计算机网络通信安全中数据加密技术的应用

张静，张洪健，周钰斌
廊坊市公安局，河北 廊坊 065000

DOI: 10.61369/TACS.2026010006

摘　　要： 随着我国社会经济和科学技术的发展，计算机设备已广泛应用于人们的生活中，给人们带来便利的同时，也引发了一系列的安全隐患问题，用户个人信息的泄露为其正常生活带来了较大的安全威胁。数据加密技术作为保障网络通信安全的核心技术，其应用研究具有重要现实意义。基于此，本文将重点探讨计算机网络通信安全中数据加密技术的应用路径，以期为优化网络通信安全防护体系提供理论参考。

关 键 词： 计算机网络；通信安全；数据加密技术；个人信息

Application of Data Encryption Technology in the Communication Security of Computer Networks

Zhang Jing, Zhang Hongjian, Zhou Yubin
Langfang Public Security Bureau, Langfang, Hebei 065000

Abstract: With the development of China's social economy, science and technology, computer equipment has been widely applied in people's daily lives. While bringing convenience, it has also given rise to a series of potential security risks, and the leakage of users' personal information poses a serious security threat to their normal lives. As a core technology for ensuring network communication security, the research on the application of data encryption technology holds important practical significance. Based on this, this paper focuses on exploring the application paths of data encryption technology in the communication security of computer networks, aiming to provide theoretical references for optimizing the security protection system of network communication.

Keywords: computer network; communication security; data encryption technology; personal information

引言

随着科学技术的不断进步，计算机网络在人们生活中扮演越来越重要的角色，如何保证网络安全随之受到了越来越多的关注。作为传递和存储信息的重要方式，计算机网络具有开放性的特点，是数据传输、信息交互的核心载体，各类敏感数据、核心信息通过网络实现高效流转，推动了各行各业的转型升级。但也带来了安全隐患，数据泄露、篡改、窃取、非法拦截等安全事件频发，威胁着个人隐私安全和企业商业利益，从而对计算机网络的健康发展产生不利影响。作为计算机网络通信安全防护体系的核心技术，数据加密技术凭借其加密解密、权限管控、信息校验等核心功能，可以有效抵御各类网络攻击，防范数据安全风险，保障数据的安全性。

一、影响计算机网络通信安全的主要因素

（一）网络漏洞

在计算机网络通信系统中，网络漏洞层出不穷，成为影响其通信安全的关键因素。网络漏洞往往存在于计算机网络硬件设备、软件应用在设计、部署以及后期维护中，为非法攻击提供了可乘之机，从而威胁网络通信过程中数据的机密性、完整性和可用性。从设计层面来看，在设计网络系统、通信协议或软件应用过程中，设计人员由于安全意识不足，忽视了安全防护机制的设计，导致计算机系统存在安全缺陷[1]；从部署层面来看，部分网络配置与软件应用的安全需求不匹配，使得存在的安全防护功能无法正常发挥，从而产生网络漏洞；从维护层面来看，当前计算机网络攻击呈现更加隐蔽性的特点，软件和硬件设备长时间不维护，将会产生新的网络漏洞，从而被非法攻击者发现，造成严重的数据泄露。

（二）安全防御不严密

计算机网络通信安全的保障，不仅需要先进的安全技术与硬件设备，更需要完善的安全防护体系与科学规范的安全管理。当前在个人或企业计算机网络维护体系中，通常仅部署单一的安全防护设备，如防火墙、杀毒软件等，缺乏系统性、整体性的防护

设计，形成了碎片化的防护格局，各防护设备之间缺乏协同联动机制，无法实现数据共享与策略协同，难以应对多样化、智能化的网络攻击[2]。同时，部分计算机网络覆盖范围不全面，多数安全防护技术多集中于网络边界与核心节点，对数据传输链路、终端设备、应用程序等环节的防护力度不足，存在明显的防护盲区，这成为计算机网络遭到攻击的重要突破口，从而影响其安全性。

