大数据技术在计算机信息安全中的应用策略探究

樊雪儿

（宁夏大学信息工程学院，宁夏 银川 750021）

摘要：“互联网 +”时代下，新媒体、网购平台、移动支付潜移默化中渗透进人们学习、生活和工作中，网络数据呈井喷之势，对计算机信息安全带来了不小的挑战。大数据是一种新型信息处理技术，可以提高数据采集、存储和传输效率，自动防御外部黑客攻击、计算机病毒，有效保证用户信息安全，对提升计算机信息安全具有重要作用。本文分析了大数据在计算机信息安全中的关键技术分析，阐述了当前计算机信息安全面临的威胁，提出运用云计算技术保证数据传输安全、运用数据备份技术避免数据丢失、分析威胁性情报与预警信息和进行网络流量分析与入侵检测，全面保障计算机信息安全。

关键词：大数据技术；计算机信息安全；关键技术；安全威胁；应用策略

引言：

随着计算机网络技术的不断发展，人工智能、大数据和云计算等新技术促进了短视频、跨境电商等新兴产业发展，为人们的生活带来了便利。然而信息技术的广泛运用不可避免地引起了各种各样的信息安全问题，例如个人信息泄露、垃圾信息、网络病毒入侵等问题，如何保证计算机信息安全成为社会热点。这一背景下，大数据在计算机信息安全中的优势越发凸显出来，可以自动搜集和储存用户计算机上的数据，及时做好数据备份和加密处理，加强用户数据保护，避免用户数据泄露，智能化识别和阻断计算机病毒、黑客攻击，并及时修复系统漏洞，保证用户账户信息安全。

一、大数据在计算机信息安全中的关键技术分析

（一）云计算技术

云计算是大数据核心技术之一，分为分布式计算的一种，通过网络对计算机内部数据进行分析和计算，把计算程序分解成无数个小程序，利用服务器系统数据进行分析和处理，并把程序计算结果回传给用户，并对计算机中的要数据进行加密保护，避免这些数据被篡改或丢失，从而保障计算机安全。目前，云计算在计算机信息安全中的应用非常广泛，不仅可以提供软件服务、平台服务，还可以通过互联网对数据进行统一管理和调度，有利于降低用户计算机维护成本，及时更新软件，提高计算机存储能力，但是对宽带网络质量有一定要求。云计算技术应用于计算机后，可以借助互联网快速传递数据、保证数据传输安全性、时效性，从而让计算机信息安全得到保障。

（二）数据备份技术

互联网时代下，无论是个人还是企业用户都面对着庞大的数据，这对计算机数据存储空间、存储安全性提出了更高要求。数据备份技术可以帮助用户扩大数据存储空间，把用户数据从主机硬盘复制到移动硬盘、其他硬盘，防止由于操作失误或系统故障导致数据丢失，从而保证计算机数据安全。目前，数据备份技术主要包括了数据库、网络数据和远程镜像等，通过互联网同步备份计算机数据，并使用专业的数据存储管理软件、硬盘来储存数据，设立单独的重要数据备份库，避免数据丢失或被篡改，从而保证数据安全。

（三）大数据处理通用技术架构

大数据在处理计算机数据过程中更加快速、流畅，这是由于采用了 Map reduce 分布式处理方式，重点处理计算机中存储的非结构化数据，主要通过 Mapp reduce 分布式处理程序和 GFS 文件系统对数据进行处理，可以对规模比较大的数据进行智能化处理，并对海量数据进行分割和处理，从而提高数据处理效率。同时，大数据处理通用技术架构适用于不同类型计算机系统，对大规模数据进行快速处理，快速、精准分析数据，为数据库管理奠定良好基础，进一步提高计算机数据安全性。

（四）大数据采集技术

大数据采集技术通过传感器、计算机上安装的 APP 来搜集用户数据，例如用户网页浏览数据、个人文件、视频资源和网络金融交易等数据，并对这些数据进行采集，实时根据数据波动，让数据得到批量操作和访问，从而分析出用户喜好、评估其中隐藏的网络风险，为防火墙运行、杀毒软件防御提供数据参考。此外，大数据采集技术可以深度挖掘用户在计算机上的各类数据，并把数据会传到系统管理平台，便于系统对用户数据进行精准分析，从而为用户画像，对用户隐私数据进行加密处理，进一步保证用户个人隐私数据安全。

