最新大数据与信息安全论文(模板5篇)

无论是身处学校还是步入社会，大家都尝试过写作吧，借助写作也可以提高我们的语言组织能力。那么我们该如何写一篇较为完美的范文呢？下面是小编为大家收集的优秀范文，供大家参考借鉴，希望可以帮助到有需要的朋友。

大数据与信息安全论文篇一

移动互联网在使用中更为方便快捷，移动通信设备体积较小，方便携带，因此移动互联网也呈现了相同的优势。移动互联网的出现打破了时间和地点的限制，人们可以借助移动互联网在任何时间和任何地点查询所需信息。

1．2有利于个人隐私的保护

在计算机上网的时代，人们的个人信息很容易受到安全隐患的威胁，用户上网的过程中，骇客可以得知用户正在浏览的内容，甚至还能够获取用户的个人信息，此外，计算机互联网还有较强的公开性，因此私人电脑端的用户信息查询相对比较容易。而移动互联网的用户不需要将移动设备之中的信息分享给其他人，因此保证了用户个人信息的保密性。用户上网活动的随机性也会有所增强，所以信息安全性也得到了显著提升。

1．3移动互联网具有更强的即时性和实用性

移动互联网可以营造更为优良的使用环境和使用条件，进而更好地满足用户的个性化需求。如利用移动互联网用户可以随时随地接发邮件，从而实现线上办公和线上购物等目的。而在传统的互联网形式中，只有在家中或办公室这种能够容纳上网设备的地点才能实现，所以移动互联网的应用很好地摆脱了上述因素的限制。

大数据与信息安全论文篇二

本文重点分析影响计算机网络系统正常运行的几大因素，从不同的方面了解计算机网络安全运行的情况，让一些不利的因素消失的萌芽状态，避免给我们带来不必要的麻烦和损失。

首先，平时要保持设备所处环境的温度不要过高，因为在设备运行时会产生很大的热量，一些设备的损坏都是因为设备的温度过高，所以要定期对空调进行检查看看运行是否正常，还有就是灰尘也可能导致设备温度过高，灰尘落在设备的通风口处使之设备的cpu及其他部件产生的热量释放不完全，久而久之就就会使设备内部部件老化，所以我们要保持所处环境的整洁。其次，设备所处环境一定要有稳定的电源输入和输出，比如ups等不间断供电系统，以避免忽然停电给设备造成的损坏，还有就是电源要有可靠的接地和避雷设备防患于未然，不要因为小失大。最后就是防盗，如果有很重要的信息，比如历年的高考招生数据或者是企业的商业机密信息资料，这些都是内部的机密资料，是不能外漏的，一旦硬件丢失造成的后果是不可估量的，所以在设备机房要有专门的监控系统并且进入者要有一定的要求。

首先我们就说一下系统漏洞的问题，我们熟知的windows操作系统，这也是我们用的最多的操作系统，一些不法分子也就通过他本身的系统漏洞来侵入我们的计算机，窃取我们的重要资料和个人隐私，由于这些系统本身的漏洞是因为系统设计之初从硬件、软件和计算机协议方面的缺陷所造成的，所以他不仅对我们个人有很大的危害，还对系统本身有很大的危害，为了使系统漏洞给我们来的各种危害降至最低点，我们应该很客观的认识这个问题，漏洞的出现是随时的，没有特点的时间也没有特点的地点，只要是我们对系统进行了改动或是系统本身的某一方面的更新，都会出现漏洞，对我们系统造成危害的漏洞主要有以下几种：

1、是vm漏洞，这中漏洞可以直接导致我们计算机里的重要信息和重要文件的丢失，不法分子主要是可以通过vm漏洞，使自己的dll文件设置在计算机上之后，和系统本身的文件一样运行，以达到他的目的性。

2、是rdp漏洞，这中漏洞主要是在我们和远程计算机正常通信的时候产生的，使得我们的获取对方的信息失败，致使我们的系统运行出现错误。

3、是我们再安装一些软件时候出现的漏洞，因为有些软件需要在因特网上更新或是注册，所以在安装过程中会打开某些我们平时用不到的端口，往往这些端口也就给了不法分子可乘之机。

