大数据时代计算机网络信息安全与防护对策研究

李志中
（广东东软学院，广东 佛山 528225）

摘要：首先，对大数据、计算机网络信息安全进行概念界定，并详细阐述了大数据与计算机网络信息安全的特点。以此为基础，对大数据时代计算机网络信息安全存在的问题及导致问题出现的原因展开深入剖析。然后通过大数据时代加强计算机网络信息安全防护必要性与迫切性的分析，从完善计算机网络安全体系，应用防护墙技术、身份认证技术、数据加密技术、密钥管理技术等多个角度提出了大数据时代计算机网络信息安全防护对策，希望本文的相关研究能够为大数据时代的计算机网络信息安全防护动作的高效开展提供借鉴。

关键词：大数据时代；计算机网络信息安全；防护对策

在全球一体化深入推进的今天，互联网、大数据、云计算、物联网、人工智能等先进技术相继出现并得以迅速发展。特别是在近几年，随着移动智能终端种类的日益丰富与快速普及，在互联网技术的推动下，社会各个领域、各种类型的数据信息呈现出井喷式的增长态势，大数据时代随之到来。

大数据时代，数据呈现出数量庞大、种类繁多、价值密度低、利用价值大、传播迅速的新特点，为人们挖掘、传递、研究、利用各类信息提供了可靠的数据支撑。当前我们尚处于“物联网”的初级阶段，但是随着信息技术的快速发展与成熟，大数据也表现出了更加广阔的开发与利用空间。

但是由于大数据本身的特点，也使得计算机网络信息安全面临着严峻威胁，各种秘密数据、敏感信息被禁窃取、遭泄露的风险不断增加。因此，加强计算机网络信息安全防护，确保各类数据信息的安全性，对于大数据时代各个领域的数据信息的安全发展有着重要意义。现阶段，虽然人们已经意识到数据的重要性，但是仍有部分人并未全面认识到数据爆炸性增长为网络信息带来的安全隐患。

现有网络安全防护体系中的很多方法与策略在面对大数据时代背景下更为庞大的数据量时，无论从安全保障系数还是可操作性等各方面，都存在严重缺陷与不足。因此，我们应在深入研究大数据自身特点以及大数据时代计算机网络数据信息所面临的各种安全威胁的基础上，建立一套与大数据环境相适应的计算机网络信息安全防护体系，以确保大数据能够最大限度地发挥其效能，实现计算机网络数据信息的安全化管理。

一、相关概念界定

（一）大数据

1. 大数据的概念

大数据这一概念最早是由美国学者阿尔文·托夫勒于 20 世纪 80 年代发表的《第三次浪潮》中所提出，他热情地赞颂大数据是“第三次浪潮的华彩乐章”。但是，“大数据”这一概念的真正流行是在 2009 年以后才开始的。

大数据（Big Data），是指以计算机技术为依托的数量巨多、体量庞大、常规数据处理技术难以对其进行高效、及时提取、搜索、分析、处理以及存储等操作的数据信息。

大数据的出现与发展从侧面说明，随着信息技术的快速发展，数据处理框架与模式已经发生了天翻地覆的变化，大数据时代的信息处理方式要更具高效性、智能性、经济性。

2. 大数据的特点

概括来讲，大数据的特点可以通过“4V+C”进行描述，即 Volume、Variety、Value、Velocity 以及 Complexity。

Volume 表示大数据数量之多、规模之庞大。常用的 GB、TB 等数据表示单位已不再适用于大数据的描述，我们在表述大数据时，往往会用到 PB（1024TB）、EB（1024PB）以及 ZB（1024EB）等单位。国际互联网数据中心预测，全球到 2025 年，智能互联设备的数量将会达到 1500 亿台，这些设备将产生高达 175ZB 的互联网数据总量。这些数据足以说明大数据之规模庞大的特点。

Variety 表示大数据数据结构之多样化。进入大数据时代，数据类型日益复杂、多变，在海量数据中不仅包括常规的结构性数据，还包括各种非结构性的数据信息，如视频、图片、音频、文字等。随着物联网、云计算等技术的日益成熟，互联网数据来源逐渐趋向多元化，包括互联网终端用户在应用互联网的过程中产生的各种类型的数据信息；各种信息管理系统以及互联网设备在运行过程中产生的操作日志、文件、数据库等；包括应用于智能家居、医学诊断、生物工程、环境保护、海洋探测、工业生产等领域的物联网传感设备与信号采集设备所产生的各种数据等。

