2023年网络安全技术专题论文 计算机网络安全中的数据加密技术论文(优秀5篇)

人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。范文怎么写才能发挥它最大的作用呢？以下是我为大家搜集的优质范文，仅供参考，一起来看看吧

网络安全技术专题论文篇一

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。

网络安全技术专题论文篇二

（1）对称加密技术。对称加密，又称共享密钥加密，即信息发送、接收方通过某种密钥分别对数据进行加密、解密。它要求通信双方在密文安全传输前，应先确定某个公用密钥。所以，只有双方都不透露密钥，方可保证数据传输的可靠性、完整性。对称加密技术，属于最常见的数据加密技术。数据加密算法大体包含des□aes与idea三种□des数据加密标准算法，主要是针对二元数据进行加密，是一种分组密码（对称64位数据），密钥可随意设置为56位，剩下8位为奇偶校验□des加密效率较高、速度较快，它的加密范围很广，在各个领域内

均有普适应用。而aes算法则是在des算法的基础上加强密钥，达到128位，使数据更安全。（2）非对称加密技术。非对称加密，又称公钥加密。简而言之，非对称加密，即信息发送与接收方分别选择不同的密钥，来对数据进行加密、解密，密钥通常包含公开密钥（加密）与私有密钥（解密）两类，现有技术与设备还无法从公钥推向私钥。非对称加密技术的前提在于密钥交换协议，通信双方在不交换秘钥的情况下，便可直接传输通信数据，不存在密钥安全隐患，数据传输的保密性显著提升。非对称加密技术，通常包含rsa□eigamal以及diffie□hellman等数据加密算法。公钥算法中应用最广的算法是rsa算法，可有效防御现有密码的攻击。非对称加密技术可应用于数据加密，同时也可认证身份、验证数据的完整性，在数字证书、签名等领域得到广泛应用。

2数据加密的表现形式

（1）链路加密。链路加密，又称在线加密，是指在网络节点中对通信链路予以加密，以确保网络的安全传输。链路加密在传输数据前，就对信息进行加密，而后在网络节点间二次解密，在多次解密、加密中，运用多种密钥来维护数据安全。通常而言，接收人在获取一个数据前，经历了多条通信链路。该过程还包含路由信息中的数据，均通过密文形式传递，链路加密有效覆盖了数据传输、接收两点。（2）链路加密技术。链路加密技术，将数据划分为多条传输线路，而后再对各个区域进行加密；当接收方收到数据时，数据已历经了数次加密，并以密文形式达到；它与节点加密技术有所不同，当数据以密文形式出现时，信息较为模糊，这就能很好地保证数据的安全性。链路加密技术的优点在于：不同区域均使用相应的加密技术，各区域的表现特征也存在一定差异，其他人通常无法获取明文数据。（3）端端加密技术。端端加密技术，即信息由端—端所提供的加密技术。换而言之，数据被发送方加密，而后被接收方解密，并始终以密文形式进行传输。与链路加密技术和节点加密技术相比，端端加密技术的加密、

解密设备均在发送方、接收方，避免了传输阶段的加密、解密次数，这从某种程度上提升了数据的’安全性。然而，端端加密技术也有其自身的缺点，其加密对象仅为内容，开头无法加密，这就容易被非法入侵者窃取数据。

3数据加密技术在计算机网络安全中的应用

（1）网络数据库加密。网络数据库管理系统主要为windowsnt□unix□操作系统级别多为c1级、c2级。可知，计算机存储系统与数据传输公共信道的安全性偏低，容易被pc机等设备通过某种方式对有价值的数据、密码等进行窃取甚至篡改。基于此，对系统内外部安全管理而言，数据加密极为关键，网络数据库用户应根据访问权限或者是设定口令字等，来加密保护核心数据。（2）软件加密。在数据加密过程中，假如杀毒软件或是反病毒软件及程序染上了计算机病毒，则不能查验该程序、数据等是否存在数字签名。因此，如要执行加密程序，则必须查验需加密、解密文件及其本身有没有被病毒感染。不过，该种检查机制对保密性要求较高，使得部分杀毒软件、反病毒软件都需运用数据加密技术，以保证软件程序的安全性。（3）无线网络的数据加密。无线网络由于其方便快捷，可以适用于较偏远的、铺设通讯线路比较困难的地区而越来越受人欢迎，但是空间上的开放性使得它暴露出来的安全问题也越来越明显。因此无线网络往往会使用一些加密算法来保证自己的数据进行安全传输。现行网络中经常使用wep算法□wpa算法，并采用统一的安全验证标准ieee802□11i□改进了加密机制中的缺陷。（4）虚拟专用网络□vpn□□现阶段，很多企事业单位均建立起了自身的局域网。因各分支机构设立在不同的地方，需通过租用专用路线来实现各局域网的联合，以便组建广域网。在vpn中，数据加密技术价值在于：数据从发送者vpn处自动通过路由器来对硬件加密，而后以密文形式将数据传输至互联网，当密文达到指定vpn时，它的路由器也会自动为其解密□vpn接受者随即可阅读明文。