1、就是养成经常给系统打补丁，清理插件和对机器进行整盘扫描病毒的习惯，这样就可以让我们很快的知道系统本身存在的问题，及时处理以免发生亡羊补牢。

2、是及时更新杀毒软件的病毒库，这样可以对进入我们系统的每一个文件进行更好的扫描，以免木马程序乘虚而入。

3、是重新安装系统，系统漏洞如果很多，病毒程序就会很快侵占我们的电脑系统，为了更好的保护我们的信息资源，重做系统不失是一个好的办法，这样可以彻底清楚本系统的不足之处。其次就是我们用户本身给网络系统造成的伤害，因为用户本身可以对系统的所有设置进行修改，这样就对系统造成了一定的隐患，之所以这么说是因为有很多公司或是企业对网络管理员的要求不是很高，管理员自身也缺乏安全意识，对访问系统的人员权限设置不是很精细，其实这样对系统的损害是很大的，比如说ftp文件服务器，如果设置权限不够具体不够明确，可以随意上传、建立和删除文件，这样就很容易把一些伪装的病毒文件上传到服务器里，另外如果这样的话对其他用户的文件也是一种威胁。如果网络管理员在不经意间泄露了网络口令，这样对系统的安全无疑是一个更

大的危害，大家都知道我们只要是用计算机就会产生痕迹，在一系列的痕迹里面系统日志显得尤为重要，因为他在时刻记录着我们的操作过程，管理员如果不及时清理这些记录也会给系统造成隐患。最后就是我们网络的拓扑结构给我们的网络系统安全造成的隐患，上述我们说的单机的杀毒软件，和修补漏洞的软件这些都是计算机系统自身的防护，其实我们防止不法分子的入侵主要是靠我们拓扑结构中的防火墙，他可以对来自外部所以文件进行必要的过滤也对我们向外走的文件进行检查，所以防火墙技术是解决网络安全的重要手段，可以说他是我们内网和外网的一扇门，这个门可以把对网络有危险的木马文件分离并扼杀在门外，使我们的网络系统更安全。

总之，网络系统安全是一个多方面跨越性的课题，因此我们要加强单人网络管理能力，加强网络建设队伍的素质，加强各方面的联动配合能力，只有这样才能让我们的网络系统更安全，更稳定。

大数据与信息安全论文篇三

在数据挖掘教学过程中，其流程主要是以下几点：首先做好数据准备工作，主要是在挖掘数据之前，就引导学生对目标数据进行准确的定位，在寻找和挖掘数据之前，必须知道所需数据类型，才能避免数据挖掘的盲目性。在数据准备时，应根据系统的提示进行操作，在数据库中输入检索条件和目标，对数据信息资源进行分类和清理，以及编辑和预处理。其次是在数据挖掘过程中，由于目标数据信息已经被预处理，所以就需要在挖掘处理过程中将其高效正确的应用到管理机制之中，因而数据挖掘的过程十分重要，所以必须加强对其的处理。例如在数据挖掘中，引导学生结合数据挖掘目标要求，针对性的选取科学而又合适的计算和分析方法，对数据信息特征与应用价值等进行寻找和归纳。当然，也可以结合程序应用的需要，对数据区域进行固定，并在固定的数据区域内分类的挖掘数据，从而得到更具深度和内涵以及价值的

数据信息资源，并就挖掘到的数据结果进行分析和解释，从结果中将具有使用价值和意义的规律进行提取，并还原成便于理解的数据语言。最后是切实加强管理和计算等专业知识的应用，将数据挖掘技术实施中进行的总结和提取所获得的数据信息与评估结果在现实之中应用，从而对某个思想、决策是否正确和科学进行判断，最终体现出数据挖掘及时的应用价值，在激发学生学习兴趣的同时促进教学成效的提升。

2.2挖掘后的数据信息资源分析

数据信息资源在挖掘后，其自身的职能作用将变得更加丰富，所以在信息技术环节下的数据挖掘技术随着限定条件的变化，而将数据挖掘信息应用于技术管理和决策管理之中，从而更好地彰显数据在经济活动中的物质性质与价值变化趋势，并结合数据变化特点和具体的表现规律，从而将数据信息的基本要素、质量特点、管理要求等展示出来，所以其表现的形式十分丰富。因而在数据挖掘之后的信息在职能范围和表现形式方式均得到了丰富和拓展，而这也在一定程度上体现了网络拟定目标服务具有较强的完整性，且属于特殊的个体物品，同时也是对传统数据挖掘技术的创新和发展，从而更好地满足当前大数据时代对信息进行数据化的处理，并对不同种类业务进行整合和优化，从而促进数据挖掘技术服务的一体化水平。

