进先进的设备和技术，无法有效防范信息泄露的威胁。其次，信息交易市场的存在给个人信息泄露带来了更大的风险[1]。一些不法分子通过非法手段收集到大量个人信息后，将其出售给有需求的买家。这种违法的信息交易频发，使得个人信息的泄露情况更加严重。缺乏有效的监管和打击机制，为信息泄露提供了可乘之机。最后，个人信息泄露对信息安全构成了诸多挑战。泄露的个人信息可能被用于身份盗窃、网络诈骗、广告骚扰等不法行为，给个人带来财产损失和精神困扰。同时，隐私泄露也会导致信任危机，用户对企业和互联网服务提供商的信心降低，对于数字化社会的发展造成不利影响。

2.2 在储存方面的安全问题

在信息社会中，储存数据是企业运营过程中非常重要的环节。随着大数据时代的到来，企业在储存数据方面的需求也越来越大，但储存方面的安全问题却日渐突出，其中数据泄露是最常见的安全问题。数据泄露指的是将机密信息泄露给非授权人员或组织的行为，泄露的信息可能包括客户信息、银行账户信息、商业机密等。由于数据泄露可能造成的损失巨大，因此，企业需要重视并采取措施来避免发生泄露。另外，扫描设备受攻击是另一个常见的储存方面的安全问题。扫描设备常用于将电子文档转换为数字格式并上传到数据库中，不法分子可以利用漏洞入侵扫描设备，将病毒或恶意软件安装在扫描设备上，从而窃取敏感数据。

2.3 数据使用监管存在明显隐患

在当今社会，数据使用监管成为了一个重要的话题。尽管法律对于信息收集和删除方面进行了详细规定和说明，但是从目前来看，一些网络营运商未能履行保护用户信息的义务，这就给用户的信息保护和权益带来了潜在的风险。第一，运营商对用户信息保护不足。虽然法律规定网络营运商必须履行保护用户隐私的责任，但是仍有部分运营商在信息收集、存储和处理等环节中未能严格遵守有关规定，容易造成用户隐私泄露和安全风险。第二，信息删除难度。用户想要删除自己的个人信息时需要先向运营商告知，然而并不是所有运营商都能够快速响应并且及时删除信息，此时用户权益受到了严重侵害。在运营商长时间无响应的情况下，用户只能自行寻求其他途径来维护自己的权益。第三，对权利救济的难度影响。在满足一定的前提条件下，用户有权向法院提起诉讼来维护自己的权利[2]。然而，在实际操作过程中，许多用户由于对法律知识的缺乏，缺乏维权的意识以及维权成本过高等问题而放弃了维权，导致用户权益难以得到有效保障。

2.4 黑客攻击

黑客攻击利用大数据环境中众多的数据种类和数量，通过主动或无意识入侵的方式来侵入计算机系统。有意识入侵通常是有计划性地入侵企业或个人计算机系统，目的是盗取、篡改或删除有价值的数据信息。黑客会深入系统内部，寻找弱点并利用漏洞进行攻击，从而获取敏感信息或控制系统。无意识入侵则不会对计算机使用过程产生直接影响，但仍然可能存在潜在的安全风险。其次，黑客可以利用网络协议、IP地址和服务器等方法，突破防线，盗取用户的个人信息。他们可能针对具体的目标进行定向攻击，通过恶意软件、网络钓鱼等手段获取用户账户、密码、银行卡信息等敏感数据。这种行为严重威胁网络安全，给用户带来财产损失和隐私泄露的风险。此外，黑客可能利用恶意代码、拒绝服务攻击等手段，导致系统崩溃或无法正常运行。这种攻击不仅会破坏数据完整性和可用性，还可能使得企业或个人无法正常工作。此外，黑客可能篡改数据、植入恶意软件，给系统安全带来长期风险。

3 应对大数据给信息安全带来新挑战的策略

3.1 加快大数据安全技术研发

随着大数据时代的到来，数据安全问题愈加突出。在信息技术方面，大数据涉及到了云计算、物联网等新兴技术的发展，这也给信息安全带来了新的挑战。在当前时代下，为了维护信息安全，必须加大对相关信息安全维护技术的投入力度，积极借鉴国外的信息安全技术和管理思想，加强对相关安全技术产品的研发力度，达到有效保障当前时代下信息安全的目的。加快大数据安全技术研发，可以从以下几个方面入手：（1）大数据安全技术标准不足，应加强标准建设。建立大数据安全技术标准是保障信息安全的基础，全面建立、合理运用适当的标准，可以有效提升大数据安全性。（2）加强对数字身份识别技术的研发。数字身份识别技术可以有效防止用户身份被盗用、伪造等问题，关键是要注重隐私保护[3]。（3）从系统架构上进行改善。加强大数据系统的监控和预警，增加安全防护层面，提高安全防护的效率和敏捷性。（4）加强大数据应用程序安全开发。在保障大数据安全方面，数据的使用和处理是至关重要的。因此，我们需要加强对大数据应用程序安全开发的规范性、标准化和专业性，以减少安全漏洞的产生。