4结语

数据加密技术是通过置换表算法、循环移位以及xor操作算法等多种加密算法来加密数据信息，以保证其传输完整性、科学性。只有立足于实践，充分应用数据加密技术，才能维护计算机网络安全，真正为使用者服务。

参考文献:

［3］宋利敏．刍议计算机信息数据的加密技术□j□□科技风，2014（14）．

网络安全技术专题论文篇三

sts教育及其在当前高中生物教学中的渗透

高中生物新课程中的sts教育初探

分子生物学的科学创新特征研究

webquest在高中生物选修课中应用的实践研究

论中关村生命科学园区的发展战略

高中生物课堂中生命伦理教育的探索与实践

我国中学生物课程改革的研究

部属师范类高校生物专业课程设置的现状研究

中、美初中生物(科学)课程改革比较初探

高压对黑腹果蝇生长发育、表型变异和分子水平上影响的研

究

生物科学与社会教学实践研究

网络安全技术专题论文篇四

：随着全球的信息化不断发展，信息网络的建立和不断发展，计算机网络技术已经广泛应用于各个领域，为人们的现代生产和生活提供了很多便利。同时，一系列网络安全问题成为关注的焦点，利用计算机网络进行信息交换的重点。计算机网络安全内涵研究，然后讨论当前计算机网络安全问题，并对计算机网络技术在网络安全维护中的具体应用进行深入研究。

：计算机网络；网络安全维护；应用

计算机网络安全主要是为了保护信息传输的机密性，防止攻击造成的信息泄露，有必要建立一个安全有效的计算机网络病毒防护软件，而且在使用网络时对收到的信息和发出严格的检查和控制。基于网络安全的计算机操作，维护数据安全，确保网络不受计算机病毒入侵和损坏。在现代社会，信息化是一项重要资源，同时享受信息通信的便利性，安全问题逐渐引起了人们的关注。近年来，一些网络安全相关技术，如病毒防火墙技术，秘密安全管理技术和智能门禁技术，智能卡技术，数字签名技术，智能认证技术等技术手段。加强计算机网络安全管理，完善安全管理技术，确保日常工作正常运行，保障信息安全，具有重要意义。

1.1操作系统自身问题

为了方便开发商继续更新升级，操作系统均具有很强的可扩展性，无论是windows操作系统，还是linux或vista操作系统，这种扩展性给不法分子攻击提供了便利，为计算机网络环境

带来了安全隐患，。计算机系统的漏洞是任何系统和程序的设计都不能做到完美兼容。网络操作基础是计算机网络安全运行的前提条件，目前很多技术漏洞存在于网络操作系统中，不法分子就会针对这些漏洞进行攻击，一旦系统维护、补丁修复不及时，是可能使网络发生攻击，对整个计算机网络带来的非常严重的安全隐患。所以用户需要做一个例行的bug修复，减少系统漏洞造成的损失。

1.2计算机病毒

计算机病毒和不法分子攻击是造成计算机网络安全问题的重要因素。不法分子在没有获得授权和许可的条件下，利用特殊的技术对他人计算机和服务器等进行未授权操作。不法分子利用多种手段进行攻击和信息窃取，对他人计算机进行控制，窃取用户的相关资料，对计算机用户的信息安全和财产安全带来很大隐患。计算机病毒是人为编写的，在网络中进行传播，对用户的数据安全和硬件安全都会造成很大的危害。计算机病毒传播较快，自身比较隐蔽，严重影响了用户的正常使用，给用户带来了很大损失。

