计算机网络安全防护中数据加密技术的应用

雷雪梅

北京科技大学 信息化建设与管理办公室，北京 100000

DOI: 10.61369/VDE.2025230040

摘　　要： 互联网的迅猛发展，使得计算机在网络安全、数据安全方面面临更多新的风险，而数据加密技术则成为数据保护最重要的手段之一。本文对其应用意义、策略进行了重点探究，目标是提高数据机密性、保障其完整性，增强网络通信及数据防护安全性。具体策略为：依据场景选对称或非对称加密算法、强化密钥生成存储与更新管理、组合加密技术并协同防火墙等措施。研究表明，重视数据加密技术，加强其科学应用，并构建完善的防护体系，有利于更好地应对安全风险，助力网络安全的稳定运行。

关 键 词： 计算机；网络安全防护；数据加密技术

Application of Data Encryption Technology in Computer Network Security Protection

Lei Xuemei

Office of Informatization Construction and Management, University of Science and Technology, Beijing 100000

Abstract: With the rapid development of the Internet, computers are facing more new risks in terms of network security and data security, and data encryption technology has become one of the most important means of data protection. This paper focuses on exploring its application significance and strategies, aiming to improve data confidentiality, ensure its integrity, and enhance the security of network communication and data protection. The specific strategies are: selecting symmetric or asymmetric encryption algorithms according to scenarios, strengthening the generation, storage and update management of keys, combining encryption technologies and coordinating with measures such as firewalls. Research shows that attaching importance to data encryption technology, strengthening its scientific application, and constructing a sound protection system are conducive to better responding to security risks and supporting the stable operation of network security.

Keywords: computer; network security protection; data encryption technology

随着信息技术的深度集成与应用，计算机网络已成为社会运转不可或缺的基础设施并深度融入人们生活，无论是日常办公、学习，还是在线购物等都能看到其身影。与此同时，计算机网络安全问题也逐渐凸显出来，不仅出现了黑客攻击事件，数据泄露和恶意入侵等事件也频繁发生，给个人用户、企业用户造成了巨大损失。数据加密技术在计算机网络安全方面发挥着重要作用，借助对数据的特殊编码，能够对数据进行转化，使其成为密文，而拥有正确密钥至关重要，唯有此，相关接收者才能正确解读，避免数据在传输、存储等过程中出现意外，如被窃取、篡改等，有利于增强数据保密性、完整性、可用性[1]。而数据解密技术作为其逆过程，则确保了经授权的用户能够使用正确的密钥，将密文准确、快速地还原为可用明文，是数据价值最终实现的保障。这一对互逆过程共同构成了数据安全流转的闭环。基于此，深入研究数据加密技术在计算机网络安全防护中的应用意义、策略具有重要的现实意义。

一、计算机网络安全防护中数据加密技术应用的意义

（一）保障数据的机密性

数据机密性指的是对信息进行保护，使其既不被泄露，也不暴露给未经授权的实体，以此来保障信息安全。数字化浪潮下，各类数据大量涌现，呈现出爆炸式增长的态势，其中包含企业商业机密、个人隐私相关数据等信息。数据加密技术有利于保障数据机密性，借助特定算法，能够把原始明文数据进行转化，使其成为密文[2]。

如电商企业对关键数据信息如用户购买记录、支付相关信息采用加密算法，有效避免了数据泄露方面的风险，既保护了用户的隐私，又大力维护了企业的信誉。而如果不对这些数据进行加密，当数据被窃取时，不仅导致用户隐私曝光、财产损失，还会给企业带来信任危机。因此，重视数据加密技术势在必行[3]。

（二）维护数据的完整性

数据完整性和数据精确性、可靠性息息相关，其强调数据在

传输、存储等过程中，不被篡改、篡改后能迅速被发现，保障信息可靠、准确。数据加密技术有利于维护数据完整性，其中，最为常用的手段为哈希算法。该算法能够对数据（包含任意长度）进行转换，使其成为固定长度的哈希值[4]。

以金融交易数据为例，所有的交易信息都会计算2次其哈希值，一次为传输前，一次为到达接收端之后，并和原始值进行对比。如果二者一致，则说明数据在这个过程中并未被篡改，为交易数据完整性提供了有效保障，即交易的金额、对象等信息没有错误，保障了交易准确性、公平性[5]。

