

数据加密技术在计算机网络云安全中的应用探究

陈二浩 耿秀义

(河南师范大学计算机与信息工程学院 河南 新乡 453007)

[摘要]随着如今互联网的全面普及和参与的人群基数越来越大,计算机网络的运行风险也在持续增加,网络信息数据将时刻处在危险之中,因此,计算机网络安全问题才成了目前人们所重点关注的一项任务,很多拥有强大保密维护作用的数据加密技术实现了充足的发展。很多的国家已经在数据加密技术方面投入了大量的资金与人力,使得目前的数据加密技术有了灵活性较高、实用性较好等特点。

[关键词]数据加密技术; 计算机网络云安全; 应用探究

[DOI] 10.12252/j.issn.2096-6261.2020.06.847

1 引言

在如今高速发展的信息时代作高效、生活便捷的同时,通常也伴随着很多不安全因素,面对着越来越先进的网络技术,人们的隐私安全也受到了严重的威胁。计算机系统漏洞、流氓软件的入侵、病毒的侵入、黑客的攻击等不利因素都对人们正常的信息传递与资料传输造成了威胁与影响。所以,数据加密技术需要得到更大的改进,保证计算机用户数据的安全。

2 据加密技术的具体特征

2.1 数据加密技术的原理

通过采用数据加密技术,能够将数据输出端输出的信息内容进行重新的编码,并且将真实原始的数据进行有效的隐藏,没有特定环境以及指令的掌握密钥难以发现真实的原始数据,从而更好地保证数据的保密性,更好地保障人们的隐私安全,避免其他人窃取重要的信息,在网络技术应用过程当中最为重要的环节便是数据的传输,通过保障数据传输的安全性,能够保证网络的整体运行。

2.2 数据加密的具体方法

数据加密的技术可以分为两种,分别是对称式加密以及非对称式加密。对称式加密主要是在掌握同一个密钥的个人用户之间进行应用,该密钥无法让其他用户,发现原文内容。通过使用对称式的加密数据,可以让同用户的加密及解密使用同一个密钥,并且改密钥非常难以破灭,对此当一个用户拥有同一个密钥的时候就能够做好密钥的保密工作,有效的保障数据的安全性,对此在对称式加密当中,密钥的安全性能决定计算机数据的安全性,当密钥管理出现问题的时候,从而容易导致相关数据的泄露,数据的传输也难以保证保密性以及安全性。除此之外,采用对称式的加密技术的加密及解密的速度与非对称式的加密技术相比较快,并且所采用的密钥比较简单,现如今很多行业都采用对称式的加密技术进行相关数据的传输更好的保障数据的安全性。

3 造成计算机安全隐患的主要因素

3.1 计算机病毒的攻击

在计算机技术应用过程当中受到最大的威胁便是计算机病毒攻击问题,由于在计算机运行过程当中容易受到病毒的攻击,从而难以保证计算机网络的安全性,计算机病毒攻击的危害比较大,产生该现象的主要原因便是在计算机病毒攻击的过程当中破坏性比较大,并且隐蔽性比较好,难以及时发现病毒的存在潜伏性比较长,容易在长时间内窃取相关的数据但是难以发现,在计算机应用过程当中,通常利用执行程序方式进行运行病毒,从另一种含义上可以被称为一项可以执行的程序,对此病毒可以在电脑中伪装成可有序执行的安全程序,通过利用信息技术对相关的信息数据进行复制传输,并且在传输的过程当中,通常以文件传输以及文件执行以及文件拷贝的方式为主。

3.2 计算机系统安全漏洞隐患问题

在计算机系统运行过程当中容易因为各种因素的影响出现一些安全漏洞问题,尽管安全漏洞问题,与病毒相比破坏力不强,但是依然会给计算机用户以及相关的数据带来极大的安全危害,计算机在运行过程当中离不开网络技术的帮助,随着网络技术的不断发展,使得计算机应用的范围越来越广,同时在网络技术发展过程当中也需要借助计算机的帮助,对网络进行维护以及保障。