1.3不法分子攻击

计算机病毒和不法分子攻击是造成计算机网络安全问题的重要因素。不法分子在没有获得授权和许可的条件下，利用特殊的技术对他人计算机和服务器等进行未授权操作。不法分子利用多种手段进行攻击和信息窃取，对他人计算机进行控制，窃取用户的相关资料，对计算机用户的信息安全和财产安全带来很大隐患。计算机病毒是人为编写的，在网络中进行传播，对用户的数据安全和硬件安全都会造成很大的危害。计算机病毒传播较快，自身比较隐蔽，严重影响了用户的正常使用，给用户带来了很大损失。

1.4数据库隐患造成的安全问题

数据库作为数据管理的核心，掌管着大量的信息和数据。数据库可以方便有效的对数据进行存储和管理，但是在安全性还存在一些问题。数据库防火墙是数据库对于信息数据保护的主要方式，数据库防火墙对于外网的攻击和非法登录有很好的限制效果。但是随着技术的不断进步，数据库的防火墙发展较为迟缓，不能对数据库进行百分百的保护。数据库虽然能避免外网的部分攻击，但是对于内网的行为限制严重不足。在用户登录授权上，管理工作不规范，人员权限下发不明确，造成数据库管理工作混乱，影响数据安全性。另外，系统和软件的漏洞也是数据库产生安全问题的重要因素。

2.1数据加密以及网络访问控制技术在网络安全维护中的应用

计算机网络在运转过程中传输的数据通常是以动态的形式存在，利用密钥对其控制是加密技术的核心，加密算法及密钥管理是加密技术的关键，密钥是数据接收者解密密文的主要攻击，加密算法则对数据进行对称加密算法或非对称加密算法，从而进行数据处理的转换，避免未经授权的用户修改数据信息。

2.2防火墙技术在网络安全维护中的应用

使用防火墙技术，计算机服务器的安全被简单有效的提升了，对服务器进行数据扫描能够从源头开始，在极短时间内中断服务器与代理服务器之间的数据传输，阻止病毒等的传播。防火墙技术主要有：（1）状态监测，监控计算机网络中的数据来识别数据信息的不安全性，这种防火墙技术的优点是显而易见的，但由于保护的延迟，缺乏一定的及时性，使用计算机网络作为一个整体，数据流的主要分析，可能导致保护延迟；（2）包过滤防火墙，主要是对由路由器上传至主机的数据进行扫描和过滤，进而拦截位置数据，在保护协议的基础上，在安全保护的基础上，反映出保护的价值；（3）应用型防火墙，应用型代理防火墙安全性较高，可以针对性的侦测和扫描应用层，在侵入和病毒作用于应用层效果显著。防

火墙技术等计算机网络安全技术，在安全防护上占有主要地位，具有明显的优势，提高了计算机网络的保护水平。

2.3防病毒技术在网路安全维护中的应用

计算机病毒和不法分子攻击是导致计算机网络安全问题的重要因素。不法分子没有授权使用其他计算机和服务器上的特殊技术，例如未经授权的操作。防病毒技术包括安装常规防病毒软件，更新杀毒软件数据库，网络下载或接收邮件等文件扫描和病毒防病毒，特别是对于未知文件，需要确认病毒然后打开；一些木马等病毒经常通过盗版软件和恶意使用操作系统对计算机进行病毒攻击，需要更新个人电脑操作系统，安装系统更新补丁，以确保最新最安全的状态系统；为了使用操作系统进行计算机攻击，计算机安装软件进行更新和升级，以减少系统漏洞。

2.4网络安全管理

提高计算机网络安全管理工作的安全性也具有一定意义，提高安全管理要求，对于计算机网络的访问进行合理有效的控制，建立健全安全管理是确保计算机网络安全的重要手段基础。加强网络安全管理的有效途径是在新网络建设初期评估和设计新网络的安全性能。加强系统评估的安全性，建立信息安全体系，确保系统的安全性和稳定性。计算机用户需要加强安全意识，尽可能提高用户的法律意识，计算机网络安全和安全需求的增长，同时需要一个良好的计算机网络安全和安全环境。

互联网技术的发展扩展了计算机网络技术的发展前景的同时，。互联网的信息开放性、共享性、匿名性使得信息的安全存在很大隐患，也带来了一些安全问题基于网络安全维护的背景，本文阐述了计算机网络安全的内涵，结合了不法分子攻击，病毒传播等常见网络安全问题。从防火墙技术，加密技术和防病毒技术等方面对计算机网络安全防护技术进行系统

分析。可以看出，加强计算机网络安全的管理，提高安全管理的技术对于保证日常工作的正常进行，保证信息财产的安全有着重要的意义。

[1]陈建平。基于工作过程的《计算机网络安全》一体化课程开发及实施研究[d]□华中师范大学，2014.

