基于计算机大数据的信息安全处理技术探索

苏嘉明

（西安科技大学高新学院，陕西 西安 710109）

摘要：如今信息技术的运用已经相当普遍，云计算、物联网技术也得到广泛应用，人们随即进入了大数据时代。伴随着信息产生速度的加快和信息量的增加，传统的信息技术已经无法满足当今时代的需要，所以，必须针对大数据的特点，对信息安全技术进行优化和改革。

关键词：计算机大数据；安全处理技术；研究探索

现阶段，网络技术已经成为人们生活、工作不可缺少的组成部分，随着网络技术的更新换代，信息传输的速度和质量都有了很大进步，甚至打破了空间和时间的限制。计算机大数据就是利用计算机技术、通信技术，为人们提供数据服务，一方面可以高效完成信息处理，另一方面，还可以帮助人们快速找到有用的信息。由于用户的不断增加，信息量的不断扩大，大数据在给我们便利的同时，也存在不少安全隐患，因此，加大对大数据信息安全处理技术的研究，有很重要的意义。

一、大数据技术的概念

大数据技术就是将人类的各种信息进行归档，接着，再通过一定方式，对信息进行整理，最后，针对人们不同需求，给人们提供有价值的信息。大数据的数据量非常非常大，而且种类繁多，在网络技术的背景下，数据的迭代速度也很快。海量的数据，需要通过科学的手段进行整理分析，继而从众多的数据中，找到人们所需要的数据，进而为人们提供更好的服务。

二、大数据时代的信息安全问题

（一）黑客攻击导致的信息安全问题

大数据的信息量巨大，其中也有不少重要和敏感的信息，如今，计算机技术越来越成熟，而对于网络的攻击手段也更加完备和隐秘。有的时候，黑客对网络的攻击甚至很难被发觉，进而就增加了信息的安全风险。除此之外，有的网络工作人员，为了谋得私利，甚至故意泄露一些信息，导致恶劣的安全问题。

（二）服务器中断导致的安全问题

网络在故障或者黑客的攻击下遭到破坏，计算机系统想要修复完成，可能需要很长一段时间。时间对于企业来说十分宝贵，如果这个时间段，企业正在举行一场重要的会议，或者正在和客户进行网络贸易谈判，那么就可能造成巨大的损失。比如文件无法传输、比如信息丢失等等，进而还会影响企业今后的工作开展。

（三）计算机病毒导致的信息安全问题

互联网是一个共享的环境，网络的最大特点就是共享，尽管网络给人们带来了极大的便利，但也给网络病毒提供了温床。有的网络病毒传染性、破坏性很强，有的高级病毒甚至还会自我隐藏，有的时候，网络安全管理人员甚至难以发现病毒的存在。于是病毒就会顺着网络蔓延开来，一方面，网络病毒会造成信息泄露、系统崩溃，另一方面由于信息的敏感性还可能造成经济损失。

（四）操作系统的安全漏洞

通过分析发现，计算机操作系统安全漏洞十分常见，这种漏洞，就是指计算机操作系统在安装时候或许更新的时候出现的漏洞，这种漏洞有的时候十分明显，很可能因此出现致命的隐患。这种常见的安全隐患，可能会让黑客入侵、病毒入侵变得容易，进而就会造成系统的不安全或者不稳定，甚至会造成系统崩溃，数据丢失。对于这一点，应该要高度重视。

（五）自然因素的影响

大数据技术十分先进，其工作效率和工作质量十分可观，但即便如此，基于大数据的信息安全，也和外界的环境有着密切的关系。计算机系统的运行需要依靠大量的元器件，很多电子元器件十分敏感，很容易受到外界的干扰和破坏。一旦这些电子元器出现问题，那么系统就可能遭遇到严重破坏，会导致数据丢失等问题。如今，计算机系统在运行的过程中，面临的外界因素不少，比如温度、湿度、震动等等，都能造成计算机系统的运行障碍，一旦服务器硬件出现问题，就会导致信息数据受损，或者信息的丢失。

（六）个人隐私泄露风险较大

大数据技术方便人们的工作生活，可是，大数据所搜集的数据，来源比较广泛，内容也比较复杂，这些数据很可能关系到人们的日常生活和企业的正常运营。如果忽视对信息安全的保护，就可能造成信息泄露的风险，大数据背景下，数据量巨大，查找和搜索的成本都有可能加大，于是，个人隐私泄露的风险也就增大了。如果泄露的关键信息，甚至会关系到生命财产安全。

