数据加密技术在计算机网络安全中的应用

李 琳 卢 镭 周 庆
江西应用技术职业学院，中国·江西 赣州 341000

【摘 要】随着科技的反发展，计算机网络安全是困扰众多网民的难题。数据加密技术作为一种新型网络安全技术，对于网络信息传输安全保障有着积极作用。将数据加密技术应用到计算机网络安全上，以数据为载体实行系统化加密处理，可以有效避免数据丢失、损毁和泄漏，提升计算机网络安全性，确保计算机安全稳定运行。本文对计算机网络安全中数据加密进行了简要分析探究。

【关键词】计算机；数据加密；网络安全；应用

计算机网络安全的风险根源在于计算机自身系统漏洞、网络病毒、黑客攻击等方面，在应对网络安全问题上，信息加密技术是一项有效手段，可以通过计算机节点加密、端对端加密、链路加密和密钥加密等多种技术来实现。对数据加密技术进行合理运用，能够有效提升计算机网络安全，当前，数据加密技术已经被广泛应用在各个领域，取得很好的成效，为计算机行业发展立下汗马功劳。

1 计算机网络安全

随着网络技术飞速发展，互联网已经融入人们日常生活工作当中，为人们带来极大便利，比如人们利用网络进行购物、订餐、购买车票和电影票、传输信息等等。计算机网络安全指的是依靠网络管理及技术保障，不断增强网络数据信息的保密性。完整性和有效性，增加网络系统运营稳定性，有效抵御黑客攻击，防止系统漏洞影响网络安全。现阶段计算机网络安全主要有网络设备安全与网络信息安全两种，也就是物理安全和逻辑安全。网络设备（物理安全）安全侧重点在于防止人为破坏网络设备，网络信息安全（逻辑安全）侧重点在于保障信息准确性、可靠性和保密性。

2 计算机网络安全存在的问题

2.1 系统自身安全隐患

人们广泛运用计算机技术进行数据信息收集和输出，在此过程中必然会用到网站及网络软件，虽然这些网站和网络软件为广大用户带来诸多便利，使人们能够高效开展查询工作，但是因为这些网站和网络软件大多会存在安全漏洞，加上部分程序设计人员故意留下的“后门”，如果这些漏洞或后门被不法分子所利用，将会严重影响到计算机网络数据信息安全，严重时会引发群体性数据泄露事件，给人们个人信息及财产安全造成不良影响[1]。

2.2 黑客入侵

黑客作为互联网时代独有产物，给人们的印象十分恶劣。其通过入侵计算机网络来窃取各类机密信息，对企业发展和个人生活造成严重影响。这些黑客大多有着很强的计算机技术水平，而且随着计算机网络的普及，黑客年龄有着低龄化的趋势，许多低龄黑客甚至还未意识到入侵他人网络是违法行为；另外，有些黑客会为了一己私利，进行有目的有针对性的黑客活动，破坏网络信息安全，造成网络数据信息丢失或者网络信息系统故障，严重影响计算机的网络安全性。

2.3 网络管理不够规范

网络系统需要工作人员进行严格管理控制才能够保障高效运行，但是由于网络管理员自身专业技术水平和专业素养的高低，使得计算机网络存在一定安全隐患。一些网络管理工作流于形式，相关人员没有严格遵守管理制度来进行操作，也没有定期开展计算机网络安全检测，使得计算机网络安全性大打折扣。

2.4 计算机病毒

病毒是最为常见的能够危害计算机系统安全的软件，一般病毒具备很强的潜伏性、破坏性和攻击性，会隐藏在非法软件或网站当中，通过光盘、U盘、移动硬盘、邮件或压缩包等载体进入用户计算机系统，一旦用户打开后，就会自动下载病毒软件至计算机系统，造成系统被破坏。虽然当前电脑基本都安装有杀毒软件，但是病毒自身也在不断进化，利用系统漏洞入侵硬盘。计算机病毒能够长期潜伏于计算机系统当中，而且能够伪装成可以有序执行的程序，通过复制和传输模式盗取用户信息，给网络安全造成极大危害。

2.5 数据库系统管理缺陷

大数据时代，数据库成为信息存储的重要节点，运用频率非常高，一般企业都会建立数据库来存储企业自身内部资料信息，这个数据库专属于企业，很多信息涉及员工个人隐私（如姓名、年龄、联系方式、家庭住址、健康状况等），是不会对外公开的，因此，数据库的安全性非常重要。通常来说，企业数据库安全等级比个人用户安全等级要高很多，但是由于等方面因素的影响，数据库安全也会受到威胁，而且一旦数据泄露，将会引发一系列严重后果。

3 数据加密技术

数据加密技术是利用密码学当中的相关知识，运用密钥、加密函数将某段信息明文进行更替或整改，使其转换成为与原来明文不一样的数据信息，加强其安全可靠性，然后再将其传递至接收方。数据接收方接收到完整数据信息后，可以通过解密密钥和解密函数进行数据信息还原，从而实现信息数据安全传递。近些年来，数据加密技术得到社会上的普遍关注，成为计算机网络安全技术的宠儿。早期的数据加密技术类型较多，如置换表算法、循环冗余校验、XOR 操作算法等[2]。

