网络信息安全数据加密技术研究

蒋东君
四川通信科研规划设计有限责任公司　四川成都　610066

摘　要：数据加密技术可以作为网络信息通讯的安全防护屏障，所以能对数据安全威胁进行有效的防控，从而避免网络数据被盗用、被篡改等一系列问题发生。因此，为了保证网络信息的传递安全，工作人员就要对数据加密技术进行合理利用。本文先概述了数据加密技术，并分析数据加密技术的几大种类，最后详细探讨数据加密技术在网络信息安全中的应用，为今后相关方面的研究提供一些可供参考的依据。

关键词：数据加密技术；网络信息；安全

Research on data encryption technology for network information security

Jiang Dongjun
Sichuan communication scientific research planning and Design Co., Ltd. Chengdu, Sichuan 610066

Abstract: Data encryption technology can be used as a security barrier for network information communication, so it can effectively prevent and control data security threats to avoid a series of problems such as network data being stolen and tampered with. Therefore, to ensure the transmission security of network information, the staff should make rational use of data encryption technology. This paper first summarizes the data encryption technology and analyzes several kinds of data encryption technology. Finally, it discusses the application of data encryption technology in network information security in detail and provides some reference basis for future related research.

Keywords: data encryption technology; Network information; security

引言：

伴随着社会、经济的高速发展，信息化技术已应用到各行各业当中，极大地促进了社会的发展，同时也暴露出各种各样的潜在安全风险。比如黑客、病毒、网络漏洞等问题造成大量敏感数据外泄，给用户带来巨大的经济损失。因此，急需加速研究并应用数据加密技术，将相关数据内容通过重编码、隐藏和加密等方式进行处理，对数据安全威胁进行有效的防控，从而使不法者不能获取到真实的信息内容，避免网络数据被盗用、被篡改等一系列问题发生。

1. 数据加密技术

数据加密技术是指网络用户在网络通信系统运行过程中数据运输的明文数据，通过科学的计算方式对现有的数据进行合理的加密，进而实现加密传输的过程，有效防止外来危险的入侵。在此过程中借助以媒介为转换的密钥方式对现有的网络信息进行合理的加密处理，通过相关密钥获取加密后的内容以此保障网络信息的安全。加密技术是网络安全技术的基石，密码是加密技术中的重点，常用加密算法有DES及其各种变形：AES、RSA/ECC、Diffie-hellman，SHA-1/SHA-256以及以代换密码和转轮密码为代表的古典密码等。目前对理论上不可破译、不可窃听的量子密码技术的研究和应用是比较前沿的课题。

大数据时代背景之下，人们摄取消息的方式从传统的单一渠道转化为多元化的智能方式，因此在网络信息环境运行过程中，社会大众更加关注网络安全的问题，网络信息通信技术在不断的更新与变革过程中，对现有的数据信息内容进行合理的安全优化。提升网络信息技术人员的综合素养，使其充分掌握网络加密技术的性能、概念以及构成，进而通过充分协调相关技术，确保网络通信的安全性。

2. 数据加密技术的种类

数据加密一般在通信的三个层次来实现：节点加密、

链路加密和端到端加密。

2.1 节点加密

节点加密技术就是在节点机上连接密码装置，保证在密码装置内完成解密数据环节，之后利用加密手段对数据密文进行设置。在整个节点加密处理的实施过程中，要准确地传输明文的网络路由信息和报头内容，其目的是确保网络节点传输环境的安全和稳定。在加密完成后，外来访问人员就不能随意查看用户数据内容，网络用户的隐私就得到了维护。

2.2 链路加密

链路加密技术属于通信线路加密，在数据信息传输的全过程中贯穿运用，是比较常见的一种加密技术。在信息通信的过程中，数据处在加密的状态下进行传播，演示数据传播的始端和终端，保护数据传播的频率、长度，从而避免黑客攻击或盗取信息，达到维护信息安全的效果。在实践应用过程中，该技术将两端加密设施融合在一起即可工作，对网络通信技术有一定的负面影响，造成传播速度和效率下降。

2.3 端到端加密

端到端加密也被称为“包加密”，也是较为常见的一种加密技术，在数据传输过程中，整体都是密文形式。但是该加密方式与链路加密、节点加密有着显著的区别。端到端加密只有在传输以前亦或是接收以后再进行加密处理，在其他过程中不需要另外作出处理。所以这种方式相比较其他两种方式更加简便，并且有着较好的稳定性，除此之外，它的应用成本也较低，相对于节点加密，这种加密技术并不会对设备有较高的要求，并不需要设备同步，即便传输过程有一个节点被损坏，那么整体数据也不会遭到影响，对网络性能影响比较低。不过该方法不能掩盖数据发出点与接收点，所以存在一定局限性。

3. 数据加密技术在网络信息安全中的应用分析

3.1 提升软件的防护能力方面的应用

网络信息通信安全发展过程中对现有的加密技术进行合理的优化创新，借助加密技术实现对网络信息的安全防护，提升软件的防护能力，确保在受到外部攻击时提升网络信息的安全性。截断网络病毒的传输渠道，在现有网络信息系统遭受攻击时，首先会由黑客通过在幕后篡改相关信息或通过网信参数获取重要的数据信息内容，导致相关信息或重要文件丢失，进而为国家、单位及个人造成较大的经济损失。除此之外，在网络信息系统使用过程中用户会选择安装不同类型的杀毒软件，但是杀毒软件自身也存在着不同程度的危险，在病毒入侵时若杀毒软件不能进行及时的数据信息保护，会对网络信息安全产生较大的影响。因此，结合网络信息安全需求对现有的加密技术进行合理的优化创新，实现对应用软件防护能力的优化提升，定期检查网络信息系统的运行情况，通过所收集的内部处理信息为其选择合适的加密技术，形成双重保护的屏障，确保在安全的环境下完成数据信息的传输，进而提升网络信息通信传输的安全性。

