数据加密技术在计算机网络信息安全中应用探讨

王在杏 王东风 李 智 王 哲 罗永会
保山市融媒体中心，云南 保山 678000

[摘要]随着信息技术的快速发展，计算机网络已成为现代社会信息交换的重要平台，其信息安全问题也日益受到关注。数据加密技术作为保护信息安全的有效手段，对其应用于计算机网络信息安全中的效果进行研究尤显重要。本研究首先介绍了计算机网络信息安全面临的主要威胁和数据加密技术的基本原理，然后通过对比分析不同数据加密算法（如对称加密、非对称加密和散列函数）在计算机网络中的应用情况和效果，最终选用了高级加密标准(AES)和安全散列算法(SHA)作为研究对象。实验结果显示，通过合理配置和使用这些加密技术，可以显著提高网络信息的保密性、完整性和可用性。此外，本研究也探讨了数据加密技术在实际应用中存在的挑战如密钥管理和性能问题，为信息安全领域的研究和实践提供了参考和启示。本研究的结果表明，数据加密是维护计算机网络信息安全的有效途径。

[关键词]数据加密技术；计算机网络信息安全；加密算法；密钥管理；信息保密性
DOI：10.33142/sca.v8i5.16434 中图分类号：TP3 文献标识码：A

Exploration on the Application of Data Encryption Technology in Computer Network Information Security

WANG Zaixing, WANG Dongfeng, LI Zhi, WANG Zhe, LUO Yonghui
Baoshan Integrated Media Center, Baoshan, Yunnan, 678000, China

Abstract: With the rapid development of information technology, computer networks have become an important platform for information exchange in modern society, and their information security issues have also received increasing attention. It is particularly important to study the effectiveness of data encryption technology as an effective means of protecting information security when applied to computer network information security. This study first introduces the main threats faced by computer network information security and the basic principles of data encryption technology. Then, by comparing and analyzing the application and effects of different data encryption algorithms (such as symmetric encryption, asymmetric encryption, and hash functions) in computer networks, the Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) are finally selected as the research objects. The experimental results show that by properly configuring and using these encryption techniques, the confidentiality, integrity, and availability of network information can be significantly improved. In addition, this study also explores the challenges of data encryption technology in practical applications, such as key management and performance issues, providing reference and inspiration for research and practice in the field of information security. The results of this study indicate that data encryption is an effective way to maintain computer network information security.

Keywords: data encryption technology; computer network information security; encryption algorithm; key management; confidentiality of information

引言

数字化时代，网络信息安全维护个人隐私和商业机密关键。网络技术进步，网络安全遭遇挑战增多，多种网络攻击手段涌现。数据加密技术确保信息安全有力手段之一，技术人员把信息变成不好破解的密文，阻止没权限的人获取和篡改。研究集中探讨数据加密技术帮助网络信息安全情况，研究人员考察技术面对网络威胁时候能不能起到作用，比较高级加密标准（AES）和安全散列算法（SHA）实际使用时候效果。技术进步很快，安全问题很突出，研究结果能帮助大家更好明白加密方法具体用处。研究还探讨了在数据加密技术应用过程中遇到的关键问题，如密钥管理和性能优化等，以提供更科学、有效的网络信息安全技术支持。总之，数据加密技术在提高网络信息的保密性、完整性和可用性方面发挥了关键作用，为构建可靠的网络环境提供了重要支撑。

1 计算机网络信息安全的挑战

1.1 计算机网络的发展和信息安全问题

信息技术快速发展，计算机网络很快成为全球信息交换中心平台[1]。网络技术发展促进社会经济兴盛发展，同时带来信息安全问题严重挑战。网络具有公开性无名性，信息传输过程会受到偷听、更改毁坏。网络空间存在多种威胁形式，包括病毒攻击、黑客入侵、恶意软件等等。威胁损害数据机密性、完好性可操作性，造成信息外泄、数据毁损业务停止。云计算、物联网大数据等新兴技术旺盛发展，信息安全挑战变得繁杂化，数据集中存储分发特点提高安全管理困难，迫切需要制定有效安全策略、使用技

