

# 计算机数据安全的实现路径

韦 鹏

杭州航策信息科技有限公司 浙江 杭州 310000

**【摘要】**：我国社会进入大数据时代后,需要重点维护和防范计算机网络的安全。考虑到原有的网络技术不能顺应社会发展的趋势,不能满足计算机网络的安全需求,网络非常容易受到攻击。为了有效解决网络安全问题,有必要分析网络自身信息的特点以及影响网络安全和信息安全的各种因素,然后提出相应的解决方案,并创建防火墙技术和防病毒技术,强调应用程序的价值,以实现提高网络信息安全性的目标。在很多情况下,信息安全问题是由内部人员有意或无意的破坏或事故引起的,例如机密存储介质的丢失或被盗,而不是外部黑客和病毒。因此,防止计算机机密信息外泄成为当今信息安全工作中急需解决的问题,而现有的信息安全产品大多是为了防止攻击、黑客和病毒,无法有效防止机密信息外泄。

**【关键词】**：计算机;操作行为分析;数据安全管理系统

## 引言

自从现有的计算机网络发展以来,已经深深地融入了人们的日常工作和生活。数据服务的高效处理实际上可以满足信息共享和信息及时传输的需要。从互联网的角度来看,提高人们的工作和生活质量。然而,互联网在为人们提供便利的同时,也带来了一些安全风险。例如,大多数人在使用电脑时,通常会在网络上存储敏感信息。如果这些信息丢失,丢失的风险将导致更大的经济损失。因此,有必要采用先进技术解决当前计算机网络运行中存在的问题,结合计算机网络运行的特点,提高计算机网络的安全性能,保护用户和公司的数据隐私。

## 1 大数据和计算机信息安全概述

### 1.1 大数据

大数据时代,已有的信息处理机制和互联网得到了优化,但尚未找到有效的计算机信息数据优化途径。存储确保了数据库信息系统的安全性,确定了其价值,提高了数据处理效率。在将数据信息引入网络系统时,如果信息量大,则不仅需要使用物理服务器来处理数据,否则,可能会导致数据重复,这样,数据就可以上传到云计算平台上,方便了信息的及时处理。这是因为云计算的特点是信息资源共享、数据存储量大、信息获取方便。

### 1.2 电脑资讯保安技术

计算机信息安全技术是指利用计算机防止对系统数据和相关信息的恶意外部攻击,在使用以及系统故障排除过程中,操纵导致数据信息缺失等,而且计算机系统可以处于稳定安全的操作环境中。电脑资讯保安需要高科技,包括资讯保安、电脑科技、密码学等。在信息时代,计算机的作用越来越重要,对网络信息系统的需求越来越大,而大数据时代

的到来,给计算机网络的信息安全带来了前所未有的挑战。

## 2 计算机数据安全风险因素

在大数据背景下,既存在问题又存在机遇,影响计算机信息安全的因素很多,不利于计算机网络技术在更广泛的数据环境中的作用。首先主要是人为操作因素、黑客、系统控制因素、病毒因素和网络系统因素。虽然电脑网络正逐渐普及,但对某些电脑系统的认识程度并不足够,这会导致显著和轻微的操作错误,以及影响计算机的安全。在许多情况下,由于用户操作不当,许多敏感数据或信息资源被泄露,同时,一些不法分子可能会植入电脑病毒,不但会破坏电脑程式,更会令整个电脑系统瘫痪,以获得相应的收益。在大数据、巨大计算机信息的条件下,黑客使用了强大的攻击手段,来挑战许多用户的计算机信息安全。其次,计算机系统本身存在一些缺陷,而且在大多数情况下,用户在下载软件或执行任务时可能会遇到信息安全问题。在这个时候,一些犯罪分子可以访问这个系统,这对用户造成了相当大的伤害。最后,在设计生活中,人们对计算机管理的认识仍然很差,这意味着计算机信息泄露的风险很高,其他许多组织,由于缺乏适当的管理,拥有个人信息的人管理计算机信息,这通常归结为信息泄漏。总的来说,在大数据环境下,威胁计算机信息安全的因素很多,本文分析了在更广泛的数据背景下解决计算机环境中信息安全问题的一些技巧。

