计算机网络工程中的数据加密与信息保护方法

谭 杰

（广西农业职业技术大学 南宁 530007）

摘 要 为保障计算机网络工程的数据安全，文中分析了数据加密与多种信息保护方法，包括加密算法、密钥管理、数字签名、节点数据加密等，探讨了身份认证、防火墙、入侵检测、人工智能防护等信息保护方法。研究结果表明，这些方法可以有效提高数据的安全性和系统的防御能力，以期为计算机网络工程提供有价值的参考。

关键词： 计算机网络工程；数据加密；信息保护方法

中图分类号 TP309.2

Data Encryption and Information Protection Methods in Computer Network Engineering

TAN Jie

（Guangxi Agricultural Vocational and Technical University，Nanning 530007，China）

Abstract In order to ensure the data security of computer network engineering, this paper discusses data encryption and various information protection methods, including encryption algorithm, key management, digital signature, node data encryption, etc., and discusses information protection methods such as identity authentication, firewall, intrusion detection, and artificial intelligence protection. The research results show that these methods can effectively improve the security of data and the defense ability of the system, in order to provide valuable reference for computer network engineering.

Key words Computer network engineering，Data encryption，Information protection method

0 引言

在信息化社会，数据泄露、黑客攻击等问题频发，给个人隐私和企业数据安全带来了巨大的威胁。计算机网络系统因其复杂性和开放性，面临着多种潜在的安全风险。因此，深入研究数据加密与信息保护方法，以应对日益严峻的安全挑战，保障数据的机密性、完整性和可用性，成为计算机网络工程领域亟待解决的问题。

1 数据加密技术在计算机网络信息安全中的应用

1.1 加密算法的选择

在选择加密算法时，需要考虑算法的安全性、效率以及适应不同应用场景的能力。对于企业级数据，可以选择AES算法，以利用其强大的加密能力和广泛的应用支持。AES算法在多个密级（128、192、256位）都能提供灵活的选项，其中256位提供了最高级别的安全保护，适用于需要极高的安全性的应用环境。对于需要进行实时数据传输的应用，如视频传输或在线通信，选择加密算法时则需要考虑算法的处理速度和延迟。在该场景下，Chacha20算法因其高效的性能和较低的处理需求，成为实时数据传输的理想选择。在物联网（IoT）设备中，由于设备的处理能力和存储空间有限，需要选择轻量级的加密算法，如Speck算法（专为资源受限的环境设计），以便在保持适度安全性的同时降低算法对资源需求[1]。

1.2 强化密钥管理

（1）应确保密钥具有高度随机性，以抵抗猜测和密码分析攻击。一种标准的做法是使用强随机数生成器（RNG）产生密钥，建议使用符合国家或国际标准（如NIST SP 800-90A）的认证RNG。生成的密钥应具有足够的长度和复杂性，避免密钥在存储或传输过程中被泄露。（2）加密密钥应存储在硬件安全模块（HSM）中。HSM可以提供物理和逻辑保护，防止未授权访问。对于软件解决方案，可使用加密的密钥库和访问控制机制，只有授权的应用和用户可以访问密钥。（3）在密钥分发过程中，必须确保密钥的安全性。使用公钥基础设施（PKI）进行密钥分发，可以安全地分发密钥，因为PKI系统中的公钥可以公开，私钥则保持私有。需要传输的密钥应通过安全通道，如TLS/SSL加密连接，以防止中间人攻击。（4）密钥使用应严格遵守安全策略，避免密钥过度使用或在不安全的环境中使用。对密钥使用进行日志记录，以监控密钥的使用情况，从而及时发现非授权使用或其他异常活动。（5）应确保不再需要的密钥从所有系统中彻底删除，防止可能的滥用行为。物理介质存储的密钥应通过物理方式销毁，如粉碎或燃烧；软件中存储的密钥应使

作者简介：谭杰（1982—），硕士，研究方向为计算机工程。

用专门的软件工具彻底清除。

1.3 提升数字签名的可信度

数字签名利用非对称加密技术，使得数据即便在传输过程中被拦截，也无法被篡改，同时确认数据来源的可靠性。(1)提升数字签名可信度的首要步骤是使用强大的哈希函数和高安全级别的加密算法。哈希函数如SHA-256或SHA-3能生成独特的、固定长度的哈希值，几乎不可能从哈希值反推原始数据，即使是微小的数据变化也会导致哈希值产生较大的差异[2]。(2)数字签名的可信度还依赖于证书管理和证书颁发机构(CA)的可靠性。证书确保了公钥的真实性，是保证数字签名可信度的关键。其中，选择受信任的CA和使用有效的证书吊销列表(CRL)或在线证书状态协议(OCSP)来验证证书状态。(3)随着计算能力的提高和新型攻击手段的出现，还需要及时更新传统的哈希函数和加密算法，以适应新的安全需求。