术手段确保网络信息安全，维护系统稳定运行。数据加密技术作为目前保护信息安全的重要工具，是应对日益严重的信息安全问题的关键手段之一。

1.2 主要的信息安全威胁

如今的网络信息保护，面临着诸多挑战。恶性程序和有害应用，通过攻击那些存在缺陷的系统，将原本完整和可供使用的资料给破坏，并使得信息走漏。欺诈性网站和心理操控攻击，凭借着巧妙的伪装，获取了使用者的私密信息，最终危害到了个人和组织的机密安全。分布式拒绝服务攻击，造成了服务的瘫痪，进而严重影响着网络的正常运作。中间人攻击，以拦截与篡改通信数据，为攻击者的隐秘盗取行为提供了可能。而不容忽视的内部风险，来自于内部员工可能利用其有限的权利，窃取或篡改重要数据。加强信息安全手段和技术的必要性更显出其重要。

1.3 现有的信息安全手段和方法

现在信息安全手段和具体方法种类丰富，目标是维护计算机网络信息保密性、完整性和可用性。防火墙是网络安全第一道防线，功能是拦截未经授权访问，保障网络安全[2]。入侵检测系统（IDS）任务是监视网络流量，目的是辨别潜在威胁和可疑活动。访问控制机制作用是确保经过授权用户才能访问敏感信息，效果是降低内部风险。加密技术属于关键手段，做法是将数据转换为密文，目的是避免信息传输过程被窃取或篡改。多种安全手段结合使用，效果是建立完善多层次防御体系。

2 数据加密技术的原理与分类

2.1 数据加密的基本原理

数据加密技术基本原理依靠信息理论，数学算法完成数据转换，达到保护信息秘密和保持信息完整具体目标。加密过程包含原始明文数据编码，转变成无法阅读密文，只有使用特定解密钥匙才能让数据变回原来样子。这个过程安全性依靠密钥安全管理和算法复杂程度保证。任何数据加密技术需要拥有混淆和扩散两个基本特点，也就是说密文不能让简单分析方法猜出原来内容，密文发生微小变化会导致输出结果出现很大不同。不同类型加密技术分别达到不同程度安全性和计算效率平衡，对称加密技术主要使用一个密钥完成数据加密和解密操作；非对称加密使用公钥和私钥一对钥匙完成加密和解密；散列函数使用固定输出长度验证数据完整性是否可靠。这些加密技术的有效结合能够在计算机网络信息安全中发挥关键作用。

2.2 数据加密的主要类型

数据加密技术关键涵盖称加密、非称加密、散列函数三大类型。称加密技术采用单一密钥执行加密解密工作，速度快，实现过程较为简单，优势明显，密钥管理繁琐麻烦。常见算法涵盖 DES、AES 两种类型。非称加密技术运用一对公私密钥，公钥负责加密，私钥负责解密，安全性较强，速度慢，计算复杂度高，常用 RSA、ECC 算法两种类型。散列函数技术不涉及解密操作，输入数据转变固定长度散列值，校验数据完整性是否可靠，常见 SHA、MD5 两种类型。各类加密技术实际应用中依据需求选择配合，达成数据可靠传输存储目标。

2.3 目前主流的数据加密算法

现在数据加密算法包含对称加密算法、非对称加密算法和散列函数。对称加密这种方法，算法有高级加密标准，名字叫 AES。这种算法运行速度快，保护数据能力很强，很多人使用。非对称加密算法这种方法，运用公钥和私钥两种密钥组成机制，完成信息加密和身份验证工作。比如安全散列算法，简称 SHA，属于一系列算法，能产生只有一种结果的固定长度散列值，帮助检查数据有没有被改动。这些算法帮助计算机网络信息安全，起到非常重要的作用。

