信息安全

DOI:10.16525/j.cnki.14-1362/n.2022.01.041

网络信息安全中数据加密技术的应用

刘　健
（天津工业职业学院，　天津　300400）

摘　要:人们在使用网络过程中会产生大量数据信息,信息安全问题随之而来,因此对数据加密技术的要求日益增大。基于此,从对加密数据技术的重要性展开探究,重点阐述了具体的技术要点,以期有关人士能够掌握核心技术,防止信息篡改、泄露等所带来的巨大不利影响,着力于提高网络信息安全与技术。

关键词:计算机网络　信息安全　数据加密技术
中图分类号:TP393　　**文献标识码**:A　　**文章编号**:2095-0748(2022)01-0119-02

1　数据加密技术的重要性

随着大数据的不断变化，网络的边界变得越来越模糊,数据信息开始在互联网上失去隐私,从而共享出现越来越多的数据。虽然对社会的发展产生一定的积极影响,但也会出现威胁网络信息安全要素。即使计算机上有防护杀毒软件,但在大数据时代,这远远不够对信息保护的需求。这时数据加密技术的出现发展,对计算机网络影响十分重要,不仅促进着计算机发展,还能推动社会进步发展,打造优质网络环境[1]。

2　计算机网络信息安全中运用的数据加密技术

2.1　节点加密

这一技术的媒介是计算机系统的节点，设置的安全节点,保证了两个节点之间信息传输的安全性。同时,依靠密码装置,将其连接到节点上,为了完成对重要保护节点的高质量加密,在加密阶段,采用密文解密的思路。密文传递是这类加密技术的主要传输形式,在加密过程中,借助中间点可以获得有效的信息数据。节点加密除了加密模式以外,还可以进行相关的解密操作。通过大量的网络信息加密实践,采用节点加密或链路加密都可以实现理想的效果。为了达到节点加密的预期目标，做好网络相关信息的安全防护,需要做好结合数据的处理,合理科学的选择加密技术,设置好信息加密位置;否则,若黑客破解时,后果不可估量。采用数据加密节点技术,可以提高整个网络数据传输的安全性，这种加密手法与链路加密技术较为相似，但是在节点加密过程中相关信息并不会出现在节点上,这样就可以对传输给节点的信息进行两次加密。节点加密技术如图 1 所示。

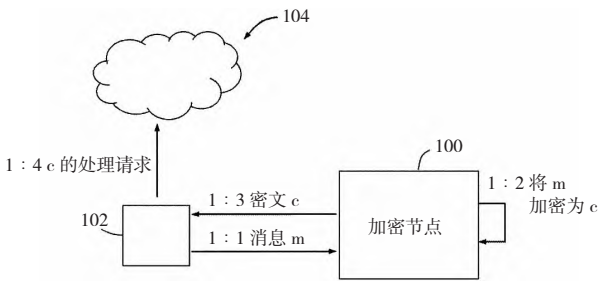

图 1　节点加密技术

2.2　链路加密

链接加密技术又称为在线加密技术，是一种通过计算机链路对传输的数据信息进行加密和保护的技术。链接加密技术需要与密钥技术相结合,数据传输前需二次加密网络传输各个节点，确保传输时所有数据信息都要经过链路中的多个节点。链路加密技术在信息传输中的密钥是不断变化来实现渐进加密和连续加密的。可将链路比作通道,在线路传递中数据信息的形式仍然是秘密文件，可隐藏数据信息的频率、长度,逐渐成为时代发展要求的新型加密技术。该技术的应用,可以提高网络环境的安全性、网络使用更加舒适、加密效果显著,进而大大提高工作效率。链接加密技术如图 2 所示。