（三）网络攻击技术不断发展

随着计算机网络技术与科学技术的不断发展，网络攻击不再局限于传统的攻击手段，如计算机病毒、木马攻击等，攻击者更青睐使用高技术水平的网络攻击技术，从而达到攻击效果提升、网络通信安全破坏力增强的目的。一方面，新型网络攻击工具更加自动化与智能化，可以自动扫描网络漏洞、识别目标节点、发起攻击并获取数据，整个攻击过程无需人工过多干预，大幅提升了攻击效率与成功率[3]；另一方面，攻击手段呈现出多样化发展趋势，除了传统的病毒攻击、木马攻击，还出现勒索病毒攻击、供应链攻击、APT 攻击等新型攻击手段，使得现有安全防护体系难以全面覆盖各类攻击场景。

二、计算机网络通信安全中数据加密技术的作用

（一）有效抵御非法攻击，保障数据安全性

数据加密技术本质上是对计算机网络用户数据进行加密的一种有效工具，以保证信息传输的完整性和安全性。在计算机网络通信过程中，数据需经过多环节传输，涉及网络节点、传输链路、存储设备等多个载体，而网络本身具有开放性、共享性的特征，攻击主体会通过拦截传输链路、入侵存储设备、破解访问权限等方式，非法获取个人隐私数据[4]。数据加密技术中的加密算法可以将原始数据转化为无序、不可识别的密文数据，使未授权主体即便通过非法手段获取到密文数据，也难以通过常规方法解读数据含义，无法从中提取有效信息，从而可以有效保障数据的机密性与安全性。

同时，技术人员主要利用加密技术对通信信息传输前的数据进行加密，且加密过程会按特定顺序对信息进行处理，链路加密后，通信信息不是一次加密，而是通过不同的链路节点进行多次加密，这样不仅可以全面覆盖数据的传输路径，还可以保证数据在传输过程中不被解密和拦截，以此保证计算机网络数据的安全性[5]。

（二）防止数据被非法篡改，维护数据完整性

在计算机网络通信中，数据的完整性至关重要，一旦遭到破坏，将会导致数据失去实际价值，从而引发一系列安全风险如数据错误导致的系统故障、篡改后的虚假数据误导决策、伪造数据引发的信任危机等。数据加密技术具有自主更新、同步传输和双重防护的特征，可以将加密处理与数据校验机制相结合，在对数据进行加密的同时，生成对应的校验信息，以此验证数据的完整性，判断数据是否被非法篡改[6]。此外，在数据传输环节，加密技术可对数据进行加密处理并生成校验码，数据传输过程中若被非法拦截篡改，校验码会出现偏差，接收端可通过校验码快速识别数据异常，及时终止数据接收或要求重新传输。

（三）阻止数据被非法访问，保护数据真实性

在计算机网络通信安全发展过程中，数据加密技术会对现有的防护体系进行排查和监管，有效确认数据真实性与授权合法性，防范非法访问、数据伪造、身份冒充等各类恶意行为，以此实现对网络信息的安全防护。一方面，在数据加密技术的支撑下，授权主体在发送数据前，会通过自身持有的密钥对数据进行加密，并附加对应的身份标识信息，接收端在接收数据后，需通过对应的密钥进行解密，同时校验身份标识信息的合法性[7]；另一方面，数据加密技术可以将密钥与授权主体进行绑定，不同的授权主体持有不同的密钥，未授权主体因不持有对应的密钥，无法对加密数据进行解密，也无法访问被加密保护的网络资源和数据，从而实现对授权合法性的精准确认。

三、计算机网络通信安全中数据加密技术的应用路径

（一）完善软件运行过程，强化存储数据安全管控

随着我国计算机网络通信用户的日益增多，存在着大量盗取网络通信用户数据的非法攻击者，导致用户或企业的计算机软件系统经常受到病毒或黑客的攻击，因此，加强数据加密技术在计算机软件中的实际应用，对于保护用户或企业的数据安全具有重要意义。一方面，数据加密技术可以对目前的计算机网络软件工作流程进行系统性、规范性保护，系统梳理软件的应用场景与常见安全隐患，以此形成双重屏障，有效降低计算机网络中的不稳定因素对软件造成的伤害。

另一方面，对于软件中储存的数据，数据加密技术可以进行加密处理，使其以密文的形式存在，当这些数据遭到非法入侵、窃取或损坏时，未授权主体无法获取数据的原始内容，从而保障静态数据的机密性、完整性和可用性[8]。此外，利用数据加密技术构建存储设备的访问控制机制，可以实现加密防护与访问管控的协同发力，如仅允许授权主体访问和操作对应的加密数据，拒绝未授权主体的非法访问请求，从而大幅度提升数据的安全性，保障软件稳定运行。