Value 表示大数据价值之密度低。大数据虽然有着非常庞大的规模，但是能够为决策提供有效支撑的数据是非常有限的，对大数据的获取与利用还需要我们在海量的数据中对有利用价值的信息进行深入挖掘。巨大的数据基数与有限的价值量之间比例悬殊巨大，由此可见，大数据价值密度之低。而正是由于大数据的价值密度较低，才需要我们通过更加精密的计算方法挖掘大数据的价值。

Velocity 表示大数据信息处理速度之快。鉴于大数据规模庞大、但价值密度却相对较低的特点，如何更快地在海量大数据中挖掘、提取有效信息成为大数据能否发挥其本身价值的关键所在，这要求大数据具备更快的传递速度、更高的处理效率。

大数据时代，随着信息更新速度不断加快，数据处理技术也要与时俱进，不断提升数据处理能力，这也是大数据时代信息处理的又一显著特点。

Complexity 表示大数据之复杂性。大数据的复杂性特点是由其规模的庞大以及数据类型多样性所决定的。大数据时代，数据的复杂性已成为影响数据分析与处理效率的关键因素。

（二）计算机网络信息安全

1. 计算机网络信息安全的概念

信息安全这一概念提出时间并不长，当前世界各国尚未对其建立统一认知。早在 2001 年召开的地 56 届联合国大会上，为更好地处理信息安全问题，世界经济文化组织就号召与会各国统一信息安全的基本概念，并就信息安全问题加强国际交流与合作。

随着信息技术的快速发展，各国对计算机网络信息安全的认知也在不断更新。2002 年，美国联邦信息安全管理法案中规定的网络信息安全的五个特征，是当前国际上对计算机网络信息安全比较统一的认识，即信息的保密性、信息的完整性、信息的可用性、信息的可控性以及信息的抗否认性。

在此基础上，我国学者将计算机网络数据信息安全进行了进一步分解，具体包括信息环境安全、信息系统安全、网络程序安全、网络数据安全四个方面。此外，还有学者认为计算机网络信息安全涵盖了网络安全、病毒防范、访问控制、操作系统安全、数据库安全以及加密与鉴别六个方面。

总之，计算机网络数据信息安全涉及到计算机科学、网络技术、信息安全技术、通信技术、密码技术等多项技术。从广义范围来看，计算机网络信息安全包括信息的真实性、保密性、完整性、可控性等；而从狭义角度分析，计算机网络信息安全指的是各项网络服务与网络信息的安全性，包括各种硬件、软件以及数据的安全。

2. 计算机网络信息安全的特点

（1）脆弱性

互联网本身具有开放性，而正是其开放性导致了计算机网络信息安全的脆弱性。开放性会带来各种不安全因素，互联网越开放，计算机网络数据信息就越不安全。计算机网络数据信息安全的脆弱性体现在计算机系统设计、应用以及维护等各个环节。

在计算机系统的设计阶段，虽然已经考虑到信息安全的相关公威胁，也难以真正做到无懈可击。在计算机系统的具体操作与维护阶段，受系统使用者的操作水平、系统管理员的维护程度等多方面因素的影响，容易暴露出计算机系统的安全漏洞，再加上各类软件本身的复杂性特征，计算机网络数据信息安全问题也就随之出现。

所以，无论是客观设计缺陷还是主观操作失误，都会影响到计算机系统的安全性，导致计算机网络系统的每个环节都存在被攻击的危险，进而出现文件受损、传输泄密以及网络瘫痪等不同程度的后果。

（2）突发性

计算机病毒往往是造成计算机网络信息安全遭到突发性破坏的主要因素。计算机病毒是指人为造成的，能够在计算机系统中快速传播与复制的代码或指令。计算机病毒具有破坏性、可复制性以及传播性等特点，其爆发通常是突发的、不可预见的。一旦发生，就能够快速地破坏计算机系统中或者应用程序中的数据，进而严重影响到计算机的正常使用，甚至会威胁到计算机系统中国的数据、信息安全。

