

计算机网络信息安全中数据加密技术应用研究

刘铭晓凡

山东省禹城市城区骇河街164号 山东禹城 251200

摘要: 最近几年,在我国计算机网络信息技术快速发展的背景下,网络系统已经形成了互通共联机制。但是,这种情况也会导致网络成为信息泄露的灾区。这就需要实现对计算机信息的整合,可以通过对数据加密技术的有效应用,及时发现其中的安全隐患,从而为计算机的稳定运行提供条件。

关键词: 计算机;网络信息安全;数据加密技术

目前,要想在信息化时代下,实现信息之间的安全传输,需要加强对数据加密技术的有效应用。在计算机信息系统上,实现对数据信息的整合,缩短时空上的距离,保证网络运行的安全性,及时消除网络信息传输中的安全问题,进而实现对重点数据信息的加密。

一、数据加密技术的特点

现阶段,为了保证计算机数据加密技术在网络信息传输中的有效性,对其原理进行了分析。其主要是通过对相关数据信息的整合和密钥后,实现函数之间的转换后,在此基础上让所发送的信息数据能够变成具有意义的密文。等到收到密钥后,可以采用科学方式对译文进行综合性解释,让其还原成为了原数据^[1]。

在对数据加密技术进行应用时,需要保证其本身具有特定的要求,加强其在特定环境中的有效应用,实现对原文内容的快速转换。其中密钥是数据加密技术中的主要组成部分,技术人员可以通过密钥,让密钥和源文件之间可以进行更加灵活地转换,进而为网络的安全运行提供保障。

二、计算机网络安全受到的影响因素

1. 信息操作系统中的隐患

计算机电脑在具体的运行中,其核心软件是操作系统。但是,计算机操作系统在运行中还存在的问题,如果其中的操作系统一旦受到病毒的影响,就会导致整体计算机运行出现问题。病毒可以直接获得用户的口令,非常容易对整体系统进行操作,在此基础上获得所有程序中的用户信息。一般情况下,病毒还会通过间谍程序,对用户的信息传输以及使用进行监视,进而导致整体服务器出现瘫痪情况。此外,病毒的入侵者还能够利用信息系统中的薄弱环节,如远程调用功能等漏洞,实现对计算机系统的侵害,严重影响了信息传输的安全性^[2]。

2. 数据库管理系统中的安全隐患

通常情况下,部分数据库管理系统在运行中会出现问题,如果不对其进行及时处理,就会对银行卡的密码,

或者是个人身份证等基本信息带来影响。这些安全问题都会通过数据库,如果其安全性不高,就会导致其泄漏给外界。这个时候病毒入侵者就会通过信息库,对用户信息进行利用,进而达到破坏计算机的目的。

3. 网络中的安全问题

虽然网络的出现和发展,能够让人类的生活更加丰富和便利。但是其在运行中还会出现信息安全问题,存在比较大的安全隐患。其主要来自传输线的破坏,或者是网络协议受到影响等,都会对计算机软件和硬件带来非常大的影响。再加上,这些不安全因素,还会对用户的信息安全带来影响。因此,需要在计算机系统的特点出发,通过对数据加密技术的有效应用,避免其对防火墙带来影响^[3]。

三、数据加密技术在计算机网络信息安全中的应用

1. 密码学

如果在密码学上对数据加密技术的应用和特点进行分析,其加密设备在公元前5世纪就已经被发明了出来。当时,羊皮是信息的载体,如果没有木棍等外界物的指导,我们就不能及时对文字进行有效阅读,这就需要羊皮缠绕在对应的木棍上,实现对文字的破译。

因此,需要加强对密码学的深入研究,明确编码和解码的特点,在数学、几何和信息技术等基础上出发,实现对数据加密技术的完善和创新。在21世纪,为了实现对社会数据信息的整合,需要对AES这种新数据加密标准进行整合。在密码学上,加强对数据加密技术的有效应用,在角度出发,实现对信息数据的保密,从而为网络系统的安全运行提供条件。

2. 经典加密算法

首先是DES。这种经典的对称方式还被叫做加密算法,部分国家已经将其作为了数据加密标准,属于一种对称性的加密解密算法。同时,DES算法还可以在加密模式下,结合预设密钥对信息数据进行加密。在解密模式下,技术人员可以使用密钥对其进行解密,不知道密钥人

非常难以对其中的信息进行破译,并不能够在短时间内,对大量的信息数据进行整合和加密处理。然而,DES加密与解密会使用相同的密钥,所以知道加密密钥后,就可以完成解密了,所以这种方式的安全性并不高^[4]。