2.3大数据背景下的数据挖掘技术的应用必须注重信息失真的控制

数据挖掘技术的信息主要是源于大数据和社会，所以在当前数据挖掘技术需求不断加大的今天，为了更好地促进所挖掘数据信息的真实性，促进其个性化职能的发挥，必须在大数据背景下注重信息失真的控制，切实做好数据挖掘技术管理的各项工作。这就需要引导学生考虑如何确保数据挖掘技术在大数据背景下的职能得到有效的发挥，尽可能地促进数据挖掘技术信息资源的升级和转型，以大数据背景为载体，促

进整个业务和技术操作流程的一体化，从而更好地将所有数据资源的消耗和变化以及管理的科学性和有效性，这样我们就能及时的找到资源的消耗源头，从而更好地对数据资源的消耗效益进行评价，最终促进业务流程的优化，并结合大数据背景对数据挖掘技术的职能进行拓展，促进其外部信息与内部信息的合作，对数据挖掘技术信息的职能进行有效的控制，才能更好地促进信息失真的控制[2]。

3数据挖掘技术在不同行业中的应用实践

学习的最终目的是为了更好的.应用，随着时代的发展，数据挖掘技术将在越来越多的行业中得以应用。这就需要高校教师引导学生结合实际需要强化对其的应用。例如在市场营销行业中数据挖掘技术的应用这主要是因为数据挖掘能有效的解析消费者的消费行为和消费习惯，从而利用其将销售方式改进和优化，最终促进产品销量的提升。与此同时，通过对购物消费行为的分析，掌握客户的忠诚度和消费意识等，从而针对性的改变营销策略，同时还能找到更多潜在的客户。再如在制造业中数据挖掘技术的应用，其目的就在于对产品质量进行检验。引导学生深入某企业实际，对所制造产品的数据进行研究，从而找出其存在的规则，并对其生产流程进行分析之后，对其生产的过程进行分析，从而更好地对生产质量的影响因素进行分析，并促进其效率的提升。换言之，主要就是对各种生产数据进行筛选，从而得出有用的数据和知识，再采取决策树算法进行统计决策，并从中选取正确决策，从而更好地对产品在市场中的流行程度，决定生产和转型的方向。再如在教育行业中数据挖掘技术的应用，主要是为了更好地对学习情况、教学评估和心里动向等数据进行分类和筛选，从而为学校的教学改革提供参考和支持。比如为了更好地对教学质量进行评估，就需要对教学质量有关项目进行整合与存储，从而更好地促进其对教学质量的评估，而这一过程中，就需要采取数据挖掘技术对有关教学项目中的数据进行挖掘和处理，促进其应用成效的提升[3]。

4结语

综上所述，在大数据背景下，数据挖掘技术已经在各行各业中得到了广泛的应用，所以为了更好地满足应用的需要，在实际教学工作中，我们必须引导学生切实加强对其特点的分析，并结合实际需要，切实注重数据挖掘技术的应用，才能促进其应用成效的提升，最终达到学以致用的目的。

参考文献：

[2]欧阳柏成.大数据时代的数据挖掘技术探究[j].电脑知识与技术,,15:3-4+9.

[3]孔志文.大数据时代的数据挖掘技术与应用[j].电子技术与软件工程,2015,23:195.

大数据与信息安全论文篇四

网络环境下的计算机安全就是指在网络环境里利用网络管理技术和控制措施，保证在网络环境下的计算机数据的完整性、可使用性和保密性。在网络环境下的计算机需要保证两个方面的安全，一个是物理方面的安全，一个是逻辑方面的安全。物理方面的安全是指系统设备中与数据有关的设施一定要受到物理方面的保护，不能使这些元件遭到丢失或破坏；逻辑方面的安全是指我们要在网络环境下保证计算机数据的完整性、可用性和保密性。

在网络环境下的计算机存在的不安全因素有很多，但这些因素主要有三类，分别是人为因素、自然因素和突发因素。人为因素指不法分子利用非法手段进入机房，或复制拷贝计算机重要的系统资源，或非法篡改数据和编制计算机病毒，或偷取破坏计算机硬件设备。人为因素是对网络环境下计算机安全问题造成威胁的最大因素。自然因素和突发因素多和计算机网络有关，网络不安全因素主要有两种，一是网络计算