## 3 计算机数据安全问题应采取防范措施

### 3.1 数据加密保护策略

在计算机网络运行期间,主要目的是传播数据和信息,以便发布各种作战命令,并正确执行内部数据和相关程序的运行。因此,可以将数据旋转模式视为预防和安全控制的关键点。通过对计算机内的敏感文件信息进行加密,可以避免

传输过程中数据被盗的风险。例如，为了提高计算机网络的安全性，采用端加密和行加密。在传输大数据网络信息的过程中，线路加密为各种特征应用密钥。即使这些信息被黑客监听，也无法解码信息内容以保护文件。Endpoint encryption 使用软件对文件信息执行实时加密。当用户收到信息时，应该以特定的格式对其进行加密以读取信息，这提高了信息传输的安全性。

### 3.2 加强规范和业务宣传

在使用电脑时，用户难免会发现操作上的错误和资料泄漏。在某些情况下，电脑制造商可能会与广告商合作，制作有关如何使用某些禁毒工具的资料小册子，如何弥补差距，如何利用网络，让用户获得高质量的售后服务。为了恢复软件和病毒搜索程序，用户可以从应用商店下载整个磁盘，定期扫描，无需单击未知页面，即可确保在安全环境中使用计算机。

### 3.3 数据的存储和循环加密，以确保数据的有效运行

数据的存储与传播对整个网络系统、新型网络系统具有一定的价值，通过在网络上共享和有效地存储和分发数据来确保数据内容的安全。大数据时代是必要的时刻。其中一种存储形式是对计算机网络中的文件进行加密，并通过加密方法不断提高整个系统的安全性，以防止数据资料被盗或遗失。利用密码学保护数据流主要是通过数字签名技术实现的，其目的是保证数据传输过程中不同数据元素的安全性，并在提供加密服务。

### 参考文献:

- [1] 刘晓玲,刘征.计算机数据库安全管理分析与探讨[J].山东轻工业学院学报(自然科学版),2013,27(01):65-68.
- [2] 李瑞林.计算机数据库安全管理研究[J].制造业自动化,2012,34(10):24-26.
- [3] 曲亮.计算机数据库安全管理探析[J].网络安全技术与应用,2013(10):29+31.
- [4] 田驰.计算机数据库安全管理分析[J].吉林省教育学院学报(上旬),2014,30(01):153-154.
- [5] 周鑫辉.大数据时代下计算机网络信息安全问题[J].轻纺工业与技术,2020,49(1):151-152.
- [6] 滕飞.大数据时代计算机网络信息安全及防护研究[J].电脑编程技巧与维护,2020,14(2):167-169.
- [7] 陈哲,郑佳佳.大数据时代计算机网络信息安全与防护措施[J].信息与电脑,2020,32(1):199-200.
- [8] 冯庆亮.大数据时代计算机网络信息安全与防护策略研究[J].企业科技与发展,2020(1):94-95,98.
- [9] 陈璐.试析大数据时代的计算机网络安全及防范策略[J].数字技术与应用,2020,38(07):193-195.
- [10] 毛颖.大数据时代计算机网络信息安全探讨[J].科学技术创新,2019(20):74-75.

### 3.4 使用适当控制技术的网络黑客

最近监控技术在韩国很普遍，很多电脑公司都在积极发展各种与电脑相关的控制技术，如统计、人工智能、密码等。应用监控技术的主要目的是控制计算机的运行状态，判断系统是否被病毒和黑客入侵。当计算机系统受到非法入侵时，监控技术允许分析和识别黑客攻击，并得到统计数据的支持，改进了系统的运行，减少了黑客非法入侵给用户带来的不必要的损失。

### 3.5 网络防火墙

防火墙主要是访问有效内部控制网络的一种手段，而且采用网络防火墙可以有效地阻止外部用户非法进入网络系统，从而为内部提供有效的保护网络环境，使网络运行稳定，该技术能够有效地保证网络交互的安全性，同时也能有效地验证网络传输的相关数据并确定目标网络数据传输的可能性，使用各种技术来创建目标防火墙访问控制，消除威胁，有效保证了内部网络环境的正常运行，保证了网络中可靠的信息安全。

### 4 结语

因此，计算机网络中的信息安全问题往往出现在信息时代的大背景下，对整个企业的信息安全构成威胁。因此，在使用计算机系统时，必须注意数据和信息的安全管理，完善相关的保护系统，数据控制机制，采用现代安全管理方法，促进数据信息的安全使用。