论数据加密技术在计算机网络安全中的应用

王梦仙　侯红科
（厦门南洋职业学院，福建 厦门 361101）

摘要：互联网时代下，人们的工作生活都离不开互联网技术与平台，但互联网为人们带来便利的同时，也出现了许多信息安全问题与挑战。因此，数据加密技术也随着计算机网络技术的更新换代同步提升。当前，数据加密技术已成为保障计算机网络使用安全的一种重要手段。基于此，本文将简要介绍计算机网络安全中的数据加密技术，并浅析数据加密技术在计算机网络安全中的应用。

关键词：数据加密技术；计算机；网络安全

计算机技术为人们带来更加方便高效的数据处理、传输和储存服务的同时，也带来了许多信息安全问题。在计算机网络中，数据在传输过程中会面临截获、篡改和伪造等各种潜在的威胁。而数据加密技术则是通过使用密码算法对数据进行加密和解密，以确保只有指定的接收方能够解密和获取数据。通过加强数据加密技术的研究和应用，可以提高计算机网络安全防护的能力和水平，保障数据的机密性和完整性，降低网络攻击和数据泄露的风险。同时，数据加密技术的发展和创新也有助于推动整个计算机网络安全领域的进步和发展。

一、数字加密技术概述

（一）对称加密技术

对称加密技术是基于使用相同的密钥对数据进行加密和解密的原理。在此过程中，发送方和接收方需要共享密钥来确保数据的保密性和完整性。对称加密算法的核心思想是通过对数据进行替代、混淆和转换等操作，使得未经授权的个体无法理解或解析出原始数据的内容。在加密过程中，发送方使用密钥将明文转换成密文，然后将密文通过网络传输到接收方。接收方使用相同的密钥对密文进行解密，还原成原始的明文消息。常见的对称加密算法有 DES、AES 等。DES 是一种经典的对称密钥加密算法，采用分组密码的方式对 64 位的数据进行加密和解密。但 DES 中的 56 位密钥长度较短，存在被暴力破解的风险，存在一定的安全性问题，现今虽然已经不再推荐使用，但 DES 仍然是安全算法设计的基础。AES 是当前应用最广泛的对称加密算法，支持 128 位、192 位或 256 位密钥对数据进行加密，以满足不同计算机网络安全需求。在网络通信、移动设备、物联网等领域，都有 AES 的身影，它起到着保护敏感信息、确保数据的机密性和完整性的重要作用。

（二）非对称加密技术

与对称加密技术不同，非对称加密技术使用了一对密钥，即公钥和私钥，用于加密和解密数据。其中，公钥可以公开给任何人使用，而私钥则只有密钥的持有者才能访问。RSA 是经典的非对称加密技术，密钥长度为 1024 位或者更长，大大增加了破解密钥的难度。但密钥长度也使加密和解密过程需要大数模幂运算。因此，相比对称加密算法，RSA 的运算速度较慢。非对称加密技术的应用范围非常广泛。一方面，可以用于保护数据传输安全。在使用非对称加密技术进行通信时，发送方首先使用接收方的公钥对数据进行加密，接收方则使用私钥对数据进行解密。这样，即使在数据传输过程中被截获，黑客也无法解密数据，保证了数据传输的安全性。另一方面，还可以应用于数字签名。数字签名可以用于验证消息的真实性和完整性。发送方可以使用私钥对消息进行签名，接收方则使用公钥对签名进行验证。此外，非对称加密技术在数字证书、数字货币等领域也有着很高的应用价值。总之，非对称加密技术作为一种高度安全和可靠的加密方式，为计算机网络安全提供了重要的保障。

二、计算机网络安全中的数据加密技术

（一）链路加密

在计算机网络中，链路指的是两个节点之间的物理或逻辑连接。由于链路是数据传输的基础，而网络链路往往是公共环境，容易受到各种病毒或黑客攻击。基于此，链路加密应运而生。链路加密通过使用加密算法对数据进行加密，从而保护数据在链路上传输时的安全性。在实际应用中，链路加密技术在局域网、广域网等各种网络环境中都有广泛的应用。例如，在企业内部局域网中，链路加密可以保护内部数据的安全性，防止机密信息被泄露。在互联网中，链路加密可以用于保护用户在网上交易、支付等过程中的数据安全。