（五）大数据分享技术

用户在使用计算机过程中会访问不同网站、访问不同程序接口，产生了大量网络数据。大数据分享技术可以帮助用户在不同网站、程序端口下载数据，实现不同平台数据共享，便于用户在各大平台上传和讨论数据，可以对个人上传的数据进行加密处理，保证个人数据传输过程中的安全性，让个人计算机数据更加安全可靠。

二、大数据时代下计算机信息安全面临的威胁

（一）网络病毒入侵

随着互联网技术的飞速发展，网络病毒成为威胁计算机信息安全的重要因素之一。网络病隐身于邮件、网页和广告中，悄无声息入侵用户电脑，盗取电脑中存储的各类信息，不仅会影响计算机系统运行，还会导致用户个人信息被窃取，影响了计算信息安全。部分不法分子会利用网络病毒对计算机进行攻击，潜伏在计算机中，在用户毫无察觉的情况下窃取或篡改个人数据，尤其是一些个人财产信息，威胁用户个人数据安全和财产安全。

（二）网络垃圾信息

“互联网 +”时代下，微博、抖音、快手、淘宝等成为人们生活中必不可少的软件，在带来便捷生活服务的同时也带来了不少网络垃圾信息，对用户计算机系统运行、信息安全带来了不小的挑战。垃圾信息一般通过网页广告、邮件、游戏等方式进行传播，会占用计算机储存空间，从而拖慢整个系统运行速度，还会植入一些木马程序，窃取用户隐私数据，从而给用户计算机带来不可

逆的破坏。此外，网络信息垃圾还会威胁计算机信息安全，对各个数据库储存的数据进行入侵、破坏，从而导致数据丢失和损坏。

（三）系统软件自身漏洞

互联网技术发展日新月异，这就要求计算机系统软件也要不断进行更新换代，才能防御计算机病毒、黑客攻击，从而保证计算机系统和信息安全。但是很多计算机软件后续更新不及时，没有及时发布更新补丁，系统漏洞无法及时弥补，难以及时评估和防御新版本的计算机病毒，导致用户计算机容易遭到计算机病毒入侵，从而导致系统瘫痪、数据丢失，影响了整个计算机信息安全。

三、大数据技术在计算机信息安全中的应用策略

（一）云计算技术应用于计算机网络信息传播

云计算在计算机信息安全建设中的应用非常广泛，把互联网和相关云平台连接起来，借助云计算技术构建模型，把计算机系统运行过程中的数据存储到云端，节省计算机主机存储空间，从而降低计算机系统运行压力，从而保证系统运行流畅度、保障计算机信息传输过程中的安全性。首先，技术人员可以利用无线局域网构建一个相对封闭、稳定的数据传输网络，确保网络信号覆盖用户计算机、移动设备使用范围，并根据用户需求配置相关技术服务软件，设定好相关网络参数和网络密码，形成完善的网络反馈信息处理模型，全面分析用户计算机数据，并对数据进行分析和处理，确保信息传输过程中的安全性和时效性。此外，技术人员可以利用流程图的方式对计算过程进行呈现，搭建远程信息隐形传递通道，借助云计算计算服务模式对用户数据进行处理，从而提高计算机网络信息传播的安全性。其次，技术人员还可以通过云计算平台分析用户行为数据、网络流量，并对比不同时间段的数据，从中分析出网络异常行为，并识别出其中潜在的攻击行为，一旦方案计算机病毒入侵或系统漏洞，可以向用户发送安全提醒，督促他们对重要数据进行备份，并使用安全软件对计算机系统进行维护，尤其是加强数据库安全管理，进一步提高计算机信息安全性和可信度。

（二）数据备份技术保障计算机信息储存安全

网络环境下，计算机在使用和运行过程中会产生大量数据，只有计算机要有足够的储存空间才能保证系统流畅、顺利运行，从而保证用户计算机信息安全。因此，企业或个人用户要积极利用数据备份技术，对重要数据进行备份，防止重要数据丢失或被篡改，从而保障个人信息安全。例如企业用户要对每天经营数据、客户信息等重要数据进行备份，并设立单独的数据库，定期更新数据库信息，利用 U 盘和网络云端进行数据备份，不断扩大云平台储存空间，从而为重要数据储存做好“双重保险”，提高重要数据储存质量。个人用户要重视数据备份，利用各类软件来备份和保存各类数据，并对个人数据库设置密码，保证个人隐私信息安全。未来，计算机科研人员要利用云平台创造更大的储存空间，对海量数据进行压缩处理，进一步扩大云端备份空间存储量，从而满足企业、个人用户数据备份和储存需求。同时，技术人员还要不断完善大数据分析技术，智能化分析计算机硬盘中储存的各类数据，筛选出其中的重要数据，并对这些重要数据进行自动备份，并自动进行实时备份与更新，从而帮助用户储存更多重要数据。