3.1 对称加密技术

此种技术也被称为共享式密钥加密技术，主要是数据信息发送方和接收方通过使用相同的密钥来进行数据信息加密和解密操作。在运用该项加密技术时，密钥是由双方在信息传递之前就共同确定的，因此，只要双方都不泄漏密钥，就能够保障数据信息传输的安全性。主要有DES、IDEA等共享密钥形式，以DES加密密钥为例，DES技术应用64位对称数据，以其中任意56位为密钥，余下8位为校验方式，使用该密钥技术进行数据信息传递，能够有效保障数据信息安全性、保密性和准确性，运行效率高、机密速度快。

3.2 非对称加密技术

这种技术俗称公钥加密技术，指的是数据信息发送方与接收

方运用不同密钥及函数进行数据信息加密及解密，由于数据信息传递双方并不需要提前交换密钥，在一定程度上降低了因密钥泄漏导致的安全隐患，保障数据信息传输安全性、保密性和可靠性。发送方使用接收方提供的公钥进行数据加密，接收方运用自身私有密钥进行解密，这样一来，信息即使在传递过程中被第三方非法截获，也会因为没有相应私钥而无法得知数据信息内容。利用数字加密是一个不可逆过程，也就是说必须有私钥才能够解密。非对称加密的主要缺陷就是加密速度很慢，由于需要强大的数学运算程序为基础，哪怕信息量很少，使用公钥加密也可能需要几个小时。

3.3 链路加密技术

链路加密技术也称为在线加密技术，主要是传输数据在物理层面之前的链路层实施加密。接收方就是位于传输途径上的所有节点机，信息在两个网络节点之间通过链路加密可以形成一次性通信链路，在经过每台节点机时都需要进行解密和再加密，直至数据信息送达目的地。链路加密传输的所有信息在被传输之前都需要进行加密，到达每个节点后对其进行解密，使用下一个链路密钥对信息进行加密后，再进行下一次传输，在抵达目的地之前，一条信息可能经过多次通信链路传输。由于在每个传输节点信息都进行解密和加密，使得链路加密掩盖了被传输信息的起点和终点。链路加密只能够保障通信链路安全，在一个网络节点上，信息是以明文形式存在的，因此，必须保障每个节点的物理安全，以免出现信息内容泄漏。但是保障每个节点物理安全需要很高的费用。

3.4 节点加密

节点加密指的是在节点处采用与一个节点机相连的密码设备，密文在该设备中进行解密后重新加密。在节点加密过程中，除了发送节点与接收节点的信息是以明文形式出现外，中间节点都只是进行密钥转换，密文在通过中间节点时只是在密码装置中解密和重新加密，节点机是没有明文通过的，有效规避了链路加密时节点容易受到攻击的弊病。节点加密技术具备较高安全性，其与链路加密有着相似之处，都是依靠链路完成对数据信息的加密，区别在于链路加密时节点有明文出现，而节点加密无明文出现。

4 数据加密技术在计算机网络安全上的应用

4.1 虚拟网络方面

随着信息技术的发展，网络覆盖面日益广泛，网络成为人们生活各方面不可分割的部分。现代企业大多建立起专属局域网，采取租赁模式，借助专业线路构建起虚拟专用网络，这个网络也被称为广域网络。保障广域网络安全有着非常重要的意义，为增强广域网络安全性能，需要将数据加密技术应用其中，实现数据信息的安全传输。数据信息可以通过数据包形式实现转换目标地址和远程访问数据，整个工作模式都是通过加密路由完成，在VPN抵达指定位置后，路由器能够自动完成数据解密处理工作。

4.2 电子商务方面

在电子商务活动中，部分软件需要用户需填写部分私密信息，这时就需要采取数据加密技术来确保电子商务系统安全，一般是采取数字证书、互联网安全协议等数据加密方式。为避免不法分子窃取用户信息，需要采取更加先进、保密性更好的数据信息加密技术，以保障用户安全[3]。

4.3 数据库方面

现阶段数据库的管理系统主要有两种，一种是Windows NT系统，一种是Unix系统，两种管理系统都有不同的安全等级之分，低等级数据系统中的存储系统极易受到黑客和病毒的攻击，而且其公共通信传输通道防御病毒能力较弱。对于黑客而言，只需一台普通计算机就能够轻松盗取数据库中的数据信息。早期的加密措施大多为设置口令、密码以及访问权限等形式，这种加密手段极易因为密码被破解而导致信息泄露。现阶段常用的加密措施时对数据库内部数据信息进行加密，这样一来，就算数据丢失或者被窃取也不会被轻易破译，保障了用户隐私和账户安全。

4.4 数字签名技术

当前在网络安全应用最多的是认证技术，该技术能够有效鉴别和确认用户真实身份信息。常用的有口令认证及数字签名认证。口令认证操作简单、成本低廉，但是安全系数不高。数字签名则是用户需要通过加密及解密来确定使用者身份，以保障使用者与原本数据库信息创作者为同一人，防止信息被未经授权用户恶意修改或窃取，确保用户数据信息完整性与安全性。

计算机加密技术对于计算机网络信息安全有着积极作用，合理运用加密技术有利于互联网安全稳定，全面保障用户账户及个人信息安全。因此，我们应当积极推进加密技术发展，为计算机网络信息安全奠定基础。

参考文献:

[1]郑辉.计算机网络信息安全中数据加密技术的应用分析[J].中国信息化,2021(03):71-72.

[2]于浩.基于数据加密技术的计算机网络安全研究[J].网络安全技术与应用,2021(03):20-21.

[3]余治强.数据加密技术在计算机网络通信安全中的应用研究[J].数码世界,2021(03):18-19.