（二）节点加密

节点加密是通过对通信中的节点进行加密，可以有效保护数据的安全性和完整性。在实际应用中，技术人员在节点处设置一个密码装置，并将其与节点相连，在该节点处需要解密密文，并将其重新加密。需要注意的是，使用节点加密必须保证路由器等设备信息处于绝对安全的状态，进而才能保证后续网络节点信息处理的安全性。常用的节点加密包括身份验证、访问控制和数据加密等。例如，在企业内部局域网中，通过对节点进行身份验证和访问控制，可以防止未经授权的外部节点接入网络，从而保证企业机密数据的安全。

（三）软件加密

软件加密主要用于保护计算机软件的安全性和完整性。在计算机网络安全中，软件加密可以有效地防止黑客获取未经授权的软件副本或篡改软件代码的行为。随着互联网技术的飞速发展，计算机软件的传播和复制变得更加容易，这给软件安全保护带来了巨大挑战。而通过对软件进行加密，可以有效防止未经授权的复制和传播。另外，软件加密还可以防止黑客篡改软件代码，从而确保软件使用者信息数据的安全性。在日常生活中，人们通常使用杀毒软件、病毒检测软件等对计算机软件使用安全进行保护，以确保计算机软件数据处于安全的运行环境。

（四）密钥加密

密钥加密技术将明文数据转换为密文数据，从而保证数据的机密性。密钥加密技术可分为公用、私用两种，公共密钥主要为数据获得方开启数据密钥，利用单独密钥提高数据使用的安全性。而私用密钥需要与接收方建立私密的数据传输通道，双方共同设置统一的密钥，以保障数据安全。公用密钥在安全性上要优于私用密钥，因为只有拥有准确密钥才能够解密和访问数据，这可以有效避免数据泄露。尤其在电子商务中，密钥加密技术在保护用户的交易数据和个人信息能够发挥出重要作用。

（五）数据库加密

数据库是存储大量敏感信息的地方，如电商平台上个人信息、银行账户数据和企业机密数据等，保护数据库中的数据免受未经

授权的访问和恶意攻击的威胁至关重要。但互联网技术的蓬勃发展，不法分子的计算机技术也越来越高。因此，除了密钥加密外，还需增加数据库加密。通过使用数据库加密算法，将敏感数据加密，使得即使数据库被黑客攻击或内部人员恶意访问，也无法直接获得明文数据。这种加密技术可以有效降低数据泄露的风险，以保护用户的隐私和企业的重要信息。

三、数据加密技术在计算机网络安全中的应用分析

（一）数据加密技术在局域网中的应用

随着互联网技术的日新月异，局域网已成为许多企事业单位的重要办公方式，企业工作人员可以通过局域网进行线上会议、跨部门数据整合和报告生成等。然而，局域网的安全性一直是一个备受关注的问题。数据加密技术在局域网中的应用，可以有效地提升局域网的安全性，保护数据的机密性和完整性。首先，局域网中的通信传输过程中，数据加密技术可以用于保护数据的传输安全。通过使用加密算法对数据进行加密，在数据传输的过程中，即使被第三方截获，也无法解密和获取其中的具体信息。这种安全机制可以防止数据被窃取，保障数据传输的机密性。其次，局域网中的文档和文件传输过程中，数据加密技术可以通过对文件进行加密，即使文件被非法访问，未经授权的人员也无法打开和查看其中的内容。这在公司的财务数据、商业机密等文件传输中尤为重要。在实际企业数据安全保护过程中，可以通过使用强密码、多因素身份验证和定期更新访问权限等访问控制措施，全面提升局域网的数据安全。另外，西工大网络攻击事件也为局域网安全防护工作提出了警醒。一方面在网络层面，应采用多层防火墙保护，细化数据访问策略。另一方面还需要将数据操作纳入统一日志系统，实现数据访问的可追溯。

（二）数据加密技术在电商平台中的应用

电子商务平台的兴起为现代商业带来了巨大的便利和发展机遇。然而，随着电商平台的广泛应用和用户规模的不断扩大，安全问题也逐渐凸显出来。数据泄露、恶意攻击和网络欺诈等问题已成为电商平台必须面对和解决的重要挑战。在此背景下，数据加密技术在电商平台中的应用显得尤为重要。一方面，用户在使用电商平台进行购物交易中，通常会涉及用户个人信息、银行账号、交易记录等大量的隐私数据。一旦这些隐私数据被他人盗取，违法使用，不仅会对用户个人造成严重的经济损失，也会使电商平台的可靠性受到质疑。对此，电商平台应采用对称加密和非对称加密技术，对这些敏感数据进行加密，以保证数据不被不法分子盗取，且即使在传输或存储过程中恶意获取，也无法获得实际有用的信息。另一方面，电商平台的交易过程中还涉及支付密码、交易金额等金融数据的处理。对此，电商平台可以在交易过程中采用密钥加密技术，以确保交易数据的机密性和完整性。只有经过正确的密钥验证，才能进行数据解密和交易确认，从而有效防止第三方的攻击和数据篡改。例如，对于支付密码，电商平台可以设置相应程序，如密码连续输入三次不正确，将立刻停止交易并锁住账户，以保障用户和交易的安全，为用户提供更加安全放心的购物体验。

