数据加密技术在计算机网络安全中的应用

余 晨
航天工业发展股份有限公司 北京 100070

摘 要：本文从计算机网络中存在的安全风险出发，着重分析数据加密技术类型及其在计算机网络安全中的应用。在计算机网络技术高速发展的社会背景下，计算机计算在人类的生产生活当中占有重要地位，而在大数据处理模式下的今天，人们的基本信息、个人隐私或是企业的内部消息等，都会保存到计算机之中，使计算机网络的使用产生了相应的网络安全问题，数据加密就是保障网络安全的关键部分，而随着技术应用的丰富，各种数据加密问题也随之而来，人们可以使用一些算法技术对信息进行加密，从而实现了信息隐蔽，进而达到保障网络安全的效果。

关键词：计算机网络安全；数据加密技术；应用

1 计算机加密技术的有关概述

1.1 数据加密概述

数据加密是按照确立的密码算法把明文信息转变为附有密钥的数字信息，同时它也是计算机安全防护的重要技术。数据保护是密钥设置的核心目的，密文种类也分为很多种，其中端口加密、节点加密、链路加密是现今数据加密的重要形式。特别是在电子商务系统与银行系统中，数据加密的运用相对宽泛。比如，在银行系统中，银行数据加密技术呈现在网络设备间的链接上。进而呈现出它和网络交换设备间的联动。在防火墙与交换机运用中，把数据信息传输至系统安全设备上实施加密处理且加以检测。数据加密技术的运用是确保数据在网络传输时，对数据发挥着重要保护作用，加密技术将数据进行密码处理，使不法者偷取信息有一定难度，对核心信息我们应该实施多次加密处理，这会起到强化保护效果，加密技术在信息输入错误时，就会使防火墙与交换机交换数据端口断开或关闭，这样做具有一定防护作用。目前，数据加密技术的运用，在计算机网络安全中发挥着重要效果，同时具有至关重要的现实运用效用及价值如图1所示。

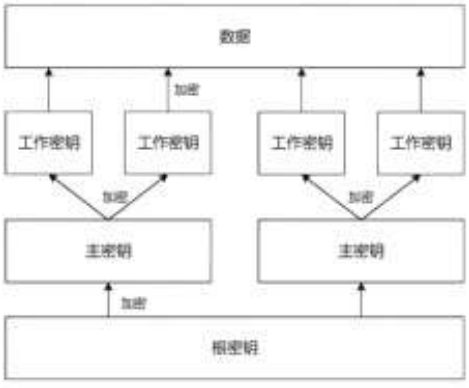

图1 数据加密技术的应用图

1.2 数据加密的运用与算法

数字签名认证技术在计算机网络技术中运用，网络认证技术是现今数据加密技术发展的最高阶段。它实际上是通过用户数据核对方式来设立用户登录权限，进而呈现防御外来侵害，保证网络安全运行。现阶段，数字签名技术的运用相对宽泛，数字签名主要是用密钥计算办法与数字加密原理保证网络安全运行的。用户数据输入正确后才能登录，同时也是数字签名认证的主要需求。

循环移位算法是数据加密算法中常见的算法，它实现了数据位置的调换。换言之，在数据传输期间，数据是以字节为单位，呈现出数据字节间的循环移位，附有较强规律性，但对破译密钥者却增添了较大难度，对数据实施必要的处理及构建密码文，该种办法适用又简单。

2 计算机网络中存在的安全风险

2.1 网络病毒

网络病毒是互联网使用中常见的安全风险，属于典型的外部安全威胁。病毒一般以恶意软件为媒介，出现在人们所使用的计算机上，当计算机启动后就会对计算机进行传染，通过入侵网络并盗取个人或企业信息的方法，获得盈利，给个人生活和企业发展带来恶劣影响。

由于网络病毒的隐蔽性较强，人们在使用计算机的时候很难发现潜伏的网络病毒，很可能人们在访问互联网的过程中就会默认地加入了网络病毒程序，令人防不胜防。由于网络病毒的传染频率非常快，潜伏性和寄生性都较强，还具有着感染性，因此许多使用者并不会容易地发觉病毒的出现，但在短时间内就会扩散至多台计算机设备，从而造成了相关的信息损失并造成很大经济损失。

2.2 系统漏洞

当前数据共享技术的运用已经日益普遍，个人计算

机在与互联网终端相连后就可以进行数据资料的上传、查看、下载，给我们的个人办公和日常生活提供了很大的方便。不过由于互联网的开放性特点，出现了许多互联网漏洞，从而造成互联网病毒的大量传播，造成了互联网瘫痪，泄漏大量用户数据，并导致巨大经济损失。