此外，计算机病毒同时还具有潜伏性，计算机病毒在经过人为设计并植入系统后，很多时候并不会立即表现出其破坏性，而是共生于合法程序中，就好比一颗定时炸弹。但是病毒在计算机系统中潜伏的时间越长，所获取的资源就会越多。在其潜伏期间，并不会影响计算机程序的正常使用，但病毒一旦爆发，就会迅速蔓延，在短期内导致信息泄露与丢失，甚至网络系统瘫痪的严重后果。作为非传统安全领域中的一个关键问题，信息安全问题所产生的破坏性往往会在没有任何察觉的前提下，攻击计算机安全防护系统。因此，鉴于计算机网络数据信息安全的突发性特征，信息安全部门应做到防患于未然，最大限度地降低其危害。

（3）全球性

信息时代，信息传播速度之快、范围之广，是信息传播领域前有未有的。互动、互联的互联网将全球汇聚为一个“地球村”。近年来，随着新媒体技术的快速发展，各类网络安全问题也逐渐暴露出来。

2020 年，欧洲某银行遭遇史上最大规模的 DDoS 攻击，其网络遭遇美妙 8.09 亿数据包的洪水攻击；2020 年 8 月，澳洲大学在线考试系统遭黑客攻击，数十万用户数据被泄露；2020 年 1 月，英国教育部网站数据库被入侵，泄露 2800 万未成年人数据；2020 年 11 月，俄黑客被指入侵美政府多个机构，超九成 500 强公司受到影响……类似事件不胜枚举。数据表明，在全球范围内，由于网络安全问题而导致重大经济损失事件时有发生。俄罗斯储蓄银行发布报告称，2018 年因网络攻击导致世界经济损失 1.5 万亿美元，2019 年损失达到 2.5 万亿美元，增长 60%。

从以上数据可以看出，计算机网络信息安全是全球性问题，没有国界限制，再加上互联网本身完全开放的特点，更是为网络阿全攻击行为提供了可乘之机。因此，大数据时代的计算机网络数据信息安全问题，还需要世界各国深化国际合作，才能更好地保护计算机网络数据信息安全。

二、大数据时代计算机网络存在的信息安全问题

（一）计算机网络系统存在安全漏洞隐患

Windows、Linnx 等系统是当前多数计算机设备所搭载的主流系统。但是这些系统本身也存在一定的漏洞，一旦遭到非法访问者的攻击，就极易出现网络瘫痪或系统崩溃等一系列问题。计算机用户在使用各种软件、程序下载网络资源时，部分病毒、木马就会随着网络资源植入计算机系统，并持续攻击计算机系统本身存在的安全漏洞，造成重要信息被窃取、系统崩溃等一系列问题。

此外，很多用户在安装程序、解压网络文件时，也时常会因为计算机系统本身所存在的漏洞，产生访问权限误报、难以抵御病毒攻击等各种安全漏洞，从而严重影响局域网或 Internet 网络中的数据信息安全。

（二）网络黑客攻击导致的信息安全隐患

大数据时代，计算机网络数据信息攻击呈现出隐蔽性特点，计算机网络数据信息面临着更加严峻的安全威胁，网络攻击手段也更加多样化，如网络黑客攻击、信息破解、人为网络入侵等，而大数据本身的低价值性，很多具有利用价值的数据信息，其完整性、安全性都被湮没于海量的网络数据信息中，从而导

致部分具有利用价值的信息受到非法访问者以及其他垃圾信息的攻击。

部分非法访问者为了获取其所需要的信息，窃取有价值的数据资源，会通过各种非法手段破解计算机系统所设置的访问权限，从而导致计算机网络系统中的重要数据信息遭到泄露、窃取甚至非法利用等安全威胁。

（三）木马病毒入侵导致的网络信息安全隐患

计算机网络数据信息的访问、传输与存储，具有开放性、共享性以及互联性等特点，而计算机网络信息的这一特点，刚好为木马病毒的入侵与传播提供了可乘之机。木马病毒是以相应的木马程度为载体，来控制接入互联网的计算机设备。这些木马病毒大多藏匿于各种网站、各类应用程序以及软件安装包中。

木马病毒入侵计算机网络系统，木马病毒会从远程客户端操控计算机系统，通过打开网络端口、发送数据的方式，窃取计算机网络中的各种数据信息，而且木马病毒一旦入侵，会长时间驻留在计算机系统的各种软硬件设备中，进而侵害整个计算机网络系统，导致计算机系统崩溃、数据信息遭到窃取，像 CIH 病毒、引导区病毒都是颇具代表性的木马病毒。