三、计算大数据信息安全处理技术分析

（一）云计算

在大数据信息安全处理技术之中，云计算是十分重要的一门技术。云计算能以并行式、分布式两种方式对数据安全进行保护，与此同时，云计算还能用网络信息资源，对海量数据进行计算和统计。云计算的应用，可以大幅度提升数据处理速度和处理的准确度，除此之外，云计算还能根据信息的特点，对数据进行组合和合理配置，大数据的利用价值就充分体现出来了。云计算的工作机制是通过网络云计算平台来完成的，首先，需要将数据进行分类，再通过任务分配机制将它匹配到相应的小程序处理单元，小程序单元接到指令对数据进行相应处理，接着，再由分支服务器对处理结果进行收集整理，最后，这些数据再传到云平台，云平台经过处理得到结果，进行反馈。云计算技术可以对巨量的数据进行高速处理，进而满足人们的需求。

（二）数据备份技术

互联网的普及，提高了生活、工作的便利性，也提高工作效率，但其中也有不少安全隐患，其中一项就是数据丢失。数据备份技术就为了避免因为故障导致的数据丢失，这项技术可以将所有数据，或者一部分数据，从服务器主机备份的其他介质上，这样就避免数据的丢失，一旦出现故障或者其他问题，还可以从其他介质中找到数据备份。互联网已经深入人们生活的方方面面，经过长时间的磨合和发展，互联网已经成为人们生活不可或缺的重要组成部分。然而，由于互联网的应用，让个人信息、企业信息、政府部门的信息保护面临巨大挑战，为此，数据备份技术就成了最重要的保护伞。只要能及时对数据进行备份，就能在出现故障的时候避免损失，也不容易出现数据丢失的问题。除此之外，数据备份技术还能降低数据传输途中的流失率，让数据传输更加安全。

（三）防火墙技术

防火墙技术可以归属到传统信息安全范畴，随着科技的发展，

防火墙技术已经取得了长足的进步，经过长时间的探索、研究和实践，防火墙技术已经基本完善，成为保护信息安全的一项重要技术。一般来讲，防火墙可以分为过滤型防火墙和应用型防火墙，防火墙技术一般用于网络内部。应用型防火墙，可以为计算机的运行提供必要环境和保障，它可以在计算运行中，进行全面监控，进而随时发现不良因素对系统的影响，如果防火墙发现病毒，就会即刻切断病毒的侵入通道，继而防止病毒入侵，保障系统安全。过滤型防火墙和应用型防火墙不同，过滤型防火墙能结合计算机特点，对计算机系统进行全面扫描检测，换言之就是对系统的全面查杀，如果发现病毒，就会马上提醒并进行消除。一定程度上说，过滤型防火墙可以将病毒消除在萌芽状态，将数据和病毒进行隔离，保证大数据信息的安全。在防火墙的帮助下，可以避免信息丢失，保证系统运行安全和稳定。

（四）身份识别技术

身份识别技术利用人类的各种特征来实现，比如视网膜、指纹、DNA，由于人类有很多不同的特点，而且一些专有的特点根本无法伪造，而且采集十分方便、可靠，利用这项技术可以对人员进行识别，准确度很高。身份识别技术也有两种方式，其一就是生物认证，其二就是密钥认证。通过研究发现，生物认证的效率和安全性，要高于密钥认证，因为生物认证，是通过人体的特征实现的。密钥认证一般用于保护人们的隐私，其中也有两种方法，称作对称密钥和非对称秘钥。不论什么秘钥，其目的就是为了保护信息安全，应用的时候，按照人们的需求，采用相应等级的密钥即可，继而来保护信息的安全。

伴随着互联网的普及，其共享性和开放性让信息安全受到严重挑战，在信息储存、传输、处理过程中，也存在不少安全隐患，会影响到数据信息安全。因此，用户要提高网络安全意识，使用正确的方法、软件、技术，提高网络安全等级，比如利用杀毒软件定期进行查杀，比如提高防火墙安全等级。只有采取合理的方式和技术，才能对网络信息进行控制和保护，从而营造一个良好的网络环境。

