DOI:10.19981/j.CN23-1581/G3.2024.18.043

数据加密技术在计算机网络信息安全中的应用

吕敬兰
(贵州农业职业学院,贵阳 551403)

摘 要:随着互联网的快速发展和普及,网络安全问题日益凸显。数据加密技术作为保障网络安全的重要手段之一,在现代社会发挥着不可替代的作用。该文从数据加密技术的基本原理入手,分析其在计算机网络信息安全领域的应用现状,探讨不同类型的加密技术的优缺点,并展望其未来发展趋势。通过研究,旨在为计算机网络安全管理提供借鉴,实现数据加密技术优化升级。

关键词:计算机网络;信息安全;数据加密;隐私保护;云计算

中图分类号:TP393.08 文献标志码:A 文章编号:2095-2945(2024)18-0185-04

Abstract: With the rapid development and popularization of the Internet, the problem of network security has become increasingly prominent. As one of the important means to ensure network security, data encryption technology plays an irreplaceable role in modern society. This paper starts with the basic principle of data encryption technology, analyzes its application in the field of computer network information security, discusses the advantages and disadvantages of different types of encryption technology, and looks forward to its future development trend. Through the research, the purpose of this paper is to provide reference for computer network security management and realize the optimization and upgrading of data encryption technology.

Keywords: computer network; information security; data encryption; privacy protection; cloud computing

随着计算机技术的持续发展,网络体系的服务范围日渐广泛,其所具备的服务能力也得到大规模提升,从而满足人民群众日益增长的物质和精神需求。在计算机网络快速发展的时代背景下,网络信息安全问题更加凸显,在计算机网络信息安全决策中整合数据加密技术,可为人们提供良好的网络环境,实现数据管理水平优化升级[1]。

1 数据加密技术概述

1.1 数据加密技术的基本概念

数据加密技术是保障信息安全的重要手段之一,可加密处理传输和存储数据,使未经授权的人员无法获取和利用数据。具体来说,数据加密技术通过加密算法和密钥,将明文(未加密的数据)转换为密文(加密后的数据),只有掌握正确密钥的人员才能将密文还原为明文,从而实现对数据的保密。

根据加密算法和密钥的不同,数据加密技术分为对称加密、非对称加密和不可逆加密3种类型。对称加密是指加密和解密使用同一把密钥,这种加密方式加解密速度快,适合大量数据的加密,但是密钥的管理和分发比较困难;非对称加密则使用2把不同的密钥进行加密和解密,其中一把是公开的,另一把是保密的,其安全性高,但是加解密速度较慢;不可逆加密则是指加密过程不可逆,即无法从密文反推出明文,这种加密方式常用于密码存储等场景。加密模型如图1所示。

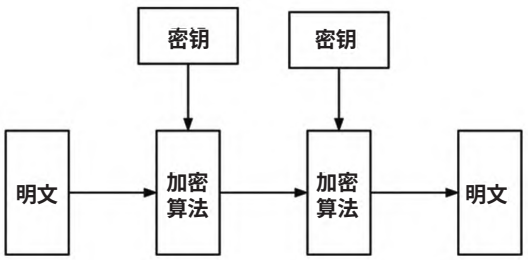

图1 加密模型

在实际应用中,数据库加密是一种常见的保护手段。数据库是信息系统中存储数据的重要场所,一旦数据库被攻击或泄露,会导致严重的后果。数据库加密技术加密处理数据库中的数据,即使数据库被非法访问或泄露,攻击者也无法获取和利用其中的数据。同时,

作者简介:吕敬兰(1978-),女,硕士,讲师。研究方向为计算机。

对于网络传输中的数据，也可采用链路层加密、节点加密和端对端加密等方式进行保护，提高数据在传输过程中的安全性[2]。

除了硬件实现的数据加密外，软件实现的数据加密也是一种常见的方式。AES、DES、RSA 等软件加密算法灵活地应用于各种场景和设备中，安装相应的软件或应用程序即可实现对数据的加密处理。数据加密技术在实际应用中需要考虑加密算法的选择、密钥的管理和分发、加密性能和安全性的平衡等多方面因素，在实际应用中需根据具体需求和场景选择合适的加密技术和方案。

1.2 数据加密技术的发展历程

在 1949 年以前，早期的数据加密技术相对简单，复杂程度不高，安全性也较低。这个时期的密码大多具有艺术特征，类似于字谜，因此被称为古典密码。随着工业革命的到来和二次世界大战的爆发，数据加密技术得到突破性进展，开始通过密码算法或者机械的加密设备，将明文转变为密文，提高通信的安全性。