（三）提升网络通信的安全性

在网络通信过程中，数据并不是高枕无忧的，而是面临诸多风险，如网络窃听、黑客攻击等。黑客可借助系统漏洞，对通信中的敏感数据进行窃取；网络窃听则通过对传输信息的截取，窥探隐私、获取商业机密[6]。数据加密技术的出现和应用，有利于提升数据在网络传输过程中的安全性。

当前，SSL/TLS（安全套接层 / 传输层安全）协议广泛应用在网络通信中，当用户登录电子商务网站的时候，基于SSL/TLS协议，对用户名、密码等信息进行加密。加密过程在这些信息传输前完成[7]。客户端、服务器在握手阶段对加密算法、密钥进行协商，加密数据通过密文形式在网络中传输。即使数据被窃取，也不用过于担心，因为攻击者缺乏解密密钥，获取的数据无法还原。这种方式有利于防止用户信息泄露；同时，也保障了通信安全，助力电子商务通过网络通信业务顺利开展[8]。

二、计算机网络安全防护中数据加密技术的应用策略

（一）根据不同场景选择合适的加密算法

数据安全需要科学合理地选择加密算法。由于使用场景不同，其安全需求、性能要求也不尽相同，为此，应根据实际情况来选择加密算法。

1. 对称加密算法的适用场景

对称加密算法作为一种加密方式，具有广泛的应用基础。其原理为加密与解密所使用的密钥相同。发送方借助该密钥来转换明文数据，使其成为密文，接收方收到之后，借助相同密钥开展逆向操作，从而对明文进行还原[9]。该算法优势是加密的速度快，对于大量数据的处理可以在较短的时间内完成，计算量小，效率高。如果对加密的速度要求较高，且通信双方存在较高的信任度，密钥管理方便，且为局域网场景，加密算法的表现较为突出。

很多企业建设了企业内部文件共享系统，企业员工彼此之间信任度较高，且局域网的环境封闭，为密钥分发、管理创造了有利条件。在此情况下，借助对称加密算法进行加密，这里主要指的是对共享文件的加密，便于员工对该文件进行快速上传、下载，有利于保障数据传输效率、安全性。

2. 非对称加密算法的适用场景

非对称加密算法，也称为公钥加密算法。其核心要义是使用一对密钥，即公钥和私钥。二者区别为：公钥顾名思义就是可以公开，所有人都能获取，并能将其用于加密数据；私钥则需要严格保密，限定为解密数据的人，即密钥拥有者才能解密。该加密方式优势为，即使公钥被窃取，也无法获得私钥，有利于保障加密信息安全。

如果对安全的要求性较高，需要使用身份认证、数字签名的独特场景，可使用该加密算法。如针对电子银行转账业务，客户使用银行的公钥来对转账信息加密。银行接收数据后，使用私钥进行解密；与此同时，银行使用私钥对交易确认信息进行数字签名，客户则可通过公钥对签名真实性进行验证，以保障交易双方身份，提高数据传输安全性、完整性。

（二）加强密钥管理

密钥在数据加密中属于核心要素，其管理的安全性至关重要。为此，应严格加强密钥管理，以保障加密技术充分发挥自身的功效。

1. 密钥的生成与存储

密钥生成应具有一定复杂度，注重随机性，从而保障其无法被破解。在生成密钥时，可借助专业随机数生成器，基于复杂算法生成密钥。该密钥在保障长度的同时，应是无规律的。以AES算法作为具体案例，密钥长度包含多种选择，如128位、192位和256位等，长度越长，破解难度越大，有利于增强数据安全性。

在重视密钥生成的同时，也不应忽视其存储的安全性。为此，可借助硬件加密模块在物理层面保护密钥，防止其被非法读取、篡改。目前，密钥管理系统的应用越来越广泛，如应用于管理密钥，为密钥安全存储、分发等提供了强大助力。

2. 密钥的更新与更换

为了降低密钥泄露风险，应定期更新、更换密钥。当前，密钥面临的安全威胁与日俱增，黑客可借助多种手段破解密钥，如果不定期更换密钥，一旦被破解，加密的数据随之会面临一系列安全风险，如篡改风险、窃取风险等。定期更换密钥有利于降低该风险，即使旧密钥被破解，由于密钥已更新，黑客也无法破解、获得加密数据的相关内容。

对密钥的更新、更换，需要遵循科学流程，明确注意事项。保障新密钥生成符合安全性要求；在更换密钥时，应确保业务连续性，降低密钥更换副作用，如系统故障、数据丢失等。如某电商平台由于未对密钥进行及时更新，使得黑客借助密钥漏洞，窃取用户订单信息、支付数据，用户蒙受经济损失的同时，也对平台声誉造成了不利影响。该案例启示我们，应重视密钥更新、更换工作，以确保数据安全[10]。