3 数据加密技术在计算机网络信息安全中的应用

3.1 数据加密技术在信息保密性方面的作用

数据加密技术信息保密性方面拥有重要作用。计算机网络信息交换过程，信息保密性保证未经许可获取首要任务。对称加密和非对称加密两种主要加密方法，明文数据转换为密文，保证信息传输过程被偷取或更改。对称加密 AES 给予加密，适合大量数据加密需求，非对称加密 RSA 靠公钥和私钥机制，适合密钥交换和数字签名场景。使用加密算法，信息内容掩盖复杂数学算法，未经许可用户解开密文，守护信息机密性。技术操作简单效果好，安全级别高，应用范围广。散列函数如 SHA 用于生成数据的唯一“指纹”，进一步增强了信息传输的安全性，确保数据未被篡改。总体而言，数据加密技术通过多层次的加密机制，为计算机网络中的信息保密性提供了坚实的保障。

3.2 数据加密技术在数据完整性保护上的应用

数据加密技术保护数据完整性方面起到关键作用，保证网络传输信息发送接收过程不被篡改或破坏。加密手段让数据产生唯一校验值，任何微小更改都会引起校验值显著变化，这样就能给予验证数据完整性具体方法。常用散列算法，比如 SHA 系列，被广泛使用到数字签名、数据完整性验证还有身份验证这些场景。这些算法能够有效检查并且阻止数据传输存储过程遭受恶意修改。加密技术加上数字签名使用，可以进一步提高信息真实性完整性，计算机网络信息安全也能因此得到重要技术支持保障。

3.3 数据加密技术在保障信息可用性上的贡献

数据加密技术能维护信息随时可用，发挥很关键的作用。网络系统信息遇到攻击后能被修复，确保数据随时可用。加密机制给出数据备份和处理计划，信息丢了或者系统出问题的时候，任何人都能拿到并修复重要信息。数据加密保证数据传递和储存时完好无损而且真实可信，防止坏人故意改动或者破坏造成信息用不了的情况发生，网络系统被攻击还能继续运行，保持业务不中断并且稳定，技术效果非常明显。

4 高级加密标准(AES)和安全散列算法(SHA)的具体应用

4.1 AES 和 SHA 的原理和特性

高级加密标准（AES）和安全散列算法（SHA）现代信息安全拥有重要位置。高级加密标准一种对称加密算法，

设计依靠替代和置换网格结构，多轮加密操作给予强大安全性和效率[4]。高级加密标准计算效率高、使用范围宽等特点，数据加密给予牢固保证。加密过程，高级加密标准能够使用不同长度密钥，比如 128 位、192 位和 256 位，不同安全需求给予多样选择。安全散列算法数据完整性验证散列函数，产生固定长度散列值。SHA256 是其常用变种，具有较强的抗碰撞能力和抗预映射攻击性能。SHA 通过确保信息在传输和存储过程中的完整性，对网络通信提供有效保护。两者结合应用时，AES 负责信息加密以保障保密性，而 SHA 则负责验证数据完整性，两者的协同作用显著提升了计算机网络信息的安全水平。

4.2 AES 和 SHA 在实际网络环境中的应用效果

AES 和 SHA 实际网络环境应用展现维护信息安全效果。AES 对称加密高效特点和卓越抗攻击能力，普遍使用无线网络通信加密协议，比如 WPA2，保证数据传输机密性。SHA 系列算法作为散列函数，数字签名和证书给予数据完整性验证，生成固定长度哈希值检查数据传输有没有被篡改。实际应用，AES 和 SHA 资源受限环境表现好，能提高计算机网络信息安全，增强系统稳定性。需要留心，使用时候全面思考密钥长度和算法复杂度，防止性能降低，确保运行顺畅。

4.3 AES 和 SHA 的限制和问题

高级加密标准（AES）和安全散列算法（SHA）计算机网络信息安全中起到关键作用，但技术也遭遇一些约束和问题。AES 安全性很多人普遍承认，但密钥管理是一个难题，大规模分布式系统中，密钥管理出错引发安全性减弱。AES 加密速度让系统性能出现压力，资源受限环境下运行效率下降明显。SHA 算法保证数据完整性表现很优秀，应对进步量子计算技术时，安全性会受到风险。对抗性攻击和算法本身脆弱性也是需要长期注意问题，技术人员必须采取措施改进这些不足。