机的网络带有薄弱性；二是网络计算机操作系统存在安全隐患。

（一）网络计算机的网络带有薄弱性

在互联网下，计算机要面对的是全球所有联网的机器，也就是说，我们每个人都可以在上网的时候向世界上任何一个地方方便地去传输和获取我们所需要的各种各样的信息。面对这种情形，计算机的安全就遭遇了空前的挑战，这些挑战来自互联网的三个特征，即互联网的开放性、共享性和国际性。

1、计算机互联网的开放性。计算机互联网是一项完全开放的技术，这种技术就使得计算机有可能面临来自各方面的攻击，这些攻击无孔不入，它们有的是从物理传输线路上对计算机进行攻击，有的是通过互联网的协议对计算机进行攻击，有的是通过计算机的软件或硬件的漏洞对计算机进行攻击。

2、计算机网络的共享性。互联网上的东西都具有共享性，网络资源人人可用，人们在使用互联网时没有什么固定的技术要求，用户可以自由上网，也能根据自己的需求随意发布和获得自己需要的各种信息，这些信息在全球范围内都具有共享性，自己的东西别人能使用，自己也能使用别人的东西。

3、计算机网络的国际性。互联网里的每一台计算机都是和全球的网络连在一起的，这就是说，你的联网计算机不仅有可能受到局域网内计算机的攻击、本地区计算机的攻击，也可能遭遇世界上任何一台计算机的攻击，所以你要时刻提防来自各个地区的网络网路入侵者的攻击，这就增加了计算机的风险。

（二）网络计算机的操作系统存在安全隐患

在互联网下，计算机的操作系统为计算机程序或其他的系统提供了一个使他们正常运行的环境，也为计算机提供了各种

各样的文件管理或其他管理功能，并为系统软件和硬件资源提供了一定的支撑环境。倘若计算机本身的操作系统软件出现了问题，那么计算机就开始出现一系列的安全隐患。

1、网络计算机操作系统本身功能存有缺陷。因为计算机系统要为计算机的管理提供多种支撑，这些管理也很繁多，不但有外设管理也有内存管理，不但有硬件管理也有软件管理。这些管理都是通过一定的程序模块来进行的，假如其中的任何一项管理出现了漏洞，当计算机与外在网络连接起来的时候就有可能导致计算机系统瘫痪，所以许多网络高手甚至电脑网路入侵者都是针对网络计算机操作系统存在的漏洞进行攻击的，他们通过一定的程序迫使操作系统尤其是部分服务器系统在瞬间瘫痪。

2、网络计算机的操作系统在网络上为计算机提供部分联网功能或服务时也会带来隐患。这些功能也许是文件的传输，也许是软件程序的安装或加载，也许是可执行文件。网络下的计算机的一个重要功能就是可以进行文件的传输，在文件传输过程中常常会带有许多可执行文件，这些文件都是人为编写的一定的程序，假如这些可执行文件的某些地方有漏洞，也可能造成系统的瘫痪。倘若有人故意在传输的文件或远程调用的软件商故意安装一些具有偷窥性质的间谍软件，那么这些文件在整个传输过程中都会受到别人的监视，因此这些程序或文件都会给计算机的安全带来麻烦，因此我们在对网络计算机进行操作时，要尽量少用或不用来历不明的或对他们的安全性存有怀疑的软件。

3、网络计算机的不安全因素跟操作系统的可创建、支持和守护进程也有一定的关联。操作系统在创建和支持进程时，可以支持被创建的进程继承创建的权利，这就为远程服务器上安装一些谍报软件提供了条件，如果有人把谍报软件以一种合法用户的假象捆绑在一个特权用户上，就能使得谍报或网路入侵者软件在不被人察觉的情况下完成它们的间谍功能。操作系统在守护进程时一些病毒监控软件刚好也是守护进程，

这些进程有的是良性的防病毒程序，有些却是病毒程序，如果碰到一些危险的进程，就有可能使得硬盘被格式化，这样就会出现安全隐患，这些安全隐患会在固定的时间发生作用，平时我们预测不到这种安全隐患的存在，操作系统的守护进程就在不知不觉中被破坏掉了。