四、计算机大数据的信息安全处理运用策略

（一）设置基于大数据技术的安全服务平台

通过对网络信息安全问题的研究，我们发现，要想从根本上提高数据信息的安全性，需要以大数据技术做支撑，设置一个完备的服务平台。服务系统平台将大数据信息进行统一管理，这样一来，就能构建出科学、合理的授权体系，同时，还能及时了解信息安全情况，如果发现安全隐患，也可以马上进行解决。安全服务系统在运行过程中需要进行自我学习，比如在查杀病毒或者安全检测时候，系统要将各种细节进行记录，如果之后再遇到同样的问题，系统就可以快速处理，进而提高了信息数据的安全。安全服务平台在运行过程中，大数据要对巨量的数据文件安全审查，并要从里面找到有危害的信息，一旦发现，马上将其删除，以保证系统和数据的安全。

（二）注意信息的动态变化

随着信息技术的不断进步，黑客攻击手段也是越来越多样化，因此，就加大了大数据技术处理信息的难度。与此同时，计算机服务器在遭受攻击的时候，仍然会出现很多数据，这样就会让大数据技术面对了更多的难题。为了保证大数据处理信息的效果，在其工作过程中，就要综合发挥各项安全措施的优势。我们要对大数据信息进行动态监控，这样就能实时掌控信息的安全情况，这样一来，我们就能为优化系统，改进信息处理方案提供最新资料。在监控过程中，各色信息的动态变化也要和场景相对应，除此之外，还要考虑到整体的运行变化。系统运行的时候进行实时监控，掌握系统运行的各种变化，再以此为依据优化、调整信息处理系统，进而可以让信息处理系统适应计算机的各种变化。如此一来，就能提高动态监管的安全性和稳定性。

（三）查杀计算机病毒

随着计算机普及和互联网的应用，各色的电脑病毒开始频频出现，所以每台需要上网的计算机，都要安装相应的杀毒软件。比如 360 安全卫士等等，合理使用杀毒软件，可以避免病毒对计算机的损害，也能减少计算机的病毒。然而，在实际操作中，由于一些新型病毒的出现，有的时候杀毒软件也无能为力。对此，就要求计算机使用者，要定期对杀毒软件进行升级和更新，一方面确保杀毒软件的正常工作，另一方面也保证其效果充分发挥出来。杀毒软件可以有效减少木马和病毒，提高计算机系统的安全性，提高计算系统的安全，也就可以保护计算机内数据的安全。

（四）做好计算机硬件设备的管理工作

为了保证计算机系统的安全，就需要加强对计算机硬件的保护和管理工作。对于计算机服务器要定期进行检查和维修，发现运行不畅或者有问题的硬件，要及时进行维修，如果无法维修，就要进行及时更换。对于储存单元，要进行必要的加密和优化，一方面保证数据安全，另一方面要保证系统运行。计算机硬件安全，是保证计算机良好运行的基础，所以，必须要加强计算机硬件的保护和管理工作，并设法提高硬件的寿命和价值，只有这样，才能保证计算机信息的安全，避免因为故障导致的损失，同时也确保信息传递的通畅。

（五）使用专业可靠的认证技术

伴随着科技的发展，出现了多种多样的认证技术，比如人脸识别、语音识别等等，这些技术，可以对信息的安全起到一定的保护作用，防止信息的泄露。如今我国认证技术的应用，可以对使用者进行真实身份识别，从而避免出现盗用的情况，进而保证信息安全。比如支付宝在登陆或者注册时候，需要填写自己的真实信息，还会进行脸部识别，对于密码的设置也有一定的要求。在最重要交易环节，需要用户输入交易密码或者是进行人脸识别，这样就可以在一定程度上，保护交易的安全，从而保护使用者的财产安全。利用可靠的认证系统，可以有效保护数据的安全，进而提升信息系统整体的安全性！

五、结语

如今，大数据信息安全依旧关系到每一个人和每一个企业，只有全方位加强对信息的保护，用科学、合理的信息安全技术才能为信息安全树立一道安全的屏障，继而才能保证信息的安全。对此，我们要从两个角度进行考虑，其一就是保障计算机系统安全，其二就是保证信息安全，我们要从根本上对病毒隐患和安全隐患进行防控，以最高的警戒级别和最高的安全意识，来保护信息和系统的安全。

参考文献：

[1] 胡国正 . 计算机网络信息安全中数据加密技术分析 [J]. 中国新通信，2020，22（15）：46.

[2] 王萍利 . 大数据技术在计算机信息安全中的应用研究 [J]. 科学技术创新，2020（12）：93-94.

[3] 庄绪路 . 大数据技术在计算机信息安全中的应用分析 [J]. 计算机产品与流通 2020（6）：160.

[4] 王渊 . 大数据技术在计算机信息安全中的应用分析 [J]. 计算机产品与流通，2020（11）：187.