[2]王蔚苹。网络安全技术在某企业网中应用研究[d]□成都:电子科技大学，2011.

[5]姜可。浅谈防火墙技术在计算机网络信息安全中的应用及研究[j]□计算机光盘软件与应用，2013,(4):33.

网络安全技术专题论文篇五

1.1大力开展学生网络道德教育

高校是高科技人才集聚地，许多计算机方面的高材生都存在于高校。学生在计算机方面的才能是把双刃剑，既能保护社会、服务社会，也能危害社会，只有加强思想道德上的教育，重视他们在网络道德上的培养，才能使他们真正为社会所用，造福社会。然而，当前高校存在的网络入侵事件有大半是来自于校园的内部，这与高校忽视网络安全教育不无关系。网络教育的滞后与脱节是造成这一现象的罪魁祸首。因此，各大高校应加强对学生的网络安全教育，通过开展网络安全知识讲座，广播、校报及课堂讲课的方式来提高学生在网络安全上的道德意识，规范学生的上网行为，提高他们的道德修养，使他们的计算机才能用到正道上，真正为社会服务。

1.2重视校园网络用户的安全教育

高校计算机网络安全不单单是高校对此不重视的问题，还因为网络用户本身的安全知识匮乏。高校应加强对校园网络用户的安全教育，引导学生树立网络安全意识，在计算机使用

过程中，要重视安装防杀毒的软件，病毒防不胜防。病毒无孔不入，因此，校园网络用户在使用计算机时，不论是打开网页还是打开邮件，都需要多一个心眼，不要点陌生且来路不明的邮件，也不可随意打开不明的链接。另外，在计算机使用过程中，软件使用的密码切忌过于简单，应重视账号和密码的保存，不可随意将密码告诉他人。网络用户在使用计算机过程中最重要的是小心，重视对自己账号的保护，时时刻刻谨慎，才不会让病毒有机可乘。

1.3加强对网络安全管理人员安全意识和技能的培训

随着校园网络的广泛应用，高校对校园网络也愈加依赖，很多重要资料和信息都录入到计算机中，这也使得对校园网络的攻击和资源盗用现象越来越严重，加强网络信息安全，提高安全管理人员的安全意识和安全技能也变得愈发重要。面对当前高校安全管理人才缺乏的问题，高校应重视引进优秀的网络安全管理人员，对管理人员的安全意识和安全技能进行进一步的培养，通过开展讲座来促进管理人员的安全意识和保密意识，通过开展集体学习来提高网管人员的专业素质，通过实际操作来提高管理人员的安全技能，并规范保密条例来降低信息和资源的安全隐患。

1.4加强校园网络安全防卫系统建设，完善规章制度

对于高校网络安全问题，可通过加强网络安全防卫系统建设来降低风险。第一，可以通过进一步完善校园网络的防火墙来阻隔外界对内部信息和资料的非法获取。第二，高校网络可以通过采取数据加密技术，如数据传输、数据存储、数据完整性的鉴别及秘钥管理。这些加密技术的严格应用大幅降低外界病毒的入侵，也便于网管人员对信息和资料的管理，及时发现问题所在。第三，采用相关软件，实时监控网络动态，密切关注在信息的传输等过程中的状况，对可能出现的不正常状况及时采取措施。另外，高校有必要建立网络安全管理的各项规章制度，以此来规范高校的网络使用，保护用

户信息安全。

计算机网络安全对校园网络建设有重要意义。一方面，计算机网络安全有利于保护校园信息和资料的安全，另一个意义上保护了师生的信息，也保护了科研成果的安全，对校园网络建设和发展产生了不可忽视的作用。另一方面，计算机网络安全意味着高校学生在安全意识上的提高和安全素质上的成长，更多的计算机人才将会投入到建设社会安全网络的事业中，这是高校网络安全意识培养的成功，是高等院校人才培养上的成功。