由于各个类型的软硬件计算机及其系统类型均会产生系统漏洞，因此硬件安全、应用软件安全性以及技术安全都将严重地制约着系统漏洞的出现和发展。因此鉴于系统漏洞所造成的计算机网络安全危害，不但必须修补硬软件缺陷，而且还必须完善网络认证的安全级别。另外，系统漏洞涉及的区域很多，涉及操作系统的应用软件、客户端、互联网上的客户端、防火墙、路由器等系统的正常工作，各个平台的操作系统也面临大量的系统漏洞。

2.3 非法入侵

在当前的网络时代，用户在使用计算机时操作不规范，就会造成信息安全危险的形成，而非法入侵则主要包括了非法登陆、个人信息丢失、拒绝网络服务、传播病毒等情况。在对以往的数据信息盗取记录统计结果分析中可以看出，数据信息被窃取的大部分因素都是由于黑客采用了非法方式进入操作系统中并攻破防火墙，从而盗取了整个计算机系统中的大部分数据信息，这样将会导致计算机管理系统遭受更大的信息安全危险，而破坏者则会首先把操作系统毁坏掉，进而对网络系统造成损害，使程序无法再正常工。在计算机数据信息管理系统中，所涉及的信息都不会非常紧密的被捆绑，因此当黑客再次拷贝数据时，数据信息就会泄漏出去，在网络的其他区域传播，安全程度就越来越低。当不法分子致使计算机网络系统的数据信息管理系统遭到破坏时，就会通过抢占了计算机网络系统的数据库，并获取了密钥和网关的掩码，然后对其执行了第二次编程，进而对计算机网络系统进行远程管理，给用户造成损失。

3 数据加密技术在计算机网络安全中的应用价值分析

3.1 电子商务

随着我国经济的不断发展，计算机发展速度加快，同时在商业发展中开始占据了更多的位置，为电子商务的发展提供了较多的技术支撑，使得人们的购物更方便，购物体验更佳。但是在实际应用中，依然存在着各种网络安全问题，使得电商中各个环节的实效性没有被完全体现。电子商务中的数据具有较强的意义，无论是对消费者还是对企业来讲都是至关重要的，所以一般在使用相关软件时尤其要注重个人信息的保护，若是其中一些信息遭到非法盗用或者是泄露，会严重危害到用户个人以及企业团体的利益。不过如今在数据加密技术的保护之下，电商的安全性被提高了许多，同时也更注重用户隐私。

3.2 计算机软件

计算机软件在应用过程中极易受到各种病毒的影响，也很容易受到黑客的侵害，这严重影响到了用户体验，同时为用户计算机使用带来了较多的威胁。所以在计算机软件使用方面需要严格注重其应用安全。可以采取多项保护措施，并将数据加密技术应用其中，促进软件使用的安全性。数据加密技术在提升计算机软件应用安全方面，具体有以下集中表现。首先用户对软件使用进行加密之后，其他用户在不得知其密码的状况下无法启动软件，所以非指定用户无法在不被允许的情况下获取用户信息。其次运用数据加密技术，能够有效帮助软件及时发现病毒迹象，用户在对软件使用过程中，若操作不当，该软件会及时提醒并阻止用户操作，防止各类病毒的侵入。再者用户在对软件操作时，数据加密技术能够在检查程序时及时发现病毒或者是其他隐患，并能够有针对性地采取清除操作，有效提高软件的安全性[1]。

3.3 数据库

企业内部一般会设有自身的数据库，随着科技发展，大量数据涌来，数据库的存在能够有效对各种信息进行筛查记录，所以数据库对于企业发展而来是非常重要的，保护数据库安全也能够更好地促进企业发展。在现实发展中，一些不法分子容易针对企业数据库来盗取信息，若一旦信息泄露，容易给企业带来非常大的损失，所以数据信息加密技术慢慢受到企业的青睐。

3.4 云服务

对于用户而言，云服务中的信息异常重要，对其进行保护，能够及时避免个人信息的泄露，如今人们所熟知的身份验证技术能够有效对云服务信息加以保护，这一技术能够有效划分用户对于设备的使用范围，从而对相关软件或者是其他系统使用划定权限，用户操作的差异性能够有效促进信息的保护。但是相对来讲，如今的云服务数据加密还并未得到高度优化，所以依然存有较多的安全性问题，相关数据单位可以适当将其数字签名技术与动态身份验证相结合，以此来对用户权限加以限制，保护用户信息，进一步降低信息风险[2]。

4 数据加密技术在计算机网络安全中的实践应用

4.1 在电子商务领域中的应用

随着计算机通信技术的蓬勃发展，电子商务应运而生并逐渐进入其发展的鼎盛时期，电子商务当中的一些订单交易信息以及用户个人身份证、账户信息和密码等安全

都需要数据加密技术来保护。通过加密技术对电子商务中的认证信息和数据签名等进行保护，可以有效提高电子商务交易的安全性。例如当用户上网进行商品购买时，会涉及个人银行卡和身份信息的安全，这些信息是必须要绝对安全，不能轻易泄露，一旦个人信息被不法分子获取，就会给用户造成严重的财产损失。数据加密技术就是在这些方面发挥其重要作用，不仅对用户的交易信息进行加密保护，同时也拓宽了电子商务的交易空间。