1.4 节点数据加密

在现代计算机网络中，数据通常在多个网络节点之间传输，包括服务器、路由器以及终端用户设备。每个节点都可能成为攻击的目标。数据在节点间传输时，加密算法需要具备高效性和安全性，确保数据即使在传输过程中被截获，也无法被未授权的第三方解读，同时节点数据加密还要求算法能在各种硬件和软件环境中稳定运行，不因系统差异而影响加密效果。在实际应用中，采用分组密码技术对数据块进行处理也是一种常见的方法，其能将数据分成固定大小的块，然后对每个块进行独立加密，使得数据处理过程可以并行化，从而提高加密和解密的速度。如常用的分组长度是128位，既可以保证加密的安全性，又不会过多地延长处理时间。为增强加密算法的安全性，还可以采用密钥扩展技术，基于一个较短的密钥生成一个较长的密钥序列，实现多轮加密。

1.5 强化网络安全系统的功能设计

(1)网络安全系统功能的强化应从整合最新的加密技术开始，确保所有的数据传输行为都通过高安全标准的加密协议进行。例如，使用TLS 1.3协议为网络通信提供端到端的加密，以减少数据传输的握手次数，提高连接的安全性和效率。TLS 1.3还能使用更安全的加密算法并简化握手过程，有效提升数据的安全性。(2)使用实时的监控和入侵检测系统(IDS)，以识别和响应安全威胁。高级入侵检测技术，如基于行为的检测，能分析网络流量中的异常模式，及早发现潜在的安全问题。IDS系统应配置自动响应功能，如在检测到攻击迹象时自动隔离受影响的部分，阻止攻击者的进一步操作。(3)应用全面的身份验证和访问控制机制[3]。多因素认证(MFA)技术被广泛应用于敏感的网络访问点，确保只有授权用户才能访问重要的网络资源。MFA可以要求用户提供多种身份证明，如密码、生物识别信息或手机应用生成的一次性代码，大幅增强了认证过程的安全性。(4)数据泄露防护。使用数据丢失防护(DLP)技术，可以防止敏感信息无意或恶意地泄露。DLP系统可以对数据进行分类和标记，并设置数据传输策略，从而控制特定信息的存储和传输，保证数据的保密性和完整性。

2 计算机网络工程中信息保护方法的应用

2.1 基于密码技术的防护策略

密码技术主要包括对称加密技术和非对称加密技术两种。对称加密技术使用单一密钥进行数据加密和解密，加解密速度快，适合于大规模数据处理。常见的对称加密算法包括AES(高级加密标准)和DES(数据加密标准)。AES支持128、192和256位的密钥长度，可以提供强大的安全保障，已成为全球标准。例如，AES-256密钥极难被破解，即使使用强大的计算资源，也需要巨大的时间成本来尝试可能的密钥组合。非对称加密技术使用一对密钥，即公钥和私钥，其中公钥用于加密数据，私钥用于解密数据。RSA是一种应用广泛的非对称加密算法，支持的密钥长度为1 024~4 096位，且密钥长度越长，安全性越高。RSA算法依靠两个大素数的乘积，使得其难以被破解[4]。

在实际应用中，可以结合对称加密技术和非对称加密技术，以达到最佳的安全效果。在典型的使用场景中，非对称加密用于安全地交换对称加密的密钥，之后使用对称加密进行数据传输。这种组合利用了非对称加密在密钥交换安全性方面的优势和对称加密在数据处理效率上的优势。

2.2 基于身份认证技术的防护策略

在计算机网络工程中，基于身份认证的防护策略是确保信息安全的关键手段。访问控制技术和生物识别技术是实现身份验证的主要方法，可以确保只有授权用户才能访问敏感数据和系统资源。