在 1949 年至 1975 年期间，随着世界上第一台计算机的诞生及计算机技术的迅猛发展，加密技术也从机械时代提升到了电子时代。这个时期的加密技术能够进行复杂的数学计算，从而使加密算法在复杂程度和安全性上都得到了很大的提高。

自 1976 年至今，现代密码学经历了重大变革。美国密码学专家狄匪和赫尔曼在 1976 年提出公开密钥密码体制的概念，是现代密码学的重大发明，也为密码学的发展提供了新的方向。在公开密钥密码体制中，加密和解密使用不同的密钥，在保证信息安全的同时，也极大地提高加密和解密的效率。

2 数据加密技术在计算机网络信息安全中的应用

2.1 传输层加密：SSL/TLS 协议

SSL（安全套接字层）记录协议在网络安全传输中起着核心作用，负责将数据进行适当的格式化、加密、压缩等操作，以凸显数据在传输过程中的机密性、完整性和可靠性。考虑到网络传输的效率和安全性，SSL 将上层协议传递下来的数据进行分块处理，每个数据块的大小不得超过 214 字节，促使数据在网络中顺畅传输，避免因数据包过大而导致传输失败。在数据分块之后，SSL 记录协议（图 2）压缩处理每个数据块，保证在不损失任何原始数据信息的前提下进行，优化传输效率并减少带宽占用。对压缩后的数据应用散列算法生成计算和添加消息认证码（MAC），然后将 MAC 附加到压缩后的数据块之后，用于在接收端验证数据的完整性和真实性。对称加密采用相同的密钥进行加密和解密，具有加密效率高、速度快的特点，适合用于大量数据的加密传输[3]。

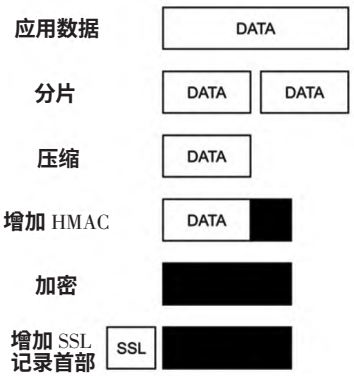

图 2 SSL 记录协议

当 SSL 记录协议接收到一个要传送的应用消息时，首先进行分段处理，每个上层消息会被分成若干个较小的段，每个段小于或等于 214 字节（即 16 384 字节）。这种分段机制确保了数据在网络中的有效传输，同时避免因数据包过大而可能导致的传输问题。接下来，这些分段后的数据可选择进行压缩，压缩必须采用无损压缩方法，提高数据完整性。压缩后的数据增加的长度不能超过 1 024 个字节，以维持数据包的合理大小。

在对数据进行压缩后，SSL 记录协议会计算每个压缩数据的消息认证码（MAC）。在 TLS 中，使用的是 RFC2104 中定义的 HMAC 算法进行 MAC 的计算。MAC 的添加确保了数据的完整性和真实性，使接收端能够验证接收到的数据是否在传输过程中被篡改。压缩后的消息和 MAC 会使用对称加密方法进行加密，注重加密和解密过程的高效性。TLS 使用 RFC2104 中的定义 HMAC 算法，其关系表达式如下

$$HMAC_k(x)=h[k^+\otimes opad\backslash\backslash h[k^+\otimes ipad]], \quad (1)$$

式中：x 表示 HMAC 消息输入，h 表示嵌入的散列函数，k^+表示左边填充 0 的密钥，长度与散列码中的块长度保持相同。$opad$ 是 01 011 100 重复的结果，$ipad$ 是 00 110 110 重复的结果。

此外，加密对内容的增加长度不能超过 1 024 字节，保证整个数据包的长度不会超过 2^{14}+2 048 字节。

SSL 记录协议为加密后的数据添加一个 SSL 头部，包含内容类型、主版本号、从版本号及压缩长度等多个重要字段，其中内容类型字段指明了封装段使用的高层协议、主版本号和从版本号则表明了 TLS 使用的版本、压缩长度字段则指示了明文段（或压缩段，如果使用了压缩）的字节长度。