（三）数据加密技术在软件中的应用

只有借助各类软件，计算机才能更好地发挥出其应用功能价值。在此过程中，数据加密技术在计算机软件中有着广泛的应用，主要用于保护软件和数据的安全。一是保护软件源代码。软件的源代码是软件的核心部分，需要重点保护以防止被盗用或篡改。通过使用数据加密技术，可以将软件的源代码进行加密，确保只有软件授权的开发人员才能够访问和修改。二是软件许可证验证。为了防止软件被非法复制或使用，可以使用数据加密技术对软件许可证进行验证。当软件启动时，自动对许可证进行验证，确保其有效性。这样可以保证只有合法的用户能够使用软件。例如，企业在进行软件安装及初次使用时，需要让软件开发技术人员现场对软件进行签名验证，防止软件在传输过程中被篡改或恶意替换。三是保护数据安全。在计算机软件中，经常需要存储和处理一些用户的个人信息和使用数据。通过使用数据加密技术，对这些敏感数据进行加密，确保只有授权的人员能够访问，从而进一步防止数据泄露和被非法获取。例如，华为云服务器提供了多种文件加密方法，如文件级别加密和应用级别的加密等。文件级别加密可以通过华为云服务器的控制台进行设置，用户只需要在控制台选择需要加密的文件，然后点击“加密”按钮即可。华为云还可以提供应用级别的加密功能，用户可以在应用服务器上设置加密策略，然后在应用运行时使用加密策略。

（四）数据加密技术在数据库中的应用

在大数据时代，人们的日常生活和工作都离不开对数据库的应用。比如，在金融行业，数据库加密可以保护用户的账户信息和交易记录；在医疗领域，数据库加密可以确保患者的病历和医疗数据的安全；在企业内部，数据库加密可以保护公司的机密信息和商业秘密。因此，数据库中数据的保护变得尤为重要。数据加密技术在数据库中的应用主要分为存储加密和传输加密。存储加密是指在数据存储到数据库之前对其进行加密处理。一种常见的方法是使用对称加密算法对数据进行加密。对称加密算法使用相同的密钥进行加密和解密，因此在数据库中存储的数据需要在被访问时使用正确的密钥进行解密。这种方法能够有效保护数据的机密性，但是密钥的管理和分发成为一个挑战。传输加密是指在数据在数据库和应用程序之间传输时对其进行加密。一种常见的方法是使用 SSL 或 TLS 协议。以支付宝为例，其在支付过程中会使用 SSL 协议加密用户的个人和交易信息。这一技术通过将数据进行加密，确保用户的敏感信息不会被恶意用户窃取和利用，提高了用户在电子商务平台上的安全感。除了存储加密和传输加密，还有其他一些数据库加密技术。例如，数据字段级加密可以对数据库中的敏感数据进行针对性加密，只有经过授权的用户才能够解密和访问这些数据。这种方法能够更加精细地控制数据的访问权限，提高数据的安全性。

四、结语

综上所述，随着现代化科技的创新发展，计算机网络安全中的局限与不足也随之暴露出来。对此，我们需要加强对数据加密技术的研究与应用，以防御计算机网络安全中的风险与挑战。通过对链路加密、节点加密、软件加密、密钥加密、数据库加密等具体加密技术的应用，维护计算机网络的稳定运行，保护各类数据信息的机密性和安全性。从而使企业工作人员和个人用户都能安全放心地使用计算机软件和网络进行工作生活，进而促进我国社会经济的高质量发展。

参考文献：

[1] 刘姜 . 数据加密技术在计算机网络安全领域的应用分析 [J]. 电大理工，2023（03）：28-31.

[2] 闫军 . 数据加密技术在计算机网络信息安全中的应用研究 [J]. 信息记录材料，2023，24（09）：152-154.

[3] 孙东旭，刘冬菊 . 浅析数据加密技术在计算机网络安全中的应用价值 [J]. 信息系统工程，2023（08）：52-55.

[4] 余松 . 基于数据加密技术的计算机网络通信安全研究 [J]. 数字通信世界，2023（07）：25-27.

[5] 董真 . 计算机网络安全中数据加密技术分析 [J]. 信息与电脑（理论版），2023，35（05）：223-225.