（四）网络操作不导致的网络信息安全隐患

计算机网络用户在对计算机网络系统进行故意操作或无意操作时，都有可能造成网络数据信息安全隐患，尤其是在进行网络购物、网站访问等数据信息操作时，会根据网络系统提供的提示信息，执行多种数据访问步骤，这就有可能泄露个人或政企机构的隐私，为非法分子窃取数据、获取信息提供便利。

由此可见，计算机网络用户在操作计算机系统的过程中，也会为计算机网络信息带来安全威胁，甚至造成严重后果。再加上很多计算机网络用户信息安全防护意识淡薄，鲜少关注网络信息安全问题，在网络信息安全漏洞处理方面经验不足，也在一定程度上加大了网络信息被非法访问、窃取与破坏的风险。

三、大数据时代加强计算机网络信息防护的必要性分析

大数据时代，数据信息已成为包括企业、行业、社会甚至国家等多个层面在内的激烈竞争的重要战略资源。进入大数据时代，随着各类数据、信息的爆发式增长，计算机网络信息安全问题被逐渐暴露出来。

随着数据总量的不断增加，大数据安全风险也在不断上升。大数据作为大数据时代各类机构，特别是各类企业、科研机构的重要资产，成为增强其核心竞争力的有力武器。因此，大数据时代的计算机网络数据信息安全问题更加需要人们的关注。

（一）大数据网络攻击具有严重危害性

大数据具有庞大的数据规模，它们分布式存储于互联网各个端口。这种存储方式使得数据处于相对简单的保护状态，很容易被网络黑客发现其所存在的漏洞而受到非法攻击，轻松实施高持续性威胁（APT），从而导致网络信息安全问题的出现。

大数据背景下，各类互联网终端用户数量巨大，《2020 年中国互联网发展趋势报告》中显示，2020 年我国移动互联用户已达 10.8 亿，全球互联网用户数量达到 46.48 亿。

在数量如此庞大的互联网终端用户中，其构成结构也极具复杂性，这些规模庞大、结构复杂的网络用户在对计算机网络系统进行访问时，其安全防御系统难以快速、实时、精准地分析、判断出访问用户的合法性、安全性，从而在一定程度上为高持续性安全威胁攻击（APT）提供了“可乘之机”。

难以有效监测 APT，是大数据时代计算机网络数据信息安全所面临的最大威胁。2020 年 11 月 14 日，据路透社和《华盛顿邮报》报道，知名 IT 公司 Solar Winds 旗下的 Orion 网络监控软件更新服务器遭黑客入侵并植入恶意代码，导致美国财政部、商务部等多个政府机构用户受到长期入侵和监视，甚至可能与 FireEye 网络武器库被盗事件有关。

奇安信 CERT 安全专家 rem4x@A-TEAM 认为，这是一场足以影响全世界大型机构的软件供应链攻击，具有极大的战略意图。APT 本身所具有的安全威胁大、攻击时间长、攻击针对性强等特点，使得 APT 所造成的网络数据信息安全问题极易突然爆发，且危害时间持续较长，再辅以相应的数据挖掘手段，黑客就能够轻而易举地从互联网终端获取有用的数据信息，从而导致数据遭到泄露，造成严重的网络信息安全问题。

（二）大数据加大了用户隐私泄露风险

现代生活对互联网的依赖程度越来越高，互联网用户的所有数据信息都会被实时记录下来。而这就增加了用户个人隐私数据信息的安全隐患。若缺乏完善的用户隐私数据安全保护机制，一旦用户仅操作不当，就可能会导致个人隐私数据遭到泄露。

大数据时代网络用户个人隐私数据信息的保护，需要功能强大的数据分析技术以及成熟完善的数据保护机制为其“保驾护航”，以不断提升数据信息安全系数。

反之，如果大数据管理系统的管理机制不成熟、不完善，可能会导致计算机网络系统的用户界定、用户分配以及部分用户隐私数据信息安全等方面出现漏洞，从而威胁到用户个人隐私数据的安全。