（三）结合多种加密技术和安全措施

网络环境错综复杂，如果仅采用单一加密技术，则无法满足安全防护相关需求。结合多种加密技术，并通过安全措施协同工作，有利于构建一个更为完善的安全防护体系，抵御网络安全威胁。

1. 加密技术的组合应用

把对称加密与非对称加密技术结合在一起，有利于发挥二者优势，使其各展所长。对称加密算法的加密速度快，能够快速处理大量数据；非对称加密算法具有较高的安全性，多应用在身份

认证、密钥交换环节。在实际应用时，常借助非对称加密传输对称加密的密钥。当用户和服务器建立通信连接的时候，由服务器发送公钥给用户，用户借助该公钥对生成的对称加密密钥进行加密，并将其发送给服务器，服务器接收后，借助私钥来解密，得到了对称密钥，然后，双方借助该对称密钥来对数据进行加密传输。

目前广泛使用的 VPN 通信技术就采用了此加密技术。借助非对称加密进行沟通协商，从而给出会话密钥，再借助对称加密对传输数据进行加密，确保密钥传输安全性的同时，提高数据加密、解密效率，此外，也使得 VPN 的通信安全性、稳定性获得了显著提升，为数据在公网传输过程中的数据保密性及完整性提供了有效保障。

2. 与其他安全措施协同

为应对日益增长的安全风险，构建网络安全防护体系至关重要。即不仅使用加密技术，还应同时采用其他安全措施，如防火墙、访问控制等。通过技术措施协同工作，提高网络和数据防护能力。如：防火墙是重要的边界防护设备，是局域网网络安全之重要防线。能够基于预设安全策略来拦截恶意访问，将未经授权的访问、恶意攻击阻挡在“门外”；入侵检测系统则通过对网络流量的监测，发现可能存在的入侵行为，并能及时警报。访问控制基于用户身份、权限来对其网络资源访问范围进行限制。

将企业网络安全防护架构作为具体的案例，数据加密技术主要工作为对企业内部数据保密性、完整性提供保障，防火墙将外部非法网络访问阻挡在外等。在这些措施的相互配合下，入侵检测系统能够迅速察觉是否有外部攻击突破防火墙，并通知管理员，与此同时，在数据加密技术的支持下，就算部分数据被窃取也不用过于担心，因为攻击者无法解密其内容。总之，借助协同工作，有利于提升企业网络安全性，降低其网络安全风险。

三、结语

数据加密技术在计算机网络安全防护中属于核心技术，在保障数据机密性、维护数据完整性和提升网络通信安全性等方面发挥着重要作用。通过基于不同场景选择对称加密算法、非对称加密算法等适合的加密算法，并加强密钥管理，包括密钥的生成与存储、更新与更换等，同时结合多种加密技术、安全措施，有利于提升计算机网络安全、数据安全的防护水平。

参考文献

[1] 顾思义 . 数据加密技术在计算机网络通信安全中的应用 [J]. 现代工业经济和信息化 ,2023,13(2):145-147.

[2] 张良梁 . 数据加密技术在计算机网络通信安全中的应用 [J]. 计算机应用文摘 ,2024,40(17):117-119.

[3] 林婧 . 数据加密技术在计算机网络通信安全中的应用探究 [J]. 数字通信世界 ,2024(4):125-127.

[4] 甘建芳 . 数据加密技术在计算机网络安全系统中的实践应用 [J]. 电脑知识与技术 ,2024,20(36):79-82.

[5] 张元元 . 数据加密技术在计算机网络安全领域的应用研究 [J]. 中国管理信息化 ,2024,27(24):175-177.

[6] 吕达 . 在计算机网络安全中数据加密技术的应用分析 [J]. 科技资讯 ,2023,21(13):19-22.

[7] 王新可 . 互联网环境下计算机网络数据安全加密技术 [J]. 信息记录材料 ,2023,24(6):76-78,82.

[8] 王艳淼 , 熊国灿 . 计算机网络通信安全中数据加密技术的应用研究 [J]. 软件 ,2022,43(4):184-186.

[9] 张宁 . 计算机网络安全中数据加密技术的应用 [J]. 微型计算机 ,2024(10):76-78.

[10] 王伟平 , 许亮 , 李国强 . 数据加密技术在计算机网络安全中的应用 [J]. 移动信息 ,2024,46(5):161-163.