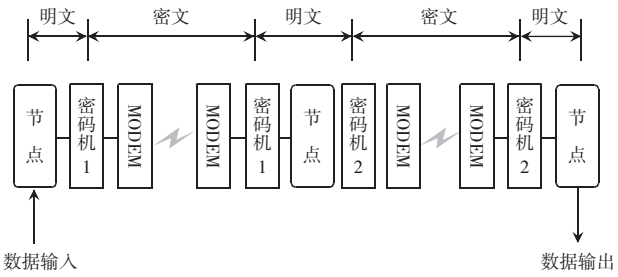

图 2　链路加密技术

2.3 端对端加密

端对端加密是一种比较新颖的加密方法，在现有数据加密的基础上,利用计算机系统的计算方法,将数据转换为秘密文件，然后以秘密文件的形式实

收稿日期:2021-09-22
作者简介:刘健(1985—),男,山东章丘人,本科,实验师,研究方向:计算机网络。

现信息在网络上的传输。如果将端对端加密和链路加密二者进行比较，选择端对端加密时，中间节点不需要使用加密、解密手段，因此不需要加密设置。伴随着技术的进步，加密可以通过软件实现，操作方式更加简单。利用端对端加密，每个用户之间都有一个安全的通道，用户需要共享密钥来进行通信，这里需要强调的是密钥总数由用户数目来决定，要求二者之间的数目相同，假设在通信中有 $n\times(n-1)=12$ 种密钥方法，每个用户都会得到$(n-1)$个密钥种类。在实践中，数目非一成不变，而是随着网络通信用户数量的增加而变化。为了安全起见，应在一定时间内重新使用新密钥，因此对密钥的使用会增加。端对端加密，其最突出的特点是将整个数据文件加密为一个整体，在接收者没有接收传输的信息之前，无论有没有密钥都不能解密并获取数据[2]。

2.4　科学的秘钥设置

定期维护和检查是必要的，为了防止信息泄露，应采取科学的维护手段。通过密钥完成解密工作，通过此方式，使信息的可靠性大大提高，信息被盗的概率也大大降低。软件的安全维护也是工作的重点。研究表明，将加密技术与软件系统技术相结合，可以起到更好的保护作用。如：定期检查、升级等。有效地防止各种病毒的感染，合理地规避安全隐患，从而大大提高系统的安全性。根据加解密的运用时密钥是否统一，可分为对称加密技术和非对称加密技术。根据加密技术对数据处理方式的异样，可分为分组加密技术和分流加密技术。

如何高效地保存好密钥成为对称加密技术的核心要求，一旦密钥被不法分子等盗取，对信息的安全性无法保障。非对称加密技术是指在加密和解密过程中使用不同密钥。公开密钥和私有密钥之间没有关系。能实现对密文的解密只能是私有密钥，进一步提高了信息安全性。因计算量大、耗时长等非对称加密的特性，导致其应用于少部分的加密工作中。但其中 RSA 算法是一种应用频率较高、相对可靠的算法，利用这一算法可完成双密钥的科学设置，更加有效地维护网络信息安全。

2.5　其他加密技术

1）需和医院、企业、学校、政府等机构一起搭建完善虚拟专用网络，联合公开密钥和私有密钥，加强对信息网络的管理，增加其安全性，保证使用虚拟专业网络的用户授权读取信息，也可通过账号、密码、IP 地址登录再操作信息。

2）在各大电商平台的发展，电子商务交易数量逐渐增长。互联网环境下，在进行交易时，双方的信息都会进行输送，若在不安全的信息环境下，极大可能丢失泄露个人信息，如：家庭住址、身份证号、银行卡号等，更甚是损失个人经济。因此，要完善商务交易系统体系，完善认证系统，降低风险指数，在用户登录时，利用账号、密码、人脸识别等方式，同时，使用数字、签名认证技术，降低或避免传送信息时的欺骗现象。

3　结语

计算机网络技术的突飞猛进，给人民群众带来生活、工作等的便利外，也存在着危害信息安全隐患因素。为了更好地维护信息安全的安全性、降低危险系数、打造良好网络环境，应根据现实情况选择最佳加密方式，重视其技术应用，不断发展并提高技术水平。

参考文献

[1]　涂胜斌，高文举.数据加密技术在计算机安全管理中的应用研究[J].电脑知识与技术，2020(30)：51-52.
[2]　魏军.数据加密技术在计算机安全中的应用[J].脑编程技巧与维护，2021(3)：93-94.

（编辑：刘楠）

Application of Data Encryption Technology in Network Information Security

Liu Jian

（Tianjin Polytechnic Vocational College, Tianjin 300400）

Abstract: When people use the Internet, a large amount of data and information will be generated, and information security problems will follow. The requirements for data encryption technology are increasing day by day. Based on this, this article explores the importance of encrypted data technology, focusing on specific technical points, hoping that relevant people can master the core technology, prevent information tampering, leakage and other huge adverse effects, and focus on improving network information Security and technology.

Key words: computer network; information security; data encryption technology