2.2 网络层加密：IPSec 协议

在 IPSec 协议族中，2 个核心协议是 AH（Authentication Header）和 ESP（Encapsulation Security Payload）。AH 协议提供数据源认证和数据完整性保护，但不提供加密服务，以验证数据的来源和完整性，但无法保密数据内容。而 ESP 协议则更为全面，提供数据源认证和数据完整性保护，还可实现数据的加密和抗重播功能。在实际应用中，IPSec 协议通过在网络层对数据包进行加密和认证，为上层应用程序提供透明的安全性。即使上层应用程序本身没有实现安全性，也可以从网络层的安全性中受益，使 IPSec 在虚拟专用网络（VPN）等领域得到了广泛应用，打消人们对其安全性的顾虑[4]。

2.3 应用层加密：PGP 加密软件

应用层加密是保障网络通信安全的重要手段之一，其中 PGP（Pretty Good Privacy）加密软件是备受推崇的一种解决方案。PGP 软件采用先进的加密算法和密钥管理机制，为用户提供了高度安全的数据加密和通信保护。PGP 加密软件基于公钥和私钥的加密体系，每个用户都拥有一对唯一的公钥和私钥。公钥用于加密数据，而私钥则用于解密数据，确保了只有私钥的持有者才能解密由相应公钥加密的信息，从而保证了数据的机密性和安全性。PGP 软件支持多种加密算法，包括 RSA、AES 等，用户根据需要选择合适的算法和密钥长度。同时，PGP 还提供了数字签名和时间戳等功能，用于验证数据的完整性和真实性，防止数据在传输过程中被篡改或伪造。PGP 加密软件的应用范围非常广泛，用于电子邮件、文件传输、即时通信等多种应用场景。在数据信息传输领域，PGP 实现端到端加密，在传输数据信息过程中不被窃取或篡改。

2.4 数据库加密技术

在数据库加密技术中，通常使用加密算法和密钥加密和解密数据。加密算法是一种将明文数据转换为密文数据的数学函数，而密钥则是用于控制加密算法的参数。通过选择合适的加密算法和密钥管理策略，实现对数据库中数据的强加密保护。数据库加密技术分为透明加密和非透明加密 2 种主要类型，透明加密是指在应用程序和数据库之间自动进行加解密操作，对应用程序来说无需进行任何修改，而非透明加密则需要应用程序在读写数据时进行显式的加解密操作。假设 E 表示加密算法，D 表示解密算法，K 表示密钥，P 表示明文数据，C 表示密文数据，则加密过程可以表示为

$$C=E(K,P), \tag{2}$$

解密过程可以表示为

$$P=D(K,C), \tag{3}$$

式中：E 和 D 是预先定义好的加密和解密函数，K 是密钥，P 是明文数据，C 是密文数据。通过选择合适的 E、D 和 K，安全保护数据库数据。

2.5 云计算中的数据加密技术

数据加密技术为数据安全问题提供了有效的解决方案，通过编码和转换数据，使得只有持有密钥的授权人员能够解密并获取数据，从而强化数据的机密性和完整性。在云计算环境中，加密技术被广泛应用在数据传输、存储和处理等各个环节。

在数据传输过程中，采用如 SSL/TLS 等协议进行加密，维护数据在网络中的安全传输，防止中间人攻击和数据泄露。对于存储在云端的数据，存储加密技术能够保障即使云端存储系统被攻破，攻击者也无法直接获取明文数据。同时，密钥管理也是数据加密技术中的重要环节，基于建立完善的密钥管理体系和使用专用硬件设备，进一步降低密钥泄露的风险。同态加密技术则允许在不解密的情况处理和计算加密数据，这一特性使其在云计算中具有巨大的应用潜力，在保证数据机密性的同时，实现数据的灵活利用和共享[5]。

3 数据加密技术的挑战与未来发展

3.1 量子计算对传统加密技术的挑战

量子计算基于量子力学原理，利用量子比特的叠加态和纠缠态进行信息处理，具有在某些特定问题上指数级的加速能力，其强大的计算能力对传统加密技术形成巨大威胁，尤其是在公钥密码体系方面。公钥密码体系，作为现代网络安全的基础，广泛应用于各种安全协议和数字签名中。然而，量子计算机的出现使其变得不堪一击，例如通过 Shor 算法在多项式时间内分解