3.3 数据仓库系统的安全隐患

企业或者事业单位在工作过程当中需要存储许多数据资料,对此为了能够保证数据资料的安全性便会建立属于自己专用的数据仓库,储存单位内部的重要数据资料信息,尽管数据仓库的安全性比个人用户的安全性比较高,但是也容易存在一些安全隐患,黑客可以在SQL当中注入漏洞,并且利用漏洞进入数据库,窃取相关的

重要数据信息。

4 数据加密技术在计算机网络云安全中的应用探究

4.1 计算机软件安全应用

计算机网络体系运行过程中,绝大多数是依托于软件功能来实现的,如浏览器网页、应用类软件等,其都需要经过相应的网络服务请求来实现的,而在此过程中,数据信息传输将面临极大的安全风险,为进一步加强系统的安全性能,数据加密技术在实际应用过程中,应以用户的实际操作为核心,通过建立相应的信息服务框架,提升计算机网络的运营质量。首先,应设定正确的密码框架,当计算机设备处于公用状态时,应对其中某一类特定运行的软件设定独立密码,当非计算机用户进行操作时,如软件密码验证错误的话,则软件本身将无法启动,此等操控形式也从根本上解决信息泄露的风险。当计算机设备遭受病毒侵袭时,数据加密技术所建构的防护体系,可令系统对数据缺失、所受攻击的部位进行相应的信息反馈,将系统当前的运行情况反馈到既定的网络体系中,此时系统将作出响应手段,对病毒进行有效处理。另外,通过数据加密技术与云端数据库的连接,可为用户提供自动化信息检索服务,依据内部数据基准的核对,对系统中原有数据的隐藏风险进行检验,以此来提升数据传输的安全性。

4.2 局域网安全应用

计算机网络体系的发展,间接推动着社会体系的信息化变革效率,目前,大部分企业在运行过程中,依托于计算机网络平台对内部各类数据信息进行综合处理,计算机设备的效率性、精准性的运营模式,可极大提升企业自身的发展效率。尤其是在企业管理方面,通过软件系统的支持,可令企业实现有序性的数据信息操控,满足自身对数据处理的需求。目前,企业在运行过程中,多以局域网的建设为主,通过各个部门内的信息节点链接,保证数据信息可在局域网内进行对点式的传输。数据加密技术在实际运用过程中,可对企业内部网的运行提供安全保障,例如,数据信息在传输过程中,内部路由器可直接对信息进行节点加密处理,对源数据信息进行备份并回传到主操作系统中,然后相应的部门在利用密钥对文件进行解密处理,在此类数据传输下,可有效提升数据信息的处理效率与处理质量。

4.3 电子商务安全应用

电子商务平台的建设,代表着一种新的经济格局,依托于网络平台可快速实现资金与货物交换,极大节省社会资源成本的消耗。然而电子商务平台在运行过程中也面临着相应的漏洞,令用户的个人信息遭受被盗窃的风险,其将令交易双方造成严重的经济损失,同时也为电子商务平台的发展带来负面影响。数据加密技术的应用,则可为用户及企业建立数据化安全框架,当用户进行某一项操作时,软件系统将自动发出协议请求,数据加密技术是在数据传输端建立一个加密节点,确保用户端所传输的数据处于一个相对安全的情况,同时系统平台中的身份认证模块、交易密码模块等,更是为整体交易流程提供相应的防护手段,令用户在电子商务平台下可进行安全性操作。

5 结语

数据加密技术能够在计算机网络安全当中得到广泛的应用,保护计算机网络的安全性。同时采用该技术能够促进互联网的进一步发展和安全性的发展,更好保障人们的隐私权利。

参考文献

[1]赵阳.数据加密技术在计算机网络安全中的应用价值研究[J].网络安全技术与应用,2018(12):32-33.

[2]田远.计算机网络通信安全中数据加密技术的应用[J].科学技术创新,2018(34):87-88.