(1)访问控制技术利用访问控制列表(ACLs)和角色基础访问控制(RBAC)来定义用户可以访问网络中的哪些资源。ACLs通过匹配用户身份与一个列表(其中详细定义了允许或拒绝的权限)来控制单个用户或用户组对文件系统、网络服务和应用程序的访问。RBAC进一步通过将权限分配给特定的角色，而不是直接分配给单个用户来简化管理过程。这种方法既减少了配置错误的风险，还增强了安全性，因为管理者可以轻松调整角色的权限，而无需修改每个用户的设置。(2)生物识别技术使用人的生理或行为特征来进行身份验证。常见的生物识别技术包括指纹扫描、面部识别、虹膜扫描和声音识别等，其可利用个体独特的生物特征进行快速和准确的用户身份验证。例如，面部识别技术能达到99.8%的准确率，而指纹识别的错误接受率通常低于0.01%。在具体应用中，生物识别系统会存储一个或多个生物特征的数字表示，当用户试图访问系统时，其会将实时捕捉到的生物特征与存储数据进行比对，从而确认用户身份。

2.3 基于网络安全设备的防护策略

防火墙技术负责筛选进出网络的数据包，阻止未授权访问，并过滤掉可能携带恶意软件的通信。网络管理员会配置一套复杂的规则，根据企业的安全需求来定义哪些服务（如HTTP，FTP）可以从外部访问。防火墙还能对内部网络进行分区，划分不同的区域，并对敏感的数据区域实施额外的保护。现代的防火墙技术还具备应用层过滤功能，能检查数据包的具体内容，进一步提高过滤的精确度。

入侵检测与防范技术可以监测和分析网络流量，以识别和响应潜在的恶意活动。入侵检测系统（IDS）可以不间断地分析网络中的行为模式，使用各种检测算法（如签名检测和异常检测）来辨识异常行为（这些行为可能表明存在安全威胁）。例如，IDS能识别潜在的DDoS攻击或网络扫描活动，并立即向管理员发出警报。入侵防范系统（IPS）可以在IDS的基础上检测入侵尝试，以主动介入并阻止这些攻击。其通常被部署在网络的关键入口点，以自动阻断识别为恶意流量的数据包，断开非法的连接，甚至自动调整网络配置以隔离攻击源。IPS的自动响应机制可以在降低人工干预需求的同时，加快防御反应速度[5]。

2.4 基于人工智能的计算机信息安全防护策略

在人工智能（AI）技术的助力下，计算机网络工程中的信息保护方法也在不断发展。在开发阶段，AI通过分析历史数据来识别代码中的常见漏洞并提供改进建议，帮助开发者修补潜在的安全隐患。例如，使用AI驱动的静态代码分析工具，可以自动检测并修复安全漏洞，减少因人为错误而导致的安全问题。在AI的支持下，Agent技术能在没有人工干预的情况下执行特定的任务。在网络安全领域，智能Agent能根据网络环境的变化自动调整安全策略，如实时更新防火墙规则或自动隔离受感染的系统，有效降低攻击的影响。此外，人工智能与VPN（虚拟私人网络）的结合，显著提升了计算机信息的安全性。AI可以分析VPN流量，识别出异常模式，帮助用户及时发现潜在的入侵企图。同时，结合AI的VPN能更智能地管理数据流，提高网络性能，同时保障数据传输的安全性和私密性。

3 结语

本文探讨了计算机网络工程中的数据加密与信息保护方法，通过分析加密算法的选择、密钥管理、数字签名、节点数据加密以及网络安全系统设计的强化措施，结合基于密码技术、身份认证技术、网络安全设备和人工智能的多种防护策略，构建了全面的信息安全防护体系。未来，随着技术的不断进步和攻击手段的日益复杂，计算机网络工程中的信息安全保护将面临更多的挑战，需要持续创新，加强技术研发与应用，以更好地保障数据的机密性、完整性和可用性。

参考文献

[1] 吕敬兰.数据加密技术在计算机网络信息安全中的应用[J].科技创新与应用，2024，14(18)：185-188.

[2] 何颖.计算机工程与网络中的数据加密与信息保护技术分析[J].电子技术，2024，53(4)：388-389.

[3] 潘能汝.大数据技术在生态数据信息保护中的作用[J].大数据时代，2024(3)：22-26.

[4] 玛丽亚木·艾斯凯尔.论智能网联汽车终端用户个人信息的保护困境及其出路[J].克拉玛依学刊，2024，14(2)：68-76.

[5] 刘杨.数据加密技术在网络安全传输中的应用[J].网络空间安全，2023，14(3)：41-44.