大质数，从而破解 RSA 等公钥密码体系。

除了对公钥密码体系的威胁，量子计算还对对称密码体系构成了挑战。对称密码体系依赖于密钥的保密性，虽然量子计算机在直接破解对称密码方面没有优势，但通过暴力搜索等方法加速密钥破解过程。此外，随着量子计算机的发展，现有的一些加密算法会变得不再安全，需要不断更新和升级以适应新的安全需求。

为了应对量子计算的挑战，发展后量子密码学是一项重要措施。后量子密码学旨在设计能够抵抗量子计算机攻击的加密算法，这些算法基于复杂的数学问题和量子物理原理，使得即使是强大的量子计算机也难以破解。再者，采用更长的密钥长度、定期更换密钥以及使用安全的密钥交换协议等措施可以降低密钥泄露的风险。融合应用多种加密技术，提高网络信息安全的整体防护能力。例如，结合公钥密码体系和对称密码体系的优势，使用公钥密码展开密钥协商和身份认证，然后使用对称密码进行数据传输和存储加密。

3.2 同态加密与后量子密码学的发展

随着信息技术的飞速发展，数据安全和隐私保护问题日益凸显，使密码学技术成为了研究热点。其中，同态加密与后量子密码学作为新兴的密码学技术，在保障数据安全和隐私方面发挥着越来越重要的作用。同态加密是一种特殊的加密方式，允许对加密后的数据进行计算，得到的结果仍然是加密的，但与原始数据直接计算的结果相对应，为云计算和大数据处理提供了广阔的应用前景。

后量子密码学则旨在设计能够抵抗量子计算机攻击的加密算法，基于复杂的数学问题和量子物理原理，强调数据安全性。目前，同态加密技术已经取得重要突破并在实际应用中展现出效率和可行性，但仍面临计算复杂度高和难以实现大规模应用的挑战。而后量子密码学领域也已涌现出多种候选算法，并在理论安全性和实用性方面表现出较好性能。

展望未来，随着技术的不断进步和应用需求的增长，同态加密与后量子密码学有望取得更显著的突破和发展。为推动其进一步发展，必须加强基础理论研究、提高技术应用水平、加强国际合作与交流以及培养专业人才队伍。通过各种努力，同态加密与后量子密码学将能够在保障数据安全和隐私方面发挥更大作用，共同构建一个更加安全的网络信息环境。

3.3 数据加密与隐私保护的平衡

数据加密是信息安全领域的一项关键技术，通过对数据进行加密处理，突显数据在传输和存储过程中的机密性和完整性。数据加密技术多种多样，包括对称加密、非对称加密、混合加密等，每种加密方式都有其独特的优点和适用场景。

数据加密技术的广泛应用提供了强大的数据安全保障，例如在在线银行交易中，数据加密保证用户的账户信息和交易数据不被窃取或篡改等。隐私保护是指通过一系列技术手段和政策措施，合法收集、使用和处理个人信息，防止个人信息被非法获取和滥用。随着大数据和人工智能等技术的发展，个人隐私面临的挑战越来越大。隐私保护技术包括匿名化、去标识化、数据脱敏等，降低个人信息泄露的风险。同时，各国政府和国际组织也在不断完善隐私保护的法律法规和标准，充分地尊重和保护个人隐私。

4 结束语

在计算机网络信息安全的领域中，数据加密技术如同坚固的盾牌，时刻保护数字资产与隐私不受侵害。随着科技的快速发展，无论是个人还是企业，都对数据安全提出了更高的要求。数据加密技术不仅满足了这一需求，还在不断地进化与完善中，应对日益复杂的网络安全威胁。从传统的加密方法到现代的同态加密、后量子密码学，每一种技术都代表人类对安全的追求与智慧。未来，随着技术的不断进步，数据加密技术将在保障网络信息安全方面发挥更加重要的作用，为构建一个更加安全、可信赖的数字世界提供坚实的技术支撑。

参考文献：

[1] 李明国.基于数据加密技术的计算机网络数据安全传输方法[J].信息与电脑，2022，34（15）：229-231.
[2] 陈运财.基于改进遗传算法的计算机网络通信数据加密方法探析[J].工程技术研究，2023，8（13）：219-221.
[3] 韩维，安业腾，史嘉琪.计算机网络安全中数据加密技术的运用研究[J].大众标准化，2023（14）：184-186.
[4] 王华.计算机网络安全中数据加密技术的应用[J].电子元器件与信息技术，2021（13）：76-77.
[5] 韦斌松.数据加密技术在计算机网络安全中的应用[J].数字通信世界，2022（12）：99-101.