4、网络计算机操作系统的远程调用功能可能给计算机带来安全隐患。我们常用的联网计算机操作系统都具有远程调节或协助功能，这种功能使得任何一台计算机都能够通过远程去调用一个巨型服务器里面的某些程序，并且这种功能还可以给远程的服务器提供一定的程序让服务器去执行。在网络计算机进行远程调用功能时需要经过许多环节，在这些环节中的某些交流沟通环节有可能出现被某些人监控的情况，这样就给计算机的安全带来了隐患。

5、网络计算机操作系统的后门和漏洞会给网络计算机带来安全隐患。操作系统的程序设计人员在对操作系统程序进行开发时总会给程序留一个后门，通过这些后门程序，设计人员可以通过绕过一些安全控制去获得对系统或者程序的访问权，但是如果这些后门程序被一些不法分子或者网路入侵者利用，那些没有被删除的后门程序就成了泄露或丢失信息的漏洞，同时操作系统程序中还存在一些没有口令的入口，这也给网络计算机的安全带来危险性。虽然网络计算机的操作系统漏洞可以通过软件升级来克服，但等到发现这些漏洞进行系统升级时，某些漏洞能使系统的安全控制变得没有意义，很小的一ige漏洞就可能使网络计算机的网络瘫痪掉。

（一）网络计算机物理层面的安全对策

我们如果想保证网络计算机的安全，最主要的就是为网络计算机提供一个安全的’物理环境，也就是说，网络计算机的机房要有必要的安全设施。在网络计算机安放的地方，我们要保证有一定的环境条件，这些环境条件是指计算机所在地的气温、空气湿度、防腐蚀度、电气的干扰等方面都要有一定

的防护措施。同时，我们要给网络计算机选择一个合适的安装环境，这些环境需要网络计算机避开一些有强烈振动的振动源和强烈声音的噪声源，同时在机房建筑物上下左右要避免有用水设备。对于机房人员的出入，也要有必要的管理措施，对于哪些机器哪些人可以用、哪些人不能用要有一定的限制，未经允许的人禁止进入机房重地。对于重要的网络计算机，我们要安装必要的防盗和安全防护措施，避免网络计算机遭受物理侵犯或非法个人或团体的侵犯。

（二）网络计算机管理层面的安全对策

在对网络计算机进行安全对策考虑时，我们需要有一定的法律法规和执行的力度。我们要对网络计算机管理或使用人员进行一些列的法制教育，包括计算机犯罪法、网络计算机安全法、保密法和数据保护法等，让他们明确自己的使用权利和义务。同时，我们还要对网络计算机管理人员进行一定的安全教育和必要的道德观和法制观的教育，让网络计算机管理人员既受到了道德观的熏陶，也受到法律法规的限制的束缚，这样我们才能不断地对网络计算机的安全管理进行完善和强化。网络计算机管理人员也要有安全意识，注意不但要防护来自网络的病毒，也要防止来自远处的网路入侵者攻击。要建立一套相应的安全管理制度。这些制度要求网络计算机管理人员必须自觉遵守，这些管理制度可以包括对人员的管理制度、对网络计算机的运行和维护制度、对网络计算机的资料管理制度、对网络计算机机房的保卫制度和对网络计算机环境的卫生打扫制度。

（三）网络计算机技术层面的安全对策

在技术层面，我们对网络计算机实时进行病毒扫描、实时对网络计算机进行监控。我们既要对网络计算机设置防火墙，也要不断地对病毒报告进行分析和对系统进行安全管理。我们在对网络计算机安全进行防范时，要注意在技术上对网络的访问进行控制，对网络权限也要进行控制，对于属性目录

级别我们也要进行控制。同时，我们也要学会对数据库进行备份和恢复，在系统发生意外时，我们要会运用数据备份和数据恢复进行及时的操作。同时，我们也要掌握一些其他技术，这些技术包括运用密码技术即网络计算机信息安全的核心技术、完善更安全的操作系统技术即不给病毒的生长提供温床的技术、切断传播途径确保计算机不受外来硬件感染病毒、提高网络反病毒技术即限制只能服务器才允许执行文件的技术等。在日常生活中确保网络计算机的安全是一个庞大的工程，它涉及到的方面比较多，不但要涉及到网络计算机的网络和操作系统、网络计算机的存放环境、网络计算机管理人员的素质和技术，还要涉及到网络计算机安全管理制度和措施等。我们在对网络计算机安全问题进行分析和寻找对策时需要具体问题具体分析，我们要把这些防范措施通过一定的手段使它们综合起来。对于网络计算机的安全防范，我们要做到以人为主，同时结合环境和法律制度进行统一的整合和教育。在对网络计算机犯罪和网络计算机病毒防范方面，我们还要同国际接轨，通过和国际相应的组织合作来共同完成确保网络计算机安全的使命。