因此，我们在通过计算机系统进行数据采集与挖掘的过程中，要将保护用户隐私数据安全放在首位，要在确保不泄露用户隐私数据的前提下进行数据的合理获取与利用。

现有技术下，大数据的采集与存储都是通过云计算平台对其进行分布式运算，在此过程中，数据信息的安全性主要体现在数据分布计算与交换的过程中，对用户隐私数据的合理获取与安全利用。

此外，大数据的数量本身就不是固定的，数据无时无刻不在产生，数量也会随着用户行为而动态增加。传统的数据保护技术主要服务于静态数据，因此，对用户隐私数据的安全保护，还需要我们关注如何更加有效地应对大数据本身所具有的动态拓展属性。

最后，大数据区别于传统数据的一个重要属性就是其本身的复杂性，因此，我们在考虑、解决计算机网络系统中用户隐私数据的安全性问题时，还要关注现有的数据保护技术能否应对大数据的复杂属性。

（三）大数据的数据存储存在隐患

大数据无论从数据类型还是数据结构等各个方面，都是传统数据不可比拟的。在大数据存储平台，大数据的增长速度呈现出非线性甚至指数级的现象。

数量如此庞大的数据在其存储过程中，必然会出现并发且频繁无序运行多种应用进程的问题，进而导致出现大数据存储错位以及管理混乱的问题，为大数据的存储与后期处理埋下安全隐患，但是现阶段的数据存储管理系统能否满足海量数据的存储需求还有待考验、论证。所以，在大数据存储环节同样处在严峻的信息安全问题。

四、大数据时代计算机网络信息安全防范对策

（一）完善计算机网络安全体系

计算机网络安全体系，主要包括网络安全硬件、操作系统以及通信协议等元素。计算机网络安全体系是一个具有开放性的互联模型，该模型中包括应用层、网络层、数据传输层、数据链路层以及物理层等多个层级结构，而在这多个不同的层级中，又分别存在着由多种网络安全模块以及会话协议所构成的数据服务机制与数据管理机制。

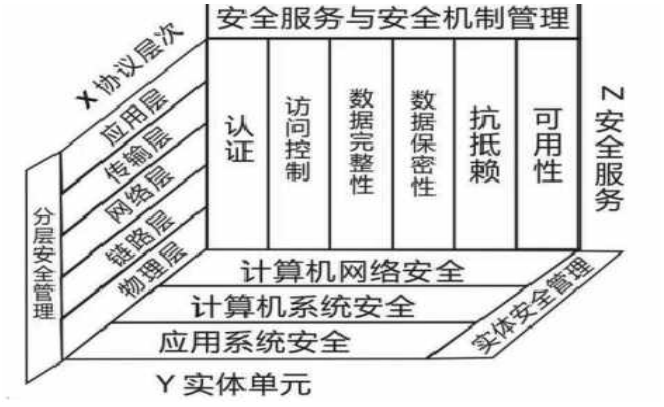

图 1　计算机网络安全体系结构框架

计算机网络安全系统这一互联模型，为用户提供包括身份认证、个人信息保密、数据访问控制等在内的多项安全服务。计算机网络安全系统在执行这些服务时，会沿着X、Y、Z三个轴向延伸，从而能够为计算机网络系统、网络数据以及计算机网络系统中的各类应用程序提供充分的安全保障。计算机网络安全体系的结构框架如图 1 所示。

计算机网络安全服务平台主要由安全服务、通信协议以及安全机制管理等多种服务结构构成，能够有效满足不同网络数据访问、传输以及存储的使用要求。

依托 TCP/IP 协议，不同网络层级的数据通过网络空间信道，分别选择相应的安全管理层级，实现对外来用户的身份认证、信息传输以及数据访问等活动的管理与控制。外来用户只有通过身份验证，才可顺利进入计算机网络系统，进行数据访问、数据下载以及数据传输等操作。反之，则无法对计算机网络系统进行相关操作。

（二）应用防护墙技术，加强网络信息安全防护

在计算机网络系统中，防火墙是控制外来用户访问、数据传输的重要端口。防护墙是由应用网关、验证工具、服务访问规则、包过滤等多个构件组成，能够有效隔离、控制专用网与公用网、内部网与外部网之间的通信数据。

在众多防护墙组成构件中，包过滤防火墙作为网络层中最为关键的控制网络，能够对 IP 地址、TCP 数据分组、数据包出入接口以及 UDP 报文数据端口号进行准确分析，同时还可精准过滤携带 IP 地址的封装数据包，快速识别网络中的 TCP/UDP 数据包。