4.2 在企业网络中的应用

数据加密技术还可以保障企业财务信息的安全，企业财务部通过加密技术将部门内部机密妥善处理，可以让企业运行更加稳定。加之近几年来社会经济不断变化，很多企业之间已经不是单打独斗的模式，它们更多的是通过财务共享实现互惠互利的合作模式，但是各企业财务部门的机密信息却是不便向合作伙伴公开的，有了数据加密技术，企业在保护自家财务信息的同时不影响和别的企业合作，这对于企业发展有着非常重要的意义，通过加密技术将企业信息数据加密处理，提升企业财务业务的安全性[3]。

4.3 在网络数据库中的应用

在网络数据运行过程中，数据加密技术通过和防火墙协同抵御木马病毒的入侵，这样可以防止网络数据被非法访问和盗取，提高数据加密的安全级别。目前我国正向大数据时代飞速发展，网络数据库借助加密技术来完成一系列传输工作，并且正确区分输入、传输、调取等功能。通过数据加密技术，借助不同密钥的权限，对特定的信息进行保护、读取，可有效防止黑客入侵。因此数据加密技术对网络数据库的信息具有显著的保护价值，也是信息能够安全储存、传输的重要媒介。通过数据加密技术，对不同数据匹配不同密钥，这也将密文的安全级别一再提高，针对不同的服务器，数据加密技术还能进行差异化处理，从而有效提高信息数据加密的深度[4]。

4.4 应用于虚拟私有网络

在现代化生活中，由于人们生活方方面面都无法离开网络，但其中存在了一定问题，例如，企业网络安全问题，企业信息被盗取的同时，网络安全也会出现一定问题，如果企业的信息被窃取可能就会造成企业财产经济利益发生损失。在计算机时代，要是建设大规模的局域网并不是很简单，需要专门的企业去租用服务器或者连接专线，在此情形下人们就形成了局域网的专属网站，利用虚拟局域网络实现了各个网络连接，也适用于企业内部的资源共享，即广域网。此过程中，由于木马病毒风险多来源于外界，企业如果不注意网络安全，则企业内部的关键信息极易流失，从而使得正常办公工作遭受一定负面影响，甚至会造成企业的内部关键信息丢失，从而对企业的经济效果形成负面影响。企业在内部有线局域网中采用数据加密技术，对数据信息传输过程进行了保密，在文档接收后，可以确保在文档传输和处理过程中没有受其他原因影响[5]。

4.5 信息加密技术的应用

信息加密技术是指在确保信息系统内容不被损坏的前提下，增加了大批必须保密的重要数据。与传统数据信息安全保密方法有所不同，信息加密后看上去如同一堆乱码，但明文信息内容却与重要信息内容完全没关系，它不但保存了重要信息系统的内容，同时还大大提高了数据信息安全的安全稳定性，进而确保了网络的平稳运行。其主要使用密钥来进行信息加密，采用嵌入算法把要保密的重要信息内容附加到明文信号中，从加密主机中经过通道传给另一主机，然后再通过密钥进行解码，在数据信息中恢复有用的信息内容，解密技术也相当普遍，此基础上要求节点两端保密设备实现相同的目的，从而实现了数据信息保密。如果袭击者完全不了解加密，将无法找到要求加密的个人信息，也无法盗取加密的个人信息。但必须关注的是，信息加密技术对互联网管理存在着较高的要求，在大量数据信息传递过程中，信息加密技术极易出现数据流失等问题。

结束语：综上所述，伴随社会经济的飞速发展，互联网与计算机技术在人们社会生产与日常生活等方面施展了更加关键的作用。社会各界也更加重视计算机网络安全，以及网络经济的迅猛发展，对数据加密技术明确提出了更高的标准与更多的要求。为了创建愈发稳定与安全的网络环境，除了应深入研究以及优化数据加密技术外，还应针对目前的网络非法攻击手段与计算机网络安全问题进一步制定高效的应对策略，进而更好地保障网络用户与计算机网络的安全。

参考文献

[1]马小翠.数据加密技术在计算机网络安全中的应用探讨[J].产业与科技论坛,2021,20(18)：42-43.

[2]杨庆成.数据加密技术在计算机网络安全中的应用[J].网络安全技术与应用，2021，(9)：23-24.

[3]吴琳琳.探究计算机网络通信安全中数据加密技术的应用[J].电子世界,2020,(23):166-167.

[4]金保林.数据加密技术在计算机网络安全管理中的应用[J].电子世界,2021，(16)：178-179.

[5]白海军.数据加密技术在计算机网络安全中的应用探析［J］. 数字通信世界，2020，184(04):123.