大数据与信息安全论文篇五

现代计算机网络的基本特征是多样性、互联性与开发性，这也导致计算机网络极易受到外来入侵者的恶意攻击和非法入侵，严重威胁到计算机网络安全。数据加密技术主要是利用先进的数据加密算法，具有较高的私密性，应用于计算机网络，能够在很大程度上提高计算机网络系统的安全性。随着现代化科学技术的快速发展，必须深入研究数据加密技术，并且不断完善与优化，充分发挥数据加密技术在计算机网络应用的重要优势。

2.1非法入侵

计算机网络非法入侵主要是网络骇客利用监视、监控等方法，非法获取计算机网络系统的ip包、口令和用户名，利用这些

资料登录到计算机网络系统中，冒充计算机用户或者被信任的主机，使用被信任用户的ip地址窃取、篡改或者删除计算机网络数据。

2.2服务器信息泄露

由于计算机程序是由专业的程序设计人员编写的，无法保证不存在漏洞与缺陷，而网络骇客往往具有专业的计算机知识和较高的计算机网络运维技能，他们往往利用这些漏洞和缺陷恶意攻击计算机网络，利用不法手段来取得这些网络信息，对计算机网络安全性与可靠性造成威胁。2.3计算机病毒计算机病毒的分布范围非常广，传播速度快，破坏性高、隐蔽性高、可依附于与其他程序。能够快速的通过网络感染其他计算机设备，甚至造成整个计算机网络系统瘫痪。通常情况下，计算机病毒主要附着在计算机程序上，一旦病毒文件被激活或者共享，在浏览或者打开其他机器时，会加速扩散和感染，形成连锁式传播，容易造成计算机网络系统损坏或者死机，丢失重要数据。2.4网络漏洞当前计算机操作系统能够支持多用户、多进程，计算机网路系统主机上可能同时运行多个不同进程，接收数据包时，同时运行的各个进程将都可能传输数据，使得计算机操作系统漏洞很容易被恶意攻击，对计算机网络安全性与可靠性造成威胁。

威胁到计算机网络安全的重要因素涉及到：网络设备的安全性与网络信息安全性，而数据加密技术则起到很好的保护作用，其主要是依据密码学，采用密码学科学技术对于网络中的数据信息采取加密的方式，并且借助于加密密钥、函数的替换或者移位，将计算机网络数据信息转换为加密信息，信息接收人员再利用解密密钥或者解密函数将加密信息进行还原，如此一来就能够在很大程度上提高数据信息传输的隐蔽性和可靠性。利用多种加密算法，数据加密技术又能分成非对称与对称加密技术，非对称性加密技术是设置不同的密钥，数据信息发送者使用加密算法，接收者使用另一套私密的解密密钥，使用不同密钥对数据信息进行加密和解密，非对称

性加密技术采用公开密钥和私有密钥，基于隐密的密钥交换协议，计算机网络用户在接收和传输数据信息时，不需要交换信息密钥，极大地提高了数据信息和密钥传递的保密性和安全性。对称性加密技术是指在计算机网络系统中，数据信息接收人员和发送人员使用同样的一组密钥进行加密和解密，对称性加密技术在计算机网络系统中的应用，由数据信息接收人员和发送人员提前商定信息密钥并且妥善保管，从而确保计算机网络数据传输的安全性、完整性和机密性。

4.1链路数据加密技术的应用

在实际应用中，多区段计算机网路系统主要采用链路数据加密技术，这种加密技术可有效划分网络相关数据和信息的传输路线，对不同传输区域和传输路径的数据信息进行加密，在计算机网络系统不同路段传输的数据信息采用不同的加密方法，这样数据信息接收人员接收到的都是密文形式的信息数据，即使网络骇客获取到这些数据信息，也无法破解数据信息的内容，具有良好的保护作用。同时，在计算机网络系统中应用链路数据加密技术，可及时填充传输的数据信息，再改变不同区段和路径传输的数据信息长度，使其产生较大差异，扰乱网络骇客对于关键数据信息的判断能力。