防火墙通过对此、分析网络管理员设定的访问控制数据与网络传输的各种数据信息，从而有效控制各种数据包的输入与输出。因此，可以将包过滤防火墙应用于多种不同的通信协议网络中，通过查验网络层中的 UDP、TCP 以及 IP 报头字段，有效防护各种不明网络攻击。

应用代理防火墙与包过滤防火墙的区别在于，自防火墙主要用于阻断内、外网络之间的通信。当应用代理防火墙发现有外部用户访问时，会自动对外部用户所传输的数据信息是否安全进行分析、审核。分析完成后，应用代理防火墙会通过网络通信协议与相关代理程序，将经过分析的数据信息传输至内网服务器，并自动筛选、舍弃其中具有安全威胁、不符合要求的数据，打通内网与外网之间的信息通道，确保计算机网络输入信息的安全性。

而从防护功能的角度来看，状态检测防火墙汇集了多种防火墙所具有的优势，能够对所截获的传输数据包进行全面分析与检查，还可在应用层随机抽取相关的状态数据信息，并将所抽取信息与计算机网络管理员所设置的通信协议、访问控制数据表进行对比，根据对比结果决定是否对向内网传输数据包中的数据。状态检测防火墙的优势还体体现在，它在处理、分析传输数据包时，速度更快、灵敏度更高。因此，状态检测防火墙更适用于网络数据包的筛选与甄别。

（三）应用身份认证技术，加强网络信息安全防护

计算机网络数据信息访问过程中的身份认证，是指通过相应的身份标识对操作者的真实身份进行识别与鉴定。身份认证往往会涉及到多方面内容的认证、审计与授权，从而有效避免合法用户被网络攻击者假冒、侵犯，威胁网络数据信息安全。

身份授权则是指在确认网络访问用户的身份后，计算机网络系统会赋予其相应的文件操作、数据访问的权限。身份审计是指访问用户在计算机网络中所进行的一切访问与操作行为，都会被计算机网络系统实时记录下来，以便于后续进行通信操作主体的核查。

计算机网络系统通常会通过 API 调用数据访问、Kerberos 授权以及动态口令等多项技术对网络访问者身份进行访问，从而实现对网络数据的有效监管与安全防护。

在此过程中，计算机网络身份认证系统会自动审核、验证访问用户所发送的动态口令，并通过使用与动态口令相匹配的网络密钥，实现对网络系统中各种数据信息的访问控制。

（四）应用数据加密技术，加强网络信息安全防护

一般来说，数据加密技术可分为端到端加密、节点加密以及链路加密等技术。借助多元化数据加密技术，能够有效提升数据信息在网络信道中传输的安全性。数据加密技术是一种将网络中所传输的各种明文数据信息按照一定的规律，转变为相应的密文，再将转变后的密文转变为明文的加密方式，在数据加密过程中，一般会使用对称以及不对称两种秘钥进行加密的类库中，以确保数据接收方能够正确解密所发送的密文。

其中，针对全部计算机网络的加密处理需要用到链路加密技术。在进行数据处理时，数据在所有链路节点的传输都是加密的，每个链路节点在接受到上一个链路节点传输的加密数据信息后，通常都是先对其执行解密运算然后再对其进行加密，以此有效保证数据信息在每个不同链路节点传输过程中的安全性。

与链路加密技术类似的是，节点加密技术通常是对各数据节点间的数据进行加密，而后通过解密运算等操作。此外，可通过K链路秘钥对网络中的各类数据进行加密处理，从而全面提升数据资源在传输过程中的安全性。

端到端加密技术是指对数据源的结点、目的结点两部分进行加密的一种数据加密方式。对于计算机网络信道中所传输的报文数据的加密，为最大限度地减少传输中间节点所存在的通信干扰，会使用源节点数据加密、目的结点数据加密的方式。

但是由于数据信息在网络信道传输过程中经常会遭到不明原因的攻击，因此，在对数据信息进行加密时，通常会使用多种加密法技术相结合的方式，通过链路加密技术、节点加密技术以及端到端加密技术相结合，有效提升数据信息在网络通信传输过程中的安全问题。