3.2 在密钥实施数据中的应用

作为一种相对成熟的数据加密技术，网络信息的密钥技术可以被认定为是数据加密技术中的核心技术。总的来说，密钥技术就是在网络数据信息密钥的表现形式发生改变的前提下，对实际加密信息的多种书写方式进行模拟，通过多种形式来加密处理网络数据信息。目前，从加密算法角度可以将密钥技术分成私钥和公钥两种技术，由于私钥技术是私人性、专用性的，所以就对其应用产生一些制约。加密保护网络信息时，如果只使用私钥技术，就会降低其保密的安全性能，要结合私钥技术与公钥技术一起使用才能促进加密信息的安全性能得到较大程度的提高。数据加密技术应用于密钥实施数据中，必须用公钥技术先完成信息文件的传输部分，对其进行加密处理，避免泄漏信息的情况发生，在此之后，数据信息被用户接收到时，就能通过私钥技术去解密数据信息。采取这样的数据信息加密方式，其最大优势就在于能对用户收到的全部数据信息加强保护。总之，在密钥实施数据中充分利用数据加密技术，可以使网络信息的存储安全得到根本保障。

3.3 在计算机文件中应用

在计算机技术发展的同时，各类软件不断增多，在文件下载或传输的过程中，可能会携带某些病毒或被黑客攻击，进而影响计算机的使用安全或影响用户信息安全。很多企业、单位都对文件加密软件有十分迫切的需求，文档加密产品也随之增多，不同加密软件采用的加密技术手段也有所不同。为了确保加密的有效性，用户应该充分了解各种加密技术，目前最常用的加密软件技术包括驱动层加密和应用层加密两种。大部分企业都会选择驱动层加密的方式，因为这种方式在操作系统底层实施加密，不会影响内部员工的操作，同时具有较好的加密效果。在企业加密的过程中，还要了解加密产品的具体功能，检测产品的安全性。如果加密软件产品不符合用户的信息加密要求，则加密效果并不理想。

3.4 在电子商务中的应用

电子商务技术的核心是网络平台，所以电子商务运转的先决条件则是网络的安全与平稳。尤其在整体运转与交易过程中，牵涉客户身份数据及其电商客户自身经济利益，一旦数据被盗取势必给交易双方产生巨大的经济影响。在电子商务安全系统中，网络交易信息安全与网络平台安全是非常关键的板块，务必创建多种准入标准与身份信息验证流程，同时采取数字签证和数字签名等不同方式实施加密处置，上述数据加密方式完全可以提供优良的交易信息安全环境，杜绝违法分子或者网络黑客针对信息资源的秘密攻击，有助于推动电子商务的可循环高速发展。

3.5 在网络数据库中的应用

在网络信息通信中，数据库是一个较为特殊的存在，因为数据库中有着丰富的数据资源，其中重要信息非常多，是储存数据的重要系统。正因为其作用特殊，所以在信息安全管理中，数据库也是不法分子最常攻击的地方，通过破坏电脑非法侵入，获得丰富数据资源。很多单位在设置数据库的密钥时，没有充分考虑到安全性问题，将密钥单纯设置为简单的数字、字母，就很容易被泄露，给企业带来极大的损失。通过数据加密处理，能够有效增加密钥难度，防止信息泄露。数据库作为网络信息通信中的关键系统，通过数据加密能够让多个密钥充分保护好数据库，提高安全系数，降低信息泄露的危害。

4. 结束语

大数据时代已经来临，如何确保网络信息上传送的数据信息不易被泄漏、替换甚至伪造等，已成为网络信息安全急需解决的主要问题，同时也面临着更多全新的挑战。然而，创造网络数据安全环境的主要技术为数据加密技术，因此，深入学习数据加密技术的基础概念及其在网络信息安全中的使用是高效确保数据信息安全的先决条件，不断深化处置数据加密技术，创建完善的技术体系与技术内涵，才能最终加固网络信息的安全堡垒。

参考文献：

[1]李真成.网络信息安全中心的数据加密技术[J].电子测试，2021（8）：84-85+126.

[2]李正伟，周锐.数据加密技术在网络信息安全中的应用探讨[J].数字通信世界，2021（6）：198-199.

[3]于家德.数据加密技术在网络信息安全保障方面的应用研究[J].通信电源技术，2021，38（2）：135-137.

[4]付振帅.网络信息安全加密技术应用探究[J].卷宗，2020，10（20）：348.

[5]李辉.关于网络信息安全中数据加密技术的运用分析[J].数码世界，2021（5）：263-264.

[6]候倍倍.网络信息通信安全中数据加密技术的应用研究[J].电脑编程技巧与维护，2021（9）：164-165.

[7]周家栋.网络信息通信安全中数据加密技术的运用分析[J].信息与电脑（理论版），2021，430（12）：221-222.