4.2端端数据加密技术的应用

端端数据加密技术与链路数据加密技术不同的是加密过程简单，便于操作。该加密技术基于专业的密文来传输信息数据，其在计算机网络系统中的应用，在传输数据信息过程中不需要加密或者解密数据信息，可有效保障计算机网络系统信息安全。端端数据加密技术的应用，运行投入和维护投入费用较少，并且这种加密技术进行数据传输时采用独立的传输路线，即使某个传输路线数据包发生错误，也不会影响系统中其他数据包，可极大地提高计算机网络系统数据传输的完整性和有效性。同时，在计算机网络系统中应用端端数据加密技术，信息接受者的ip位置可及时撤销，其他网络用户无法

解密数据信息，这在很大程度上降低了网络骇客篡改或者窃取数据信息的几率，也就保证了计算机网络的可靠性与安全性。

4.3数据签名信息认证技术的应用

近年来，数据签名信息认证技术的应用范围越来越广，其作为一种重要的保护技术，主要通过鉴别和确认用户身份信息，防止其他非法用户获取用户信息，从而保障计算机网络系统安全。数据签名信息认证技术的应用包括口令认证和数字认证两种方式，口令认证比较简便、快捷，使用费用较低，因此应用非常广泛；数据认证主要基于加密信息，从而有效核实密钥计算方法，有效提高计算机网络系统数据信息的安全性和有效性。

4.4节点数据加密技术的应用

节点数据加密技术主要是利用加密数据传输线路来保护计算机网络数据信息，在数据信息传输之前，通过节点数据加密技术对数据信息进行加密，这样就使得数据信息以密文形式进行传输，并且数据信息加密后在计算机网络系统中传输时难以被网络骇客识别，可有效提高数据信息的安全性。然而，节点数据加密技术在计算机网络系统中的应用也存在一些问题，这种加密技术需要数据信息接收者和发送者采用明文形式来加密数据信息，一旦数据信息受到外界环境影响，会直接影响数据信息的安全性。

4.5密码密钥数据技术的应用

密码密钥数据技术主要是采用公用密钥和私用密钥，公用密钥具有较高的安全性，在数据信息传输之前进行加密，可防止数据信息泄露，使用私用密钥时，数据信息接受者和发送者需提前商议密钥，采用相同的密钥对数据信息进行解密和加密，并且在计算机网络系统中应用密码密钥数据技术，使

私用密钥和公用密钥互补，有效提高计算机网络系统的安全性。

5.1网络系统管理和安全管理方面

随着科技的不断发展，网络化技术的发展也极为迅速，而且，网络所遍布的范围也越来越广，而要确保计算机网络发展有着更好的延续性，就必须向着网络系统管理以及安全管理方向发展，全面提升计算机网络安全管理意识，进而有效的避免或降低被骇客的攻击以及病毒的破坏。网络越先进，安全越重要。在日常工作中，我们始终把系统安全稳定运行作为信息科技的要务，并结合实际情况，采取措施保证安全生产。一是强化员工安全意识。二是加大信息系统安全检查力度。三是细化应急预案。四是创新安全防范技术。我们还应探讨和发现隐性问题，把问题消灭在源头。

5.2标准化网络方面

由于互联网没有设定区域，这使得各国如果不在网络上截断internet与本国的联系就控制不了人们的见闻。这将使针对网络通讯量或交易量纳税的工作产生不可见的效果。国家数据政策发布的不确定性将反映在混乱的条款中。标准化网络一是提升了个人信息安全的识别，提示了风险的隐蔽、可见性，提高整改防控意识。二是使安全生产有了明确的量化标的。三是建立了激励与约束。四是采取现场检查方式进行监管检查，风险提示明确，问题处理表述清楚。五是规范工作流程。六是采取各点详查、随机抽查、现场提问使网点安全生产落实到实处。七是监管评价与重点工作考核结合。

当前，计算机网络系统存在很多安全隐患，数据加密技术在计算机网络安全中的应用，结合计算机网络系统的不同需求，选择合适的数据加密方法，提高计算机网络系统的安全性和稳定性。