（五）引用密钥管理技术，加强网络信息安全防护

密钥管理技术是依托大数据云计算技术的密钥管理与维护功能，对储存于云服务器中的密钥进行有效管理。计算机网络用户在云计算服务平台登陆个人账号后，可以自动获取相关私钥，以有效满足自身操作需求，以此顺利访问、获取、控制网络系统中的数据资源、应用程序。

在密钥交换与管理的过程中，需要运用EDI电子数据交换技术、DES算法加密等技术，以此为各类数据信息的访问、传输与存储提供相应保护。若用户想要重置、更改云服务器中所设置的密钥，则需要通过程序设计对称密钥的加密、解密方式，以确保对计算机网络系统中密钥的统一分配与管理。

（六）利用大数据安全技术，加强网络信息安全防护

借助大数据安全技术，能够从物理、系统、网络、存储、访问、审计与运营等多个角度保护计算机网络信息安全。在大数据的生命周期中，大数据安全技术能够有效防护计算机网络数据信息产生、采集、传输、分析、处理、存储与应用等所有环节。充分利用现有的大数据安全防护技术，能够有效提升数据信息的安全系数，从而有效规避数据泄露、数据篡改、数据丢失以及越权访问等安全问题的发生。

因此，大数据时代的数据安全技术也要通过设计更多的工具产品、完善相关技术标准、构建相应的安全规范、提升安全服务质量等方式，来对网络信息进行安全防护。

首先，利用相关工具产品，采取相应的安全防护策略，建立完善的大数据信息安全模型，并在数据收集、整理与存储阶段，划分具体的数据类型；利用“数据树”等相关大数据处理程序，自动性、持续性地对大数据的类型、价值、安全性进行分析、审计与评估，为后续快速、高效提取、处理价值数据奠定基础，从而确保在大数据况下的各个节点间都能够实现加密安全通信，最大限度地降低大数据在传输过程中遭到攻击威胁。

与此同时，在收录、存储各类数据信息的过程中，还要注意随时标记所处理的数据，在增强大数据安全系数的同时，不断提升大数据处理效率与质量。

在大数据存储过程中需要添加数据标识时，若数据库中没有关于该标识的记录，则会直接将该标识存入数据库内。若该标识已经存在于数据库之中，该数据将会被直接存入数据库。

在数据标识存入数据库后，计算机系统用户可借助相应的大数据处理程序对数据进行快速处理，以便于后续数据的提取与进一步处理。基于分布式计算的大数据框架下，在数据传输过程中，对数据进行加密处理是极为重要的一环。

对此，可通过在大数据框架的服务器端与客户端分别配置相应的数据传输加密配置文件，实现对通信数据与密钥的分别存储，以不断增强数据在分布式数据框架下传输的安全性。

在大数据储存过程中，对大数据的动态监控与安全存储也是其中的重要一环。在对大数据进行动态化监控与存储的过程中，要安全监控存储程序，实时监测数据存储进程，以获取动态性的存储数据，并以此为依据完善计算机网络系统信息安全监控机制，从而确保大数据动态并发存储的有序进行，使得增强网络数据信息管理系统的安全系数与可靠性能。

五、结语

总之，大数据时代的计算机网络信息安全监管，需要在进一步完善计算机网络安全防护体系的基础上，借助大数据安全技术、身份认证、密钥管理、数据加密等多项技术，加强对计算机网络系统中用户访问、数据传输以及数据存储的安全防护，才能最大限度地避免信息安全问题的发生，确保计算机网络信息系统的安全运行。

参考文献：

[1] 王小朋 . 试论虚拟专用网络技术在计算机网络信息安全中的应用 [J]. 网络安全技术与应用，2021（02）：10-11.

[2] 宋泱瑾 . 大数据背景下计算机网络信息安全风险和解决对策研究 [J]. 电子元器件与信息技术，2021，5（01）：26-27.

[3] 沈宏吉 . 计算机网络应用安全问题分析与防护措施探讨思路总结 [J]. 数字技术与应用，2020，38（12）：190-192.

[4] 任洪波，吴咏梅 . 计算机网络信息安全技术研究 [J]. 石家庄铁路职业技术学院学报，2020，19（04）：51-55.

[5] 刘亚楠 . 大数据时代计算机网络信息安全及防护策略浅析 [J]. 信息与电脑（理论版），2019（06）：212-213.