（三）大数据提高计算机系统防御能力

首先，大数据技术可以对计算机运行过程中的所有数据进行分析，智能化识别出其中的威胁信息，从而发布预警信息，进一步提高计算机系统防御能力。例如大数据技术可以对计算机历史安全事件数据进行分析，识别出其中的风险数据特点、危险信息之间的关联性，处理海量异构数据，帮助用户洞察计算机病毒和黑客攻击，从而更好地防范网络攻击，从而保证计算机信息安全。其次，大数据可以对计算机历史数据进行分析，筛选出其中的危险数据，建立威胁情报预测模型，利用这一模型识别出类似网络威胁风险，一旦发现网络威胁，可以自动进行拦截，从而提高计算机系统安全性，更好地保障计算机信息安全。例如当计算机威胁情报预测模型监测到相似的异常流量、数据波动时，就会认定计算机遭受了计算机病毒或网络黑客攻击，系统会自动发送安全警报，提醒用户及时开启网络防护，及时阻断网络威胁，避免计算机病毒入侵计算机，从而保证用户数据安全。此外，大数据技术可以提前预判网络风险，提醒用户及时升级计算机防火墙、杀毒软件和安全补丁，并调整网络配置，提高计算机系统防御能力，既可以保证计算机系统流畅、安全运行，又可以保证用户信息安全。

（四）大数据应用于网络流量分析和入侵检测

大数据技术可以实时监测、分析计算机网络流量数据，并把实时数据和历史数据进行对别，从而识别出异常流量，识别网络攻击类型、系统漏洞，捕捉到异常信号，并快速分析出网络攻击特点，及时启动相应的网络安全防御，帮助用户抵御网络攻击，保证计算机数据安全。例如大数据技术可以通过机器学习算法建立正常网络流量模型，并设定好正常流量数据峰值，明确计算机网络正常流量行为特征，一旦发现异常网络流量，系统可以第一时间识别潜在的入侵风险，并及时拦截异常流量，提高计算机信息安全行。此外，大数据技术可以对用户行为进行分析，例如用户网页浏览喜好、历史数据、网络使用时间等数据进行分析，绘制用户画像，对计算机系统运行时间、各大账号登录时间等进行监测，一旦发现用户异常行为第一时间进行拦截或身份验证，从而提高网络入侵检测准确性，更好地保护计算机信息安全。例如当系统监测到用户账号登录地址异常、账号登录时间异常，就会被标记为登陆异常，并向系统发送安全警报，要求用户进行身份验证，进一步提高计算机信息安全防御能力。总之，大数据技术在计算机网络流量监测、入侵监测中发挥着重要作用，可以帮助用户实时、智能化监测，一旦发现异常流量、用户账号异常登录，可以自动开启防御和拦截，更好地保障计算机系统安全，提高计算机信息安全性。

四、结语

总之，大数据技术在计算机信息安全中有着广泛应用前景，不仅可以帮助用户智能化收集、分析和管理各类数据，还可以借助云端实时备份数据，从而帮助用户保护重要数据，避免个人信息泄露。技术人员要不断创新和推广大数据技术，把大数据应用在计算机数据备份、计系统防御和网络流量分析和入侵监测中，实时监测计算机网络运行状况，识别网络计算机、黑客攻击风险，拦截计算机病毒和攻击，保障用户计算机信息安全，促进计算机行业健康发展。

参考文献：

[1] 李旭 . 大数据技术在计算机信息安全中的应用分析 [J]. 中国信息界 ,2024(1):93-96.

[2] 李汉尧 . 大数据技术在计算机信息安全中的应用探究 [J]. 电子测试 ,2021(24):3.

[3] 孙冰 . 大数据技术在计算机信息安全中的应用研究 [J]. 电脑乐园 ,2022(2):0106-0108.