5 数据加密技术实际应用中的挑战和展望

5.1 密钥管理在数据加密中的角色和挑战

在数据加密技术的实际应用中，密钥管理是确保加密系统安全性的核心要素[5]。密钥是数据加密和解密过程中的关键组件，其管理的有效性直接影响系统的整体保密性和完整性。密钥管理面临诸多挑战。密钥的生成、分发、存储和更新都需要安全可靠的机制，以防止未授权访问和潜在的安全漏洞。密钥的生命周期管理需要解决密钥过期和替换的问题，以确保系统持续的安全性。这要求开发复杂的策略和工具来管理和监控密钥使用情况。密钥管理还因需兼顾性能和安全性而更加复杂，因为复杂的密钥管理系统可能影响系统的性能。密钥管理在数据加密中扮演着至关重要的角色，需要深入研究以在安全性和可用性之间找到平衡点，为计算机网络信息安全提供坚实的保障。

5.2 数据加密在提升网络信息安全性中的性能问题

数据加密技术在提升网络信息安全性中面临性能问题，主要体现在加密和解密过程的计算开销上。复杂的加密算法尽管能提供更高的安全性，但也会对系统资源产生显著消耗，导致数据处理效率降低，增加网络延迟。在高流量和实时数据传输的环境下，这一问题尤为突出。加密技术与现有网络架构和应用的整合也可能引发兼容性问题，增加部署和维护的复杂性。为平衡安全性与性能，需优化加密算法的效率，探索轻量级加密方案，并提升硬件加速能力。性能提升的要确保安全强度不被削弱，保障网络信息的安全性与可用性。

5.3 数据加密技术的未来发展和应用前景

数据加密技术的未来发展和应用前景展现出广阔的空间。随着量子计算技术的发展，传统加密方法面临挑战，量子密码学可能提供新的解决方案，以确保信息安全。机器学习与人工智能的结合也为动态加密提供了更多可能性，通过智能检测和预测威胁，实现更高级别的安全防护。随着物联网的普及，小型设备对轻量级加密技术的需求将持续增长，提高加密效率和适应复杂网络环境将是未来发展的关键。全球对于更加安全的数据交换机制的需求，必将推动数据加密技术的不断革新与突破。

6 结束语

本研究对数据加密技术在计算机网络信息安全中的应用进行了深入探讨，首先概述了计算机网络信息安全面临的各种威胁以及数据加密技术的核心原理。通过实证分析比较了多种加密算法（包括对称加密、非对称加密和散列函数）在保护网络信息安全中的具体效果，并将高级加密标准（AES）与安全散列算法（SHA）作为主要研究对象。研究证明，在恰当的配置与使用下，这些加密技术大幅增强了网络信息的保密性、完整性和可用性。尽管取得了一定的研究成果，但数据加密技术在实际应用中仍存在诸多挑战，如密钥管理的复杂性和加密过程中的性能优化问题。后续研究可考虑深入探讨密钥生成与管理的自动化方案，以及探索更为高效的加密算法，以进一步提升加密技术在网络信息安全中的实用性和效率。此外，随着量子计算等新兴技术的发展，未来也需关注这些技术可能对现有加密算法构成的威胁，并提前研究相应的防护措施。本研究的发现和讨论为计算机网络信息安全提供了理论支持与实践指导，希望能为信息安全领域的学者和实践者带来启发和帮助。

[参考文献]

[1]杨凯.计算机网络信息安全中数据加密技术应用[J].IT 经理世界,2020,23(8):92-92.
[2]土可心.计算机网络信息安全中数据加密技术[J].网络安全技术与应用,2022(1):22-23.
[3]伍岳.探讨计算机网络信息安全中数据加密技术[J].电子世界,2020(21):151-152.
[4]高铭泽.试论计算机网络信息安全中数据加密技术[J].计算机产品与流通,2020(5):53-53.
[5]王晓明,秦聪,冯伟.计算机网络信息安全中数据加密技术分析[J].科学与信息化,2022(16):77-79.

作者简介：王在杏（1990—），女，汉族，云南保山人，本科学历，研究方向为广播电视技术维护。