其次是MD5。MD5消息这种算法还被叫做128位加密算法,一般会在信息检测中应用,属于一种不可逆性加密技术。所以此技术在用户登录密码中等工作中得到了有效应用。这种算法可以将任意的长度和字符串进行转变,这种转换并不可逆。但是,相关学者在对此数据加密技术进行分析时,发现由于其中的字符之间转换没有逻辑,所以其并不能将相关的数据信息破译为原来的信息。

部分学者在对MD5算法进行分析时,发现其对明文长度不要求,但是输出密文有固定的128位,其在网络数据加密的应用存在一定局限性,整体的实用性并不高。最后是RSA加密算法。这种方式在后期已经发展成为了完善的RSA体制。此算法是通过两个大素数的乘积,对素数的难题进行解决,主要以两个大素数的乘积等作为公钥,加强对运算式结果的分析,将其作为私钥,在此基础上实现对相关信息的加密。

然而,私钥只有合法人员才可以掌握,在理论上说私钥是能够通过公钥素数的乘积等,对数据信息进行分析的。但是,这种运算量非常巨大,是一种安全性非常高的加密方式。

3. 强化防火墙的防御效果

计算机网络系统在运行中,要想实现对信息的安全性保护,要积极发挥防火墙在其中的作用。主要是实现对网络安全的维护,加强对计算机网络安全保护。通常情况下,电脑在运行中都具有防火墙,其具有危险检测的效果。如果用户访问了一些网页,或者是下载了其他资料,其就会对网页和资料的安全性进行检查。当其在发现网络安全隐患问题后,就会及时提醒用户^[5]。

因此,相关的技术人员需要加强对数据加密技术的有效应用,对防火墙进行建立,科学应用计算机技术,保证计算机网络系统运行的安全性。同时,还可以在此防火墙的基础上,帮助用户实现对网络风险的综合性防御。在应用防火墙的过程中,还能够在此基础上使用服务器,构建安全平台,对电脑中的各种数据进行整合,实现对相关信息的综合性检测和扫描,及时处理电脑在运行中所存在的安全问题,为网络信息系统的安全运行提供条件。

4. 强化计算机软件的功能

当前,随着计算机技术在社会发展各个领域中的有效应用,相关的技术人员对网络系统中的软件功能进行了强化。同时,还需要采取措施做好计算机软件的加密

和保护工作,保证数据加密技术在具体信息保护工作中的有效应用。如果用户在应用计算机网络时,并没有在其中输入正确的密钥,或者是已经出现了多次错误输入等情况,就会导致软件不能更加正常和稳定的运行。

这就需要积极发挥计算机系统的保护效果,及时发现恶意病毒,然后科学应用数据加密技术,对计算机网络进行完善,减少其受到其他因素的攻击。此外,还要实现对防御性软件的安装,及时提醒用户定期清除病毒,实现对病毒的综合性防御。如果在计算机系统的运用中,发现了病毒痕迹,要及时处理,进而不断强化计算机网络运行的安全性。

5. 加强数据加密技术在局域网中的应用

研究发现,如果应用信息技术,设立局域网,不仅能够实现信息之间的传输,还可以实现对数据信息的整合。特别是在使用局域网中,要想进一步保证信息传输的稳定性和安全性,要对信息数据等进行严格地加密处理,让数据可以在传输时,自动存储到路由器中。如果其传输到其他的路由器时,就可以实现自动解密^[6]。

此外,加强数据加密技术在局域网络中的有效应用,还能够保证信息接收者可以直接获取自己所需要的信息。同时,还要加强对各种数据加密方式的科学应用,主要是为了防止信息泄露,保证信息数据的安全性,促进信息之间的有效传输,为网络信息系统的安全运行提供保障。

四、结束语

总而言之,以前的计算机信息加密技术已经不能满足社会发展的要求了。要想保障当前网络信息传输的安全性,需要在不同的角度出发,加强对数据加密技术的有效应用。同时,还可以通过对数据加密算法的分析,促进数据信息之间的传输,加强对用户信息的保护,进而避免计算机网络在运行中出现信息泄露问题。

参考文献:

- [1]周悦.计算机网络信息安全中数据加密技术应用研究[J].电脑知识与技术:学术版,2019,15(18):11-12.
- [2]徐大海.数据加密技术在计算机网络信息安全中的应用[J].中国新通信,2020,22(10):2-2.
- [3]许济宁.数据加密技术在计算机网络信息安全中的应用研究[J].数字通信世界,2020,No.185(5):224-224.
- [4]林海钊,陈伟.数据加密技术在计算机网络信息安全中应用研究[J].数字化用户,2019,(37):85-85.
- [5]赵云普.计算机网络信息安全中数据加密技术的研究[J].通信电源技术,2020,v.37;No.198(6):119-120.
- [6]徐立志.计算机网络信息安全中数据加密技术的研究[J].中国新通信,2020,v.22(7):131-131.