（二）借助数据加密技术，构建全链条安全防护屏障

数据加密技术可以对计算机网络通信中的现有数据进行合理、科学、规范地加密操作，使其在最终链路传递过程中以密文的形式进行呈现。将数据加密技术应用于计算机网络通信中，可以构建全链路、全方位的加密防护屏障，保障数据在全流程中以密文形式存在，抵御各类安全威胁，保障数据安全传输至目标节点[9]。其一，在数据传输过程中，端到端加密技术可以以密钥的形式，将数据在发送端进行加密，在接收端进行解密，以此保证数据传输的安全性。在传输过程中，所有中间设备均无法获取数据的原始明文，仅能处理密文数据。

其二，链路加密、节点加密等辅助加密方式，可以自主形成多层次加密防护体系，对全链条进行综合加密，以防范链路层面的非法监听和拦截；其三，数据加密技术可以覆盖所有类型的网络传输场景，包括有线网络传输、无线网络传输、局域网传输

等，并生成针对性的加密信息，以此帮助用户检验数据的完整性，为数据传输安全提供全方位的保障。

（三）加密数据处理环节，提高动态数据安全性

数据处理是计算机网络通信安全中的关键环节之一，在计算机网络系统接收到数据后，会经过解析、运算、转换、展示等一系列处理流程，然而在此过程中，数据会脱离保护状态，遭到非法截取、篡改、泄露等安全风险，直接威胁数据的机密性、完整性和真实性。因此需要将数据加密技术应用于数据处理环节，防范动态数据安全风险[10]。首先，采用数据加密技术，可以根据数据处理的流程和需求，实现加密和解密的实时切换，从而形成闭环管控，保证数据在处理过程中仅在授权范围内以明文形式存在，防范数据在处理过程中的非法泄露和篡改；同时，数据处理环节的加密应用，需结合数据处理设备的安全防护，对参与数据处理的服务器、终端设备等进行加密管控，防范设备被入侵后的数据泄露。

其次，数据加密技术可以对接收到的数据进行加密处理，仅允许授权主体在授权的终端设备上查看解密后的明文数据，一旦终端设备未授权或脱离授权环境，展示的数据立即变为密文，从而实现精准加密防护；最后，数据加密技术可以对数据处理过程进行全程审计和监控，记录数据的处理流程、处理主体、处理时间等相关信息，及时发现数据处理过程中的异常行为，如非法解密、非法截取、非法篡改等，采取对应的应急处置措施，防范安全风险的扩大。

四、结语

综上所述，数据加密技术是保障计算机网络通信安全的核心支撑。通过强化软件存储加密、构建全链条防护屏障、加密数据处理环节等路径，可有效保障数据的机密性、完整性与真实性。

参考文献

[1] 祖晓明 . 数据加密技术在计算机网络通信安全中的应用策略 [J]. 信息记录材料 , 2024, 25 (02): 30-32.

[2] 曹剑锋 . 数据加密技术在计算机网络通信安全中的应用实践 [J]. 数字技术与应用 , 2024, 42 (02): 103-105.

[3] 虞凤娟 . 基于数据加密技术的计算机网络通信安全设计 [J]. 信息与电脑 (理论版), 2023, 35 (18): 181-183.

[4] 魏凯明 . 数据加密技术在计算机网络通信安全中的应用 [J]. 中国新通信 , 2022, 24 (24): 1-3.

[5] 耿宇 . 数据加密技术在计算机网络通信安全中的应用 [J]. 石河子科技 , 2022, (04): 22-23.

[6] 常青 . 计算机网络通信安全中数据加密技术的应用 [J]. 数字技术与应用 , 2021, 39 (12): 237-239.

[7] 张令 . 计算机网络通信安全中数据加密技术的应用研究 [J]. 科技资讯 , 2021, 19 (33): 14-16.

[8] 候倍倍 . 计算机网络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, (09): 164-165.

[9] 吴文臣 , 郭伟伟 . 数据加密技术在计算机网络通信安全中的应用 [J]. 网络安全技术与应用 , 2021, (04): 22-24.

[10] 戴禄君 . 数据加密技术在计算机网络通信安全中的应用 [J]. 网络安全技术与应用 , 2021, (04): 24-25.