3.2 及时有效销毁个人隐私数据

首先，用户的私人敏感信息可能存在于各种凭证中，如车票、快递包装、银行存取款记录和账单等。这

些凭证一旦丢失或被他人获取，就有可能导致个人隐私泄露和身份盗窃风险。因此，用户应该养成良好的习惯，及时保存重要的凭证，并妥善保管。其次，对于无用的凭证，用户应进行及时销毁和丢弃。例如，过期的车票、快递包装和账单等，可以选择彻底破坏或使用安全的文件销毁方式进行处理。通过撕碎、切割或使用专业的文件销毁机械，可以确保敏感信息无法被恢复和利用，从而避免隐私泄露的风险。最后，电子设备也是个人隐私泄露的重要来源。用户应定期清理和删除手机、电脑或其他设备中的敏感信息。这包括删除聊天记录、浏览历史、缓存文件等，确保个人隐私不被他人获取。同时在处理电子设备时，用户还应注意选择可靠的数据擦除工具，确保敏感信息被完全清除。

3.3 加强病毒防护

在当今网络时代，恶意软件和病毒的攻击已经成为了普遍存在的威胁，对用户的计算机系统和个人信息都带来了严重的危害。第一，为了最大程度地保护计算机安全，用户应当定期学习计算机网络信息安全防护技巧，并时刻保持网络信息安全防护意识。这包括了解密码安全原则、使用双因素认证、设置强密码、定期更新软件补丁等措施[4]。通过学习和实践，操作人员可以加深对网络安全问题的认识，并能够主动采取有效的防范措施。第二，用户还应当加强基本的网络安全管理。这包括定期更新操作系统和安全软件的版本，关闭电脑中的“自动播放”、使用数字证书等安全策略，避免接收来路不明的文件，以及不轻易上外网等措施，这些措施可有效提高电脑系统的安全性。第三，为了提高病毒防护的效果，用户需要在计算机中安装高质量的病毒防护软件。主流安全软件提供了全盘扫描、病毒查杀等全面的引擎，用户可以通过手动扫描及时发现电脑中的病毒。此外，用户还可以开启实时防护系统，及时发现并处理入侵电脑中的恶意软件和病毒，避免给计算机带来损害。同时，在日常使用电脑的过程中，用户需要保持警觉，避免接收来路不明电子邮件、下载不明文件等行为。

3.4 完善安全监管制度

要提升网络安全，除用户个人的自我安全防护外，更需要监管部门和相关企业积极进行安全监管，加强网络安全技术的投入，制定相应的监管标准和责任机制，全方位保护数据安全。一方面，监管制度建设是保障网络安全的重要手段之一。监管部门应根据用户常见的安全问题进行针对性制定监管标准，引导相关企业和个人加强网络安全防护。同时，向企业和个人提供训练机会、技术支持和安全指导，协助其掌握网络安全技术，保证网络安全。另一方面，建立信息安全责任机制也是保障网络安全的重要措施。这种机制应区分不同领域和部门，建立各自的安全防护责任。在电信和互联网等领域，每个企业应当建立相应的安全保障机制，指定专人负责网络安全的监督和管理。同时，要强化监管力度，加大对网络安全违法行为的打击和处罚力度，保护用户网络安全往不受侵害。

结语

综上所述，大数据技术的发展为我们带来了无限的可能性，但同时也会带来不少安全隐患。信息安全问题是一个需要我们持续关注的议题，在保障网络安全方面，个人和机构都有不可推卸的责任。我们应该加大对相关信息安全维护技术的投入力度，并积极借鉴国外的信息安全技术和管理思想，加强对相关安全技术产品的研发力度，达到有效保障当前时代下信息安全的目的。同时，大数据安全技术的研发也需要多方参与，共同发挥各自的优势，推动大数据安全技术标准化、规范化、系统化发展，保障网络安全和数据隐私。

参考文献

[1]官节福.大数据时代计算机网络信息安全及防护策略研究[J].计算机产品与流通,2019(11):47.

[2]唐超,唐美艳.探析大数据时代计算机网络信息安全及防护策略[J].数字技术与应用,2019,37(10):203-204.

[3]李蹊然.大数据时代计算机网络信息安全及防护策略研究[J].数字技术与应用,2019,37(10):190+192.

[4]高淑美，徐婕.基于大数据的生物医学信息安全管控平台建设研究[J].信息与电脑（理